淺談資訊安全與管理

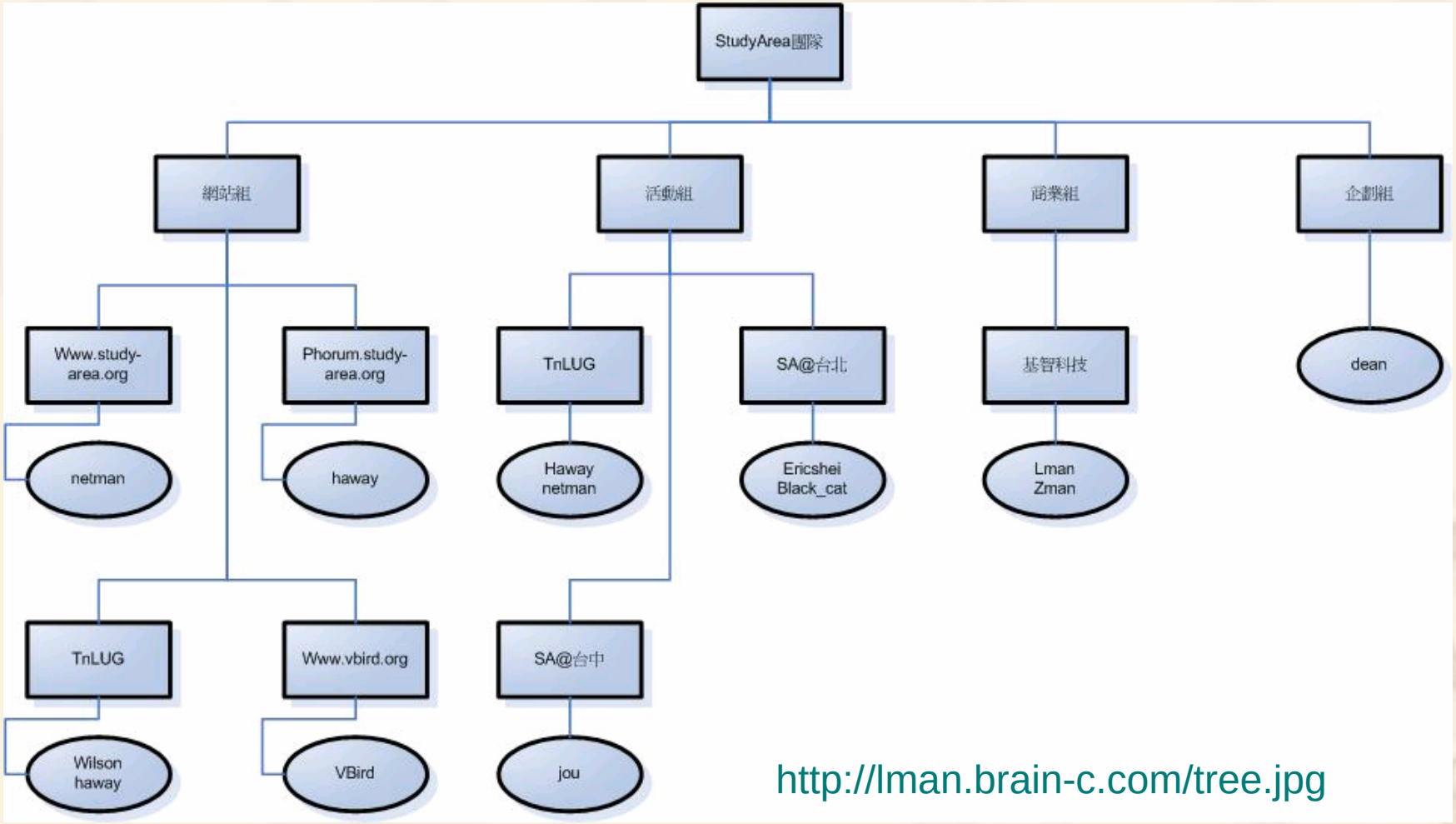
VBird
<vbird@mail.vbird.idv.tw>

2005/11/06

Study Area 團隊簡介

- Study Area：
  - 最早由 Netman 發起，主持 http://www.study-area.org 網站的撰寫；
  - 台南幫 TnLUG 的成立，加入梁楓、鳥哥等主要核心成員，舉辦大型 Linux 群英會；
  - 酷學園成立 (http://phorum.study-area.org)，將 Open Source 帶到全台，而有：台北@SA、台南@SA、台中@SA 等等窗口；
  - Study Area 爲一學習園地，其人才培養由基智科技負責培訓，所有商業行爲亦委由基智科技負責，讓加入 Open Source 的朋友們不擔心麵包的問題；

