

財團法人國家實驗研究院國家地震工程研究中心
資訊安全管理制度維護服務案
組織全員資訊安全認知及法令宣導

講師：NII產業發展協進會 邱瑩青
日期：2010/5/31

大綱

- 與您相關的資訊安全
- 您的駭客威脅
- 個人資訊安全須知
- 資訊安全工具
- 資訊安全案例
- 結語

Page • 2

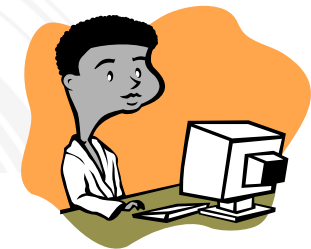
■ 與您相關的資訊安全

- 您的駭客威脅
- 個人資訊安全須知
- 資訊安全工具
- 資訊安全案例
- 結語

Page • 3



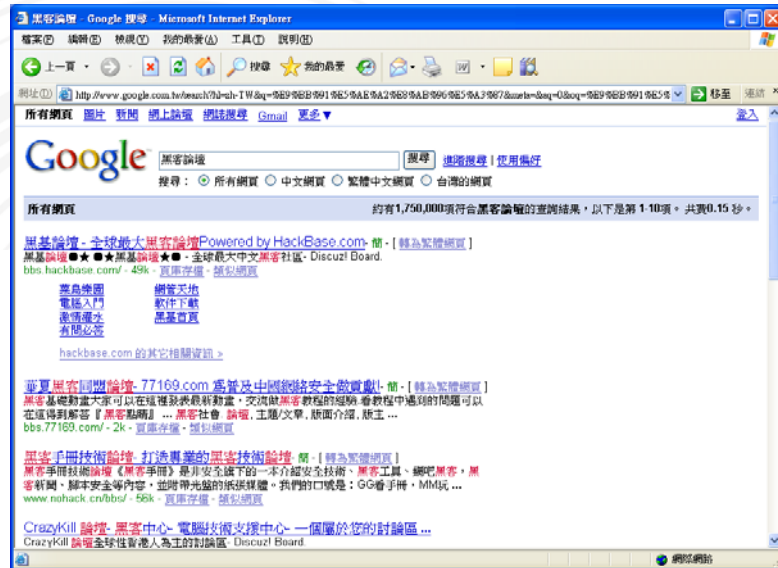
