防駭簡易入門

（一）基本觀念

1. 重視網路安全及具有危機意識
2. 清楚每部連線主機提供的網路服務、連線範圍及網路使用者
3. 不必要的服務必需將其關閉
4. 隨時注意新公布的漏洞、入侵事件
5. 使用防火牆系統
6. 密碼不要取得太簡單
   - 至少 8 位元
   - 應由字母、數字和特殊符號交叉組合而成
   - 避免用自己名字的英文拼音、常用的英文單字、電腦中常出現的單字及出生日期等
7. 經常檢視系統記錄、日誌檔等
8. 不隨便讀信
9. 不隨便執行陌生人的軟體
10. 不隨便下載網路上的軟體
11. 定期檢查系統設定檔、啟動檔及登錄檔（registry）

Hkey_Local_Machine\Software\Microsoft\Windows\Currentversion\Run
Hkey_Local_Machine\Software\Microsoft\Windows\Currentversion\RunService

12. 定期作備份

將系統碟與資料碟分開存放

- 用 ghost 作備份

（二）駭客工具

1. P/PORT 掃描
   - Nmap (http://www.insecure.org/nmap)
     - (ping) nmap –sP 210.240.39.*
       nmap -sP 210.240.39.0/24
     - (port) nmap -sT 210.240.39.3 (-sT 為內定值)
     - (port) nmap -sU 210.240.39.3
     - (Stealth) nmap -sS 210.240.39.3
     - （OS） nmap -O 210.240.39.3
   - ipscan
     - Angry IP scanner (www.angryziber.com/ipscan)
     - IP Network Browser (ftp://www.newhua.com/IPNetworkBrowser.exe)
   - Portscan
     - Portscan (www.zone-h.com/en/download/category=39/)
2. 網路芳鄰掃描
   - netview (含 ipscan、portscan、及密碼破解)
     www.webattack.com/get/netview.shtml

3. 漏洞掃描
   - ISS (www.iss.net)
   - NESSUS (www.nessus.org)
   - SATAN (www.porcupine.org/satan)
   - 漏洞舉例：
     - c:\con\con ; c:\nul\nul ; c:\aux\aux
     - \\210.60.47.50\c\con\con　只要對方資源分享設成 read，即可使其當機
4. 木馬程式
   - BO2K (bo2k.sourceforge.net)
   - SubSeven (home.t-online.de/home/TschiTschi/subseven_20.htm)
   - 掃除木馬可用下列程式
     - cleaner　(www.moosoft.com)
     - Trojan Hunter (www.mischel.dhs.org/trojanhunter.jsp)
5. 紅客帝國之七種兵器

冰河、IPhacker、OICQ“補丁”、Superscan3.0、文件捆綁專家、郵箱終結者、流光（小榕軟件下載）

6. 密碼入侵
   - brutus (www.hoobie.net/brutus/brutus-download.html)
   - wwwhack (http://www.gnusec.com/resource/security-stuff/Password Tools/)
7. 入侵偵測系統

   SNORT　(www.snort.org)

（三）防駭軟體
   - 免費

ZoneAlarm (www.zonelabs.com)
天網 (www.skynet-taiwan.net) 下載服務－試用下載－免費註冊
   - 收費

Lockdown2000
Blackice

（四）偵測本身電腦狀況

賽門鐵克網路安全診斷室（www.symantec.com/tw-ssc ）進入「入侵弱點偵測」，可掃描網路漏洞、NetBIOS 可用性、特洛依木馬、瀏覽器隱私權四大項

（五） 其他攻擊
   - DOS (Denial of Service)、DDOS (Distribute Denial of　Service)
   - 郵件炸彈 (Kaboom, Haktek)

     Kaboom　(http://elitesecurity.addr.com/email.html)

     郵件炸彈可用下列程式清除
     - email remover (http://www.eremover.bizhosting.com/)
     - email chomper (http://www.sarum.com/echomp.html)
   - Ping to Death
   - IP Spoofing

（六）參考網站

1. www.stic.gov.tw 進「資通安全通訊網」－「SDI 註冊」
2. www.cert.org.tw

3. www.rootshell.com
4. Linux 安全交流網

（七）參考書籍

1. 中國大陸的駭客技術 松崗 閻雪編著
2. 網路安全最佳化 碁峰 李蔚澤、胡銘珍譯
3. 駭客入侵不求人 碁峰 林東和
4. 駭客實戰不求人 碁峰 林東和
5. 對不起駭到你 第三波 秘密客
6. 駭客解凍 Web 網站篇 知城科技 鮑友仲