Study Area 團隊簡介



http://lman.brain-c.com/tree.jpg

什麼是資訊安全？

- 你的資料放置在電腦上面，該資料很重要，那就是資訊；
- 這些資訊可能在任何管道被不法取得，因此，如何讓你的電腦可以保障這些資訊，那就是安全。
- 根據這樣的說法，因此，你必須要在兩部分加以考量：
  - 單一主機上頭的資料安全：file permission等；
  - 網路上頭的安全性：漏洞、防火牆補強等。

幾個不懂資安人員的困惑

鳥哥的被駭全記錄

來自 moto 的一個小故事

鳥站最近被攻擊的記錄

鳥哥的被駭全記錄
--鳥哥的電腦學習歷程

- 大學前：
  - 因爲要玩 DOS Game 所以需要摸command；
  - 而且需要瞭解批次檔(*.bat)；
- 大學：(都與資訊/電腦無關的環工….)
  - 自學程式語言(Basic/Quick Basic)
- 碩士班：
  - 買第一部電腦，開始瞭解 PC 的硬體架構；
  - Windows 95 出現，玩系統的超頻、與穩定性測試；
- 博班：
  - 研究需要而接觸 Unix；
  - 利用 PC 上的 Linux 替代方案；

鳥哥的被駭全記錄
--鳥哥的 Linux 學習歷程

- 以 Windows 的概念接觸 Linux 時期：
  - 直接安裝 Red Hat 6.1，完全以系統預設值來安裝；
  - 只會圖形介面的操作方式；
  - 圖形介面整合度不好，容易當機；
  - 最糗的遭遇：**以『重新安裝』來切換 Run level……**
- 瘋狂架站時期：
  - 對於 Linux 系統並不熟悉，也不懂網路安全概念
  - 買書，按圖索驥架設各種網站，主要: Mail, Web, Proxy
- 傷心失意階段：
  - 曾被 FTP 2GB 的問題，導致整個區網停頓
  - 追蹤後，發現 mail server 已被列入黑名單中
  - Proxy server 被發現嘗試入侵國外的主機系統….

鳥哥的被駭全記錄
--鳥哥的 Linux 學習歷程(續)

- 重新奮發向上階段：
  - 將系統完全關閉，並閉關開始學習Linux基礎。
  - Study Area 之『電腦基礎』與『網路基礎』；
  - http://www.study-area.org
  - 架設測試機，實作階段，磨練功力；

- 網站撰寫階段：
  - 紀錄自己發現的各項問題與解決之道；
  - http://linux.vbird.org
  - 開始瀏覽Internet上面的種種問題，並設法以自己的想法解決。

鳥哥的被駭全記錄
--鳥哥的 Linux 學習歷程(續)

- 接觸不同網路規模與環境階段：
  - 小型網路環境：家裡、宿舍、實驗室
  - 稍微大一點的環境：系上網路環境
  - 再稍大一些：補習班與小公司
  - 算是中型企業：入伍後接觸的網路環境(南巡局)

- **規模不同，思考不同**
  - 小型企業：環境單純、價格第一
  - 中大型企業：環境複雜、基本配線與硬體搭配很重要、各項物品的售後服務、**Total Solution 才是王道**！

鳥哥的被駭全記錄
--鳥哥的 Linux 學習歷程(續)

- 第一階段：
  - 會一點電腦概念，自以爲了不起，接觸 Linux 就直接搞架站，導致整個區網的網路安全性問題；
  - 由上而下(爲了搞架站，才不得已學習 Linux 基礎系統)的學習，粉累；
- 第二階段：
  - 遭遇挫折，開始平心靜氣的由下而上學習(先學Linux系統基礎，網路基礎，架站完全先不碰)，很累，但是很有成就感。
  - 從前遇到的問題，都『不是問題』；
- 第三階段：
  - 視野開拓、認識更多網路朋友；
  - 會使用 Linux 不是最重要的，用 Linux 達成目的才是重點。還有 free software的概念、total solution 的概念等。