專業駭客
特定目標



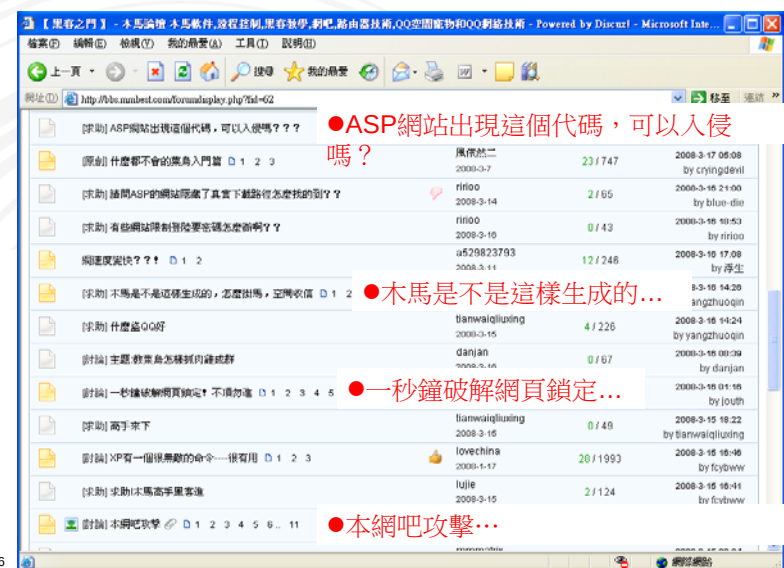
一般使用者
亂槍打鳥

Page • 4

透過網路駭客論壇就可以找到駭客工具和教學

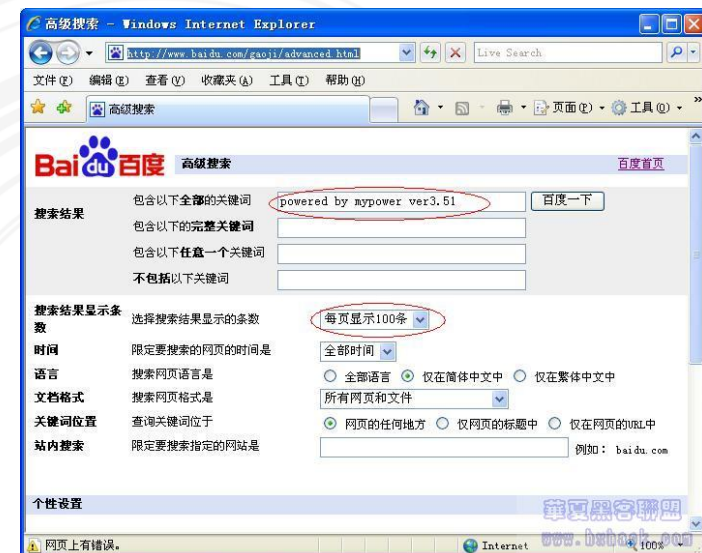


各種詳細的駭客入門教學



某網頁撰寫工具被發現有一個系統漏洞，
有駭客撰寫了一個工具
可以透過這個系統漏洞進行入侵，
並將工具放在網路上...

入侵網站後端範例



選擇目標



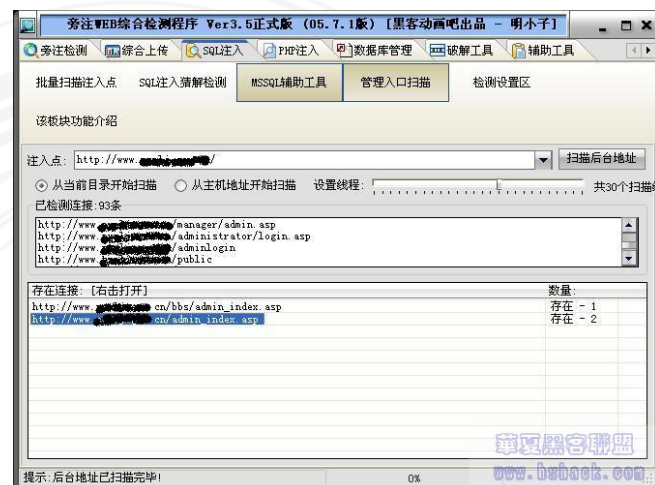
Page • 9

使用駭客工具破解得到帳號密碼...