來自 moto 的一個小故事

- http://moto.debian.org.tw/viewtopic.php?t=6572
  - 起因：只是因爲那名『優秀的駭客』懷疑自己被踢出聊天室而已～

鳥站最近被攻擊的記錄

- http://phorum.vbird.org/viewtopic.php?t=21939
  - 起因：只是因爲大家給的建議偏向於實際處理；
  - 結果：鳥站遭受到 DDoS 的攻擊約 5 分鐘；

重大問題

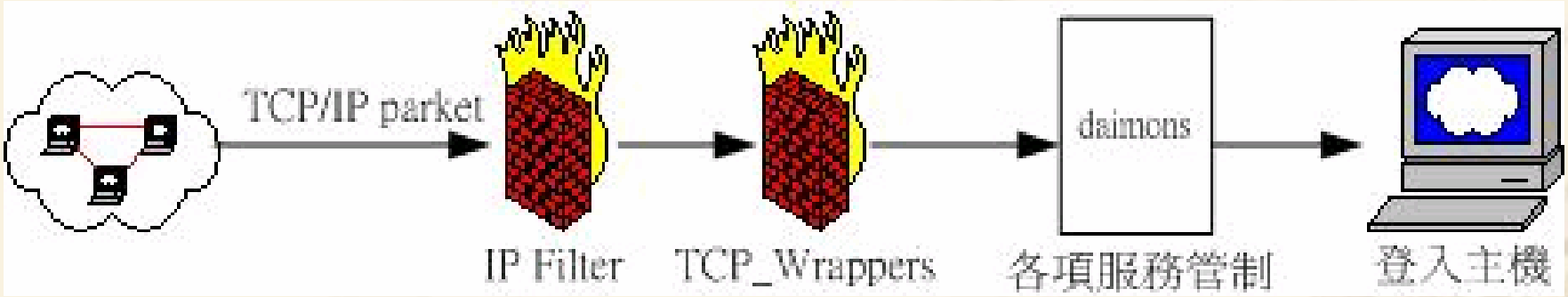
- 駭客軟體取得容易，小孩也可以拿到機關槍，誰會被掃射到？只有天知道；
- 網管人員沒有良好的訓練，『制約』性的行爲觀念『被入侵？啊就重灌就好了～有這麼嚴重嗎？』報告～確實已經很嚴重～ @_@
  - 頻寬被耗光、工作無法進行；
  - 作爲僵屍電腦，被 cracker 利用於攻擊別人；
  - 影響單位或者是您自己的隱私或機密資料；
- 網站定位的問題：
  - 單一主機：維護上較爲簡單；
  - 內部主機：需要區分什麼是是內？什麼是外？使用者層級？教育訓練？標準操作程序 (SOP) 的製作等等；

主機資料被竊取的方法

- 物理攻擊：
  - 偷走你的主機、拔掉你的硬碟、完蛋！
  - 利用開機程序，進入單人維護模式，取得資料！走人～
  - 所以.....只要任何人在您的主機前面，任何事都可能發生；
- 網路攻擊
  - 利用主機原本的核心漏洞：如故事中的駭客軟體、網路上去得的惡意攻擊程式碼等等；
  - 利用 daemons 的漏洞：反正防火牆本來就能夠通過；
  - 利用管理員的疏失：file permission 設計錯誤、網路的濫用、資源分配的不均，以及來不及更新維護的時間點。

主機資料被竊取的方法

- 網路攻擊
  - 主動攻擊
    - client 端主動連接到主機；
    - 利用主機的漏洞或者是 daemon 的服務來連線；
    - 能否使用還與主機的資源有關(file permission, configuration….)
    - 主機通常都會記錄該資訊在登錄檔內！！



主機資料被竊取的方法

- 網路攻擊：
  - 被動攻擊
    - 利用資料在 Internet 上面傳遞時的封包取得；
    - 在 Router 上面 (firewall) 架設監聽軟體 (tcpdump/sniffer)
    - 誘導管理員安裝不知名的軟體；
    - 誘導管理員瀏覽不正常網站；
  - 莫名的問題：
    - 來自內部的破壞(網路的濫用與誤用)；
    - 來自上層的壓力(不合理的要求須知)；
    - 來自離職員工所植入的木馬或者是其他軟體～

主機的保護--物理防護

- 關於機房：
  - 重要資訊重地，不可隨意進出；
- 關於離職員工：
  - 針對其帳號密碼的取捨～
- 關於單一主機的實體保護：(先確定不會被搬走，密碼才有意義)
  - Case 要加鎖；
  - 電源按鈕的保護；
  - BIOS 密碼；
  - 啓動裝置的維護 (硬碟、軟碟、光碟的開機順序！)
  - OS Loader 的密碼保護！

主機的保護--主機資源

- 關於使用者帳號、群組：
  - 系統登入的問題：
    - login
    - PAM (/etc/pam.d/, /etc/security/, /etc/nologin, /etc/securetty)
  - 帳號管理的問題
    - UID與帳號的對應 (爲何不要使用數字類型的帳號？)
    - 使用群組分類，ex>可否使用 su 或 sudo 等重要群組；
    - 多人控管主機的問題： su 還是 sudo ？
    - /etc/shadow 的權限與控管

主機的保護--主機資源（續）

- 關於 filesystem 的保護(基礎中的基礎，重點中的重點)：
  - 檔案系統的掛載參數 (保護 filesystem 的方法之一)：
    - quota,
    - read only
    - no dev
    - no suid/sgid
    - no exec
  - SUID/SGID/SBIT (與執行時的 PID 權限有關啊！)
    - SUID：binary file (program)
    - SGID：較常用在目錄上，與 effective group 有關。
  - file permission
    - user/group/other, Read/Write/eXecute
    - 檔案與目錄的差異 (W 與 X 對目錄的意義)

主機的保護--主機資源（續）

- 關於軟體 (packages) 來源的保護：
  - 軟體來源：
    - rpmfind, sourceforge
    - 各主要 Linux distributions 官方網站
  - 軟體的追蹤檢驗：
    - RPM 套件的 GPG 簽章： *.sign
    - 檔案的指紋資料 md5：md5sum
  - Linux distributions 的選擇：
    - 最新就是最好？
    - 一定要更新到最新的 distributions ？？
  - 套件的更新：
    - apt, yum, up2date, YOU 均可！

主機的保護--主機資源（續）

- 關於登錄檔(日誌資料)與備份的保護：
  - 日誌保護：
    - 控制登錄檔的查詢帳號： file permission (仍須考慮各 daemon 的權限)
    - 利用 logrotate 控制登錄檔的大小，增加效能；
    - 利用隱藏屬性 attr (+a) 亦即 chattr, lsattr 等指令；
    - 設定登錄檔主機，以及使用 printer 來登錄重要資訊(確保資料正確性)。
    - 使用工具直接分析登錄檔內容(方便管理與查詢)；
  - 備份的重要性(利用 tar, dd 等工具)：
    - 原始備份；
    - 完整備份與部分資料備份；
    - 儲存媒體的選擇、保存與可攜帶性；

主機的保護--主機資源（續）

- 關於系統異常的偵測：
  - 異常行爲：
    - 不正常斷線？不正常重新開機？多餘的網路連線？過高的 CPU 使用率
  - 登錄檔的遺失；
  - 檔案權限無預警的變更；
  - 多餘且無法確認的隱藏檔；
  - suid/sgid 檔案的增加；
  - 基本的偵測工具：
    - http://www.rootkit.nl/projects/rootkit_hunter.html
    - http://www.tripwire.com/

主機的保護--網路安全

- 網路服務的概念：
  - 主機透過某種伺服器，亦即啓動某個 binary program 變成 PID 後，以提供網路服務(佔用 socket 啓動 port)；
  - 該網路服務是否能夠讀取主機的資源，與主機的 filesystem 有關 (牽涉到檔案的 owner/group 與 rwx 還有 suid/sgid 等等)
  - 該網路服務本身的設定檔資訊也有相當程度的關連；
  - 如果 program 程式碼寫的不好？
    - 臭蟲 (bugs)
    - 安全漏洞 (security)

主機的保護--網路安全（續）

- 網路安全的第一步：針對主機的資源部分
  - 先確定網路服務所提供的資訊；
  - 該資訊的機密等級；
  - 針對該資訊的機密等級所設定的 permission 是否合宜？
  - 確定讀取者的權限資料；
  - 確定該網路服務 daemon 能夠進行的權限；
  - ex>
    - samba 提供給使用者的資料權限設定？
    - NFS 是否搭配 NIS 提供資料？
    - Apache 提供的資料是否合宜？是否需要保護？是否製作目錄保護？
    - FTP 是否需要提供上傳？上傳資料是否提供下載？
    - .....