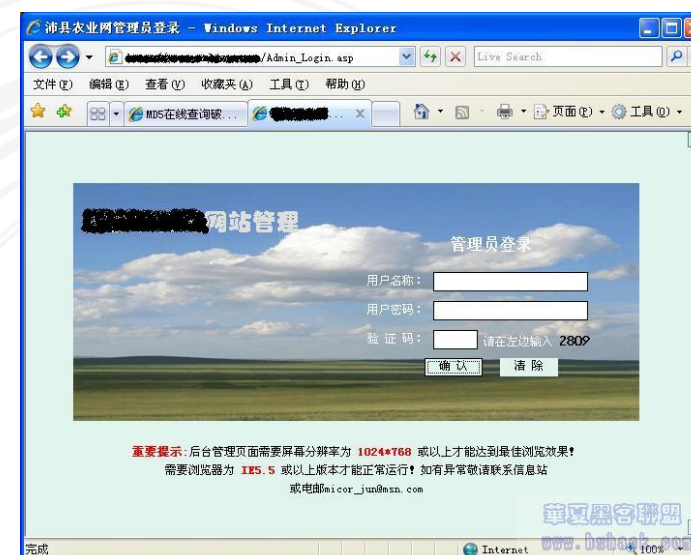
Page • 10

用駭客工具猜測網站後端網址



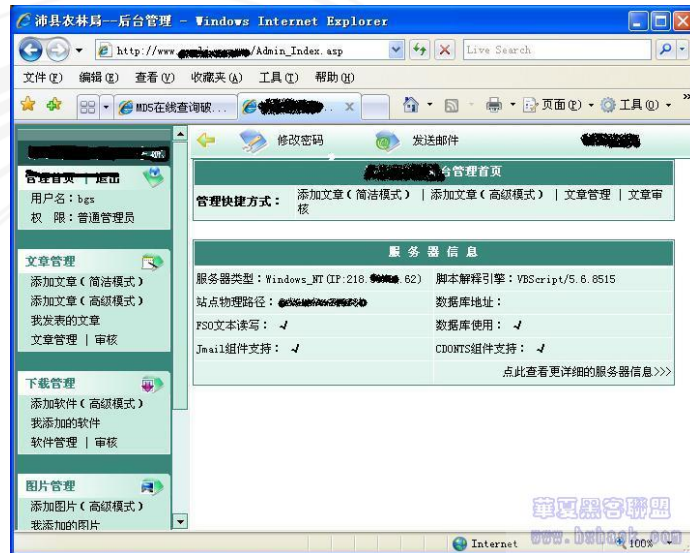
Page • 11

得到網站後端網址



Page • 12

輸入帳號密碼，進入了網站後端系統~



Page • 13

所以，不要覺得您不會是駭客的目標~
這些玩家駭客並沒有特定目標，
只要是系統有漏洞、疏於防護的，
可能就是他的目標！！

Page • 14

- 與您相關的資訊安全
- 您的駭客威脅
- 個人資訊安全須知
- 資訊安全工具
- 資訊安全案例
- 結語

Page • 15

媒體報導「駭客入侵拍女子裸照」

- 駭客以木馬程式植入他人電腦，再遠端開啟女子電腦上的攝影機...



Page • 16

http://v.youku.com/v_playlist/f346901p4.html

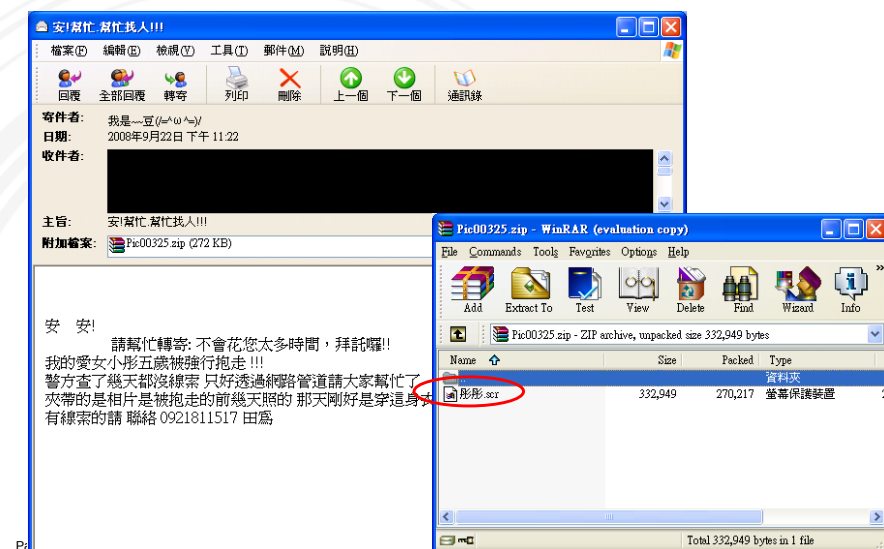
CCTV曝光網路黑客驚人內幕

(20'26)