主機的保護--網路安全（續）

- 網路安全的第二步：針對主機的 daemon 部分
  - 網路服務程式之漏洞更新、distributions 的核心更新；
    - 利用 apt, yum, you, up2date 等 distributions 提供的資源定時更新；
  - 關閉不需要的 port number ；
    - chkconfig - -level 35 servicename off
    - /etc/init.d/servicename stop
  - 規劃主機提供的服務：
    - 越簡單，越容易找到問題，並設法解決；
    - 越複雜，越容易出問題，而且不容易處理；
  - 利用自我測試，檢查主機與服務的安全：
    - rootkit hunter
    - Nessus 主動式偵測
  - 簡化與安全化 daemon 所提供的服務權限： ex> SSH。

主機的保護--網路安全（續）

- 網路安全的第三步：針對防火牆部分
  - 利用簡單的 tcpwrappers/super daemon 控管
    - /etc/hosts.allow, /etc/hosts.deny
    - 修改 port number (/etc/services) 成爲非正規協定的 port；
  - 利用防火牆控管：
    - Proxy 與 iptables 的利用；
    - iptables 封包過濾的機制與規則訂定；
    - 自我測試與攻擊

主機的保護--網路安全（續）

- 網路安全的第四步：針對區域內網路的物理分級
  - 規範出物理網段的區別：
    - 對較大型企業來說，內部網域不見得是安全的！
    - 最重要的資訊應該獨立出物理網段來處理；
    - 架設區域內部的防火牆系統。
  - 利用非軍事區 (DMZ)
    - 可使用 iptables 配合 SNAT/DNAT 達成內部主機設定；
    - 防火牆維護較爲不易，但主機較爲安全；
  - 查詢與追蹤資訊安全論壇：
    - http://www.cert.org.tw
    - http://www.securityfocus.com/
    - 各主要 distributions 提供的 errata 資訊

資料的保護

- 資料的流通：
  - 透過 TCP/IP 的 router 傳遞資料；
  - 在 switch, hub 上面，亦可接受該封包；
- 資料的加密：
  - 明碼：telnet, ftp….
  - 密碼：SSH, SSL, https…
    - 使用非對稱式金鑰
  - VPN 的建置：
    - 以 IP 隧道讓您的內部 IP 可以在 Internet 上面傳遞；
    - 可以避免大部分的資料外漏問題。

主機的安裝到上線

- 1. 安裝前準備：
  - 準備好硬體，先不要接網路線；
  - 選擇較新的 distributions 來安裝；
  - 事先規劃好未來的主機用途，以決定各個 partition：
    - 選擇是否搭配 NAS, SAN 或者是 RAID 等儲存設備；
    - 是否選擇使用 LVM 等等；
  - 事先搜尋好 yum, apt, you 等主機，以及下載 client 端軟體；
  - 下載 distributions ，並檢查 md5 的資訊，確認無誤後，準備安裝….

主機的安裝到上線（續）

- 2. 開始安裝與 post-install procedure：
  - 依照主機的服務目的、未來規劃，開始進行 partition；
  - 選擇較小安裝的項目，分項選擇所需要的軟體；
    - 通常建議加裝 kernel-source, gcc, make 等軟體維護套件組。
  - 不需要的服務就不要安裝到主機上面；
  - 設定 root 密碼嚴格一些；
  - 若可能，設定 Grub 開機密碼 (各有利弊，自行決定)。
  - 安裝完畢並重新開機後：
    - 使用 netstat 檢查開啓的服務，沒有必要的就關閉；
    - 使用 chkconfig 關閉開機就啓動的服務
      - finger, ftp, imap, pop2, pop3, talk, portmap, telnet, samba, nfs, rsh…
    - 分析系統已安裝的套件，沒有必要的就將他移除～