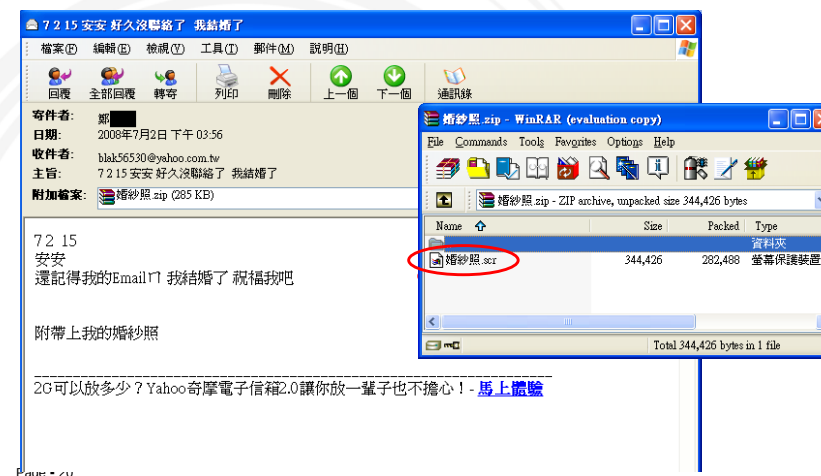
「社交工程」，就是詐騙！
透過電子郵件等方式偽裝身份
誘騙您上勾受騙…

假冒的身份；友善、誘惑的內容…

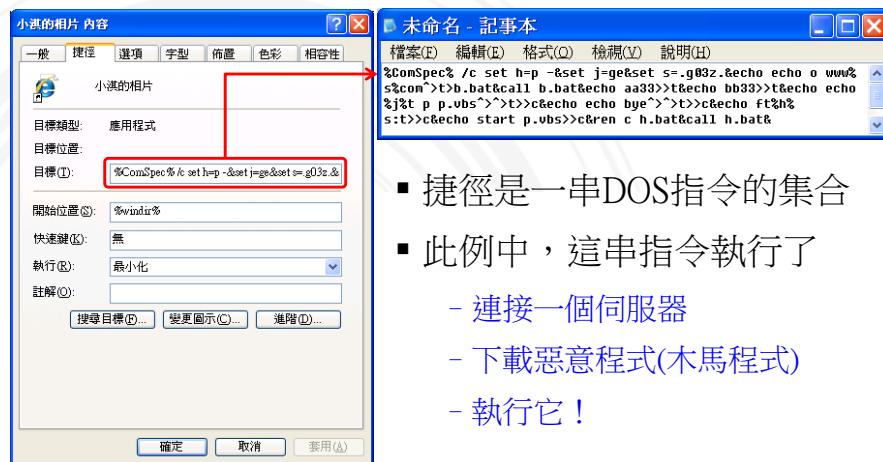
很多人真的會熱心地開啟觀看和轉寄



朋友說他結婚了，
但您有查覺這是惡意程式詐騙郵件嗎



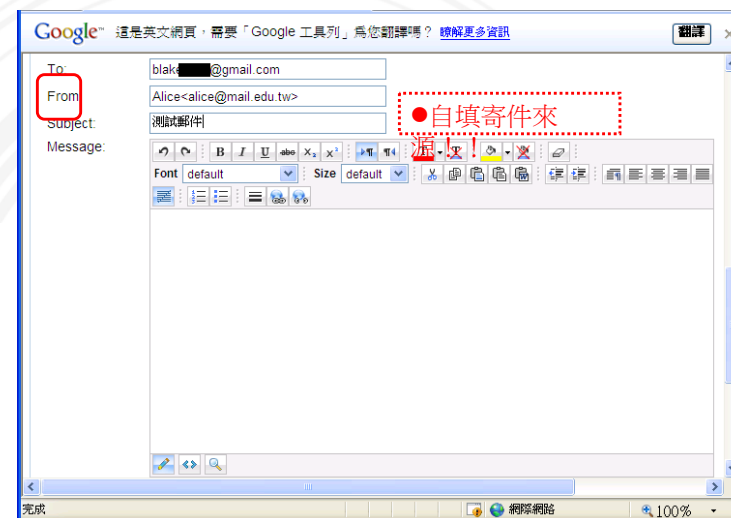
「捷徑」攻擊技倆解析



- 捷徑是一串DOS指令的集合
- 此例中，這串指令執行了
 - 連接一個伺服器
 - 下載惡意程式(木馬程式)