主機的安裝到上線（續）

- 3. 準備連線與更新套件：
  - 架設基礎防火牆：
    - iptables -F
    - iptables -X
    - iptables -Z
    - iptables -P INPUT DROP
    - iptables -A INPUT -i lo -j ACCEPT
    - iptables -A INPUT -m stat --stat ESTABLISHED,RELATED -j ACCEPT
  - 設定好網路參數 (IP, network, netmask, gateway, dns"/etc/resolve.conf….)
  - 安裝 ATP/YUM client 軟體，並且設定好主機的相關資訊
  - 接上網路線，進行連線測試；
  - 開始進行主機系統的完整 update 更新！

主機的安裝到上線（續）

- 4. 主機的開機密碼與 run level 制訂：
  - 進入 grub shell ，取得 md5 密碼後，進行修改
    - grub

```
grub> md5crypt
Password: *******
Encrypted: $1$84p.91$oJq.ceQm7AttsXZfycXsk/
```

    - vi /boot/grub/menu.lst
      - password --md5 $1$84p.91$oJq.ceQm7AttsXZfycXsk/
  - 修改 run level 相關資訊：
    - vi /etc/inttab
      - id:3:initdefault:
      - #ca::ctrlaltdel:/sbin/shutdown -t 3 -r now
    - init q

主機的安裝到上線（續）

- 5. 主機的帳號管理：
  - 以 PAM 管理 SSH 能登入的帳號：
    - vi /etc/pam.d/sshd

```
auth    required  pam_listfile.so item=user sense=deny \
    file=/etc/sshusers onerr=succeed
```

    - vi /etc/sshusers (內容輸入帳號，一行一個帳號，例如 root)
  - 關閉 root 能登入 ssh 的功能；
    - vi /etc/ssh/sshd_config
      - PermitRootLogin no
    - /etc/init.d/sshd restart
  - 使用 userdel 刪除不必要的系統帳號；
    - 但不可亂刪除～很多系統帳號是必須的！
    - shutdown, uucp, news, halt, operator, games, gohper, rpc…不需要。

主機的安裝到上線（續）

- 5. 主機的帳號管理（續）：
  - 修改使用者自訂密碼的長度：
    - vi /etc/login.defs

      PASS_MIN_LEN 8
  - 設定使用者一登入系統就得要修改他們的密碼：
    - chage -d 0 useraccount

      其實就是修改 /etc/shadow 第三欄位而已！
  - 設定使用者登入的時間 (強制驅離！)
    - vi /etc/profile

      export TMOUT=1800

主機的安裝到上線（續）

- 5. 主機的帳號管理（續）：
  - 身份切換的動作：
    - 禁止使用 su 的帳號： (將該帳號加入 nosu 這個 group 當中！)
      - groupadd nosu
      - vi /etc/group　　#(後面加上不許使用的帳號)
        - nosu:x:512:john,qoo
      - chgrp nosu /bin/su
      - chmod g= /bin/su
  - 僅有屬於 wheel 這個群組的使用者才能夠使用 sudo 的設定：
    - visudo
      - %wheel　ALL=(ALL)　ALL
    - 將某些 user 加入到 wheel 群組當中即可！
  - 使用 sudo 執行 su 的方式
    - sudo su -　　(輸入自己的密碼而非 root 的密碼！)

主機的安裝到上線（續）

- 6. 登錄檔的保護：
  - 將登錄檔加上隱藏屬性 +a 的旗標：
    - chattr +a /var/log/messages …
  - 修改 logrotate 的相關資訊：
    - vi /etc/logrotate.d/syslog
      - /var/log/messages …… (
        - sharedscripts
        - prerotate
        - chattr -a /var/log/messages
        - endscript
        - sharedscripts
        - postrotate
        - chattr +a /var/log/messages
        - ….
        - endscript

主機的安裝到上線（續）

- 7. 檔案系統的保護：
  - 讓純資料用的 partition 去除不必要的 filesystem 參數
    - vi /etc/fstab

      /dev/hda3 /home ext3 defaults,nodev,noexec,nosuid 1 2
    - 常見的掛載點： /tmp, /home 都可以加上上面的參數。
  - 設定讓 RPM 資料庫搜尋可能有問題的檔案 (非 configuration)
    - rpm –V `rpm –qa`
    - 如果出現 binary 有被更動，很需要注意ㄟ！

主機的安裝到上線（續）

- 8. 針對主機提供的服務，啓動防火牆：
  - Kernel 2.4 以後，使用 iptables 封包過濾：
    - 主要以：關閉所有，開放特定爲主！
    - 記得要開放 icmp 某些 type 的封包
    - 信任內部、Internet 則不被信任！
    - 可以加上 TCP Wrappers 來協助處理；
    - 建議製作成 shell script 啓動開機！

主機的安裝到上線（續）

- 9. 針對主機提供的服務，進行備份策略的擬定：
  - 鳥哥的備份策略(主要依據開放的服務來思考)：
    - 主機的基本資料與設定檔：
      - /etc, /home, /var/spool/mail, /usr/local/, /var/log…..
    - 主機提供的各項服務基本路徑：
      - /var/named, /var/www/html, /srv/, /var/lib/mysql…..
    - 備份的週期：
      - 每天備份常態性變動的資料 (/var/lib/mysql)
      - 每週備份一次主機的重要資料(連同 ftp 到鄰近主機作異地備援)
      - 每月一次，將該重要資料複製到隨身硬碟，並燒錄成 DVD 光碟存放。
- 10. 正式上線啦！
  - 註：每件工作，習慣上，我都會記載在自己的工作紀錄檔案內。

本機網路安全的維護

- 網路安全的思考：針對各個服務思考可能的入侵行爲？
  - WWW
    - 是否需要設計 SSL 連線機制？
    - 是否某些 CGI 需要設定保護目錄 (.htaccess)
  - Mail server
    - 是否需要使用 pop3s ？
    - 是否具有 open relay (http://www.ordb.org)
    - 是否需要 webmail 的幫助？
    - 是否需要 SMTP 的身份認證協定之啓動？
  - FTP Server
    - 是否一定需要 FTP 主機？
    - 有沒有更佳的替代方案？ (vsftpd, sftp ….)

本機網路安全的維護（續）

- 網路安全的思考：針對各個服務思考可能的入侵行爲？
  - DNS server
    - 是否需要使用 chroot ？
    - 是否開放 client 端的 transfer ？
    - 設定正確與否？
    - 是否需要完整的資料上傳 (whois 資料庫？)
  - SSH server
    - 是否開放 root 身份登入？
    - 是否對整個 Internet 開放？
    - 可否配合 DDNS 或者其他動作制訂相關 IP 取得給予登入？

網際網路傳送資料

- 較危險服務：
  - 一些明碼的服務，建議更換：
    - telnet, ftp, pop3.....
- 將物理網段切割清楚：
  - 內部則爲信任區域；
  - 外部則不爲信任區域；
- 使用更安全機制：
  - 利用 VPN 傳送資料！
  - 多以 SSL 機制 (ssh, https) 進行重要資料傳遞！
  - 設定良好的防火牆與路由規則！

末端分析的重要性

- 使用登錄檔分析軟體：
  - Logwatch (Red Hat 系統的預設分析資料)
  - Logfile.sh (鳥站提供的簡易分析軟體)
  - 各個相關服務所提供的登錄檔分析軟體
    - Proxy： sarg
    - Apache： awstat
- 使用入侵偵測：
  - Rkhunter：
    - http://www.rootkit.nl/projects/rootkit_hunter.html
  - 直接搜尋系統資訊：
    - Tripwire
    - Findsuid.sh (鳥站提供)

管理員建議

- 應製作標準操作程序，方便萬一你不在座位上的時候……
- 應多學習、查閱 script ，建立主機的自動化維護動作；
- 應隨時做好教育訓練；
- 應隨時查閱最新的 security 資訊；
- 應隨時主動攻擊自己的機器；
- 應具有高標準的道德觀，與老闆的溝通管道應暢通；
- 平時的生活：
  - 到處參加研討會；
  - 到處查閱論壇最新資訊；
  - 隨時主動對內部員工發佈最新病毒、木馬、更新資訊等 email 訊息；
  - 最好是天天喝茶看報紙！

主要參考資料

- 網路安全百寶箱；
- http://www.study-area.org/tips/security.txt
- 酷學園討論區
- 鳥站討論區
- MOTO討論區