 - 執行它！

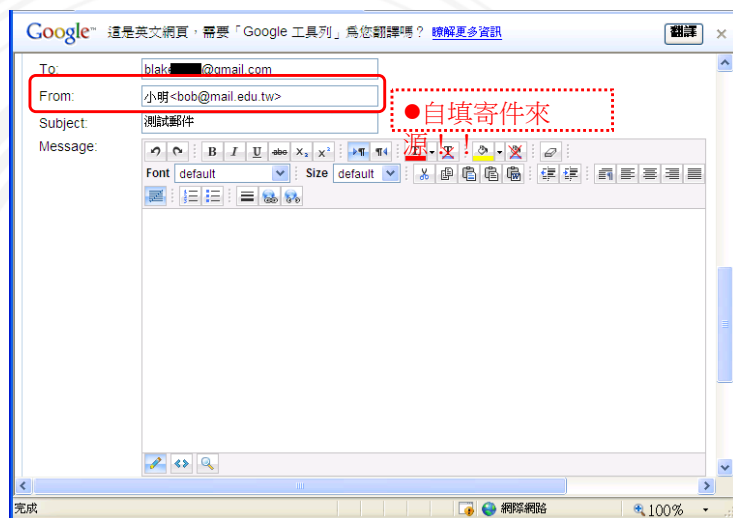
Page • 21

偽冒身份的電子郵件(1)

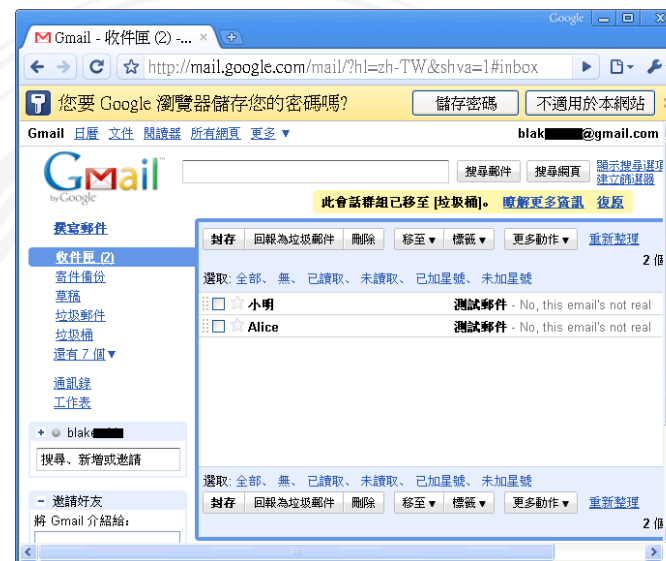


Page • 22

偽冒身份的電子郵件(2)



Page • 23



Page • 24

政府社交工程演練電子郵件範例

■ 郵件主題

- 政治新聞
- 影劇新聞
- 情色主旨
- 休閒娛樂

■ 郵件類型

- 惡意網頁連結
- 惡意Word檔

演練電子郵件(政治新聞)



演練電子郵件(影劇新聞)



演練電子郵件(情色主旨)

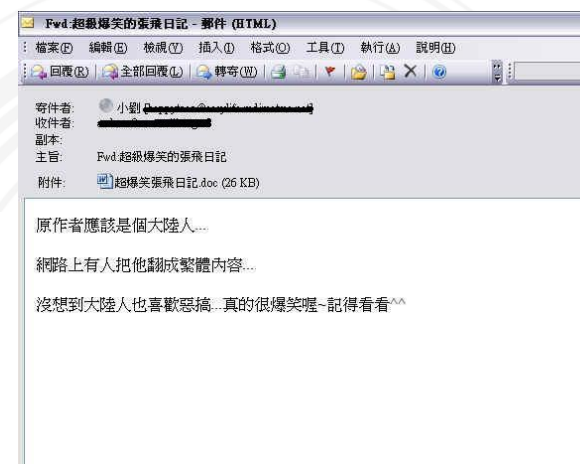


演練電子郵件(休閒娛樂)



Page • 29

演練電子郵件(休閒娛樂)



Page • 30

<http://www.youtube.com/watch?v=urE8KCT6Shk&feature=related>

寄發匿名及偽造的E-Mail點選中木馬
(4'17)

Page • 31

<http://www.youtube.com/watch#!v=AHA4fxaOSvQ&feature=related>

將影片檔嵌入呼叫網頁木馬的事件
(3'59)

Page • 32

<http://www.youtube.com/watch#!v=FZXCBAnpVqA&feature=related>

將不同種類的程式與木馬網綁

(7'53)

除非您瞭解電子郵件附檔的來源、
您知道會收到該附檔，否則請勿開啟

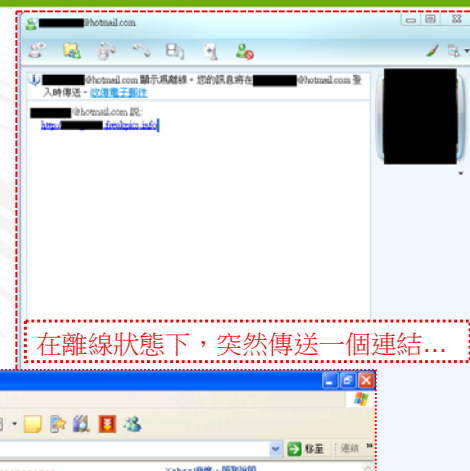
如果電子郵件來自不知名人士，
請勿因為好奇心隨意開啟郵件和附檔

<http://www.youtube.com/watch?v=zA-H0BXdmx0>

電子郵件社交工程宣導影片

(4'40)

- 釣魚網站
- 即時通傳送惡意連結



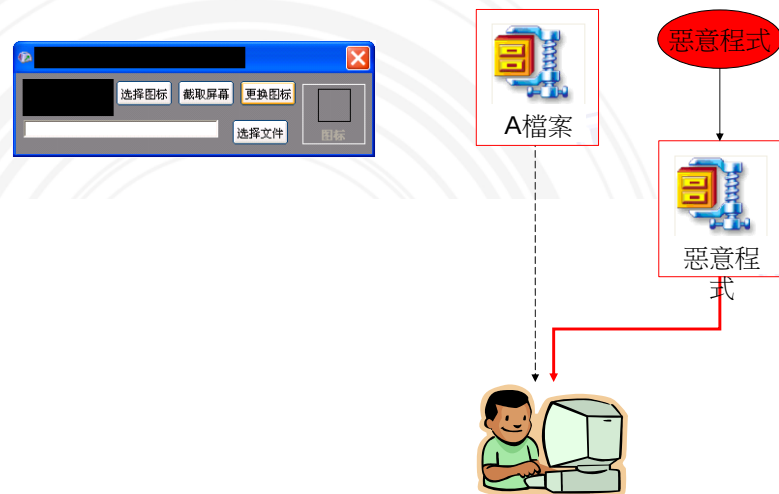
在離線狀態下，突然傳送一個連結...



<http://yahooo.c65.163ns.com/data/bak/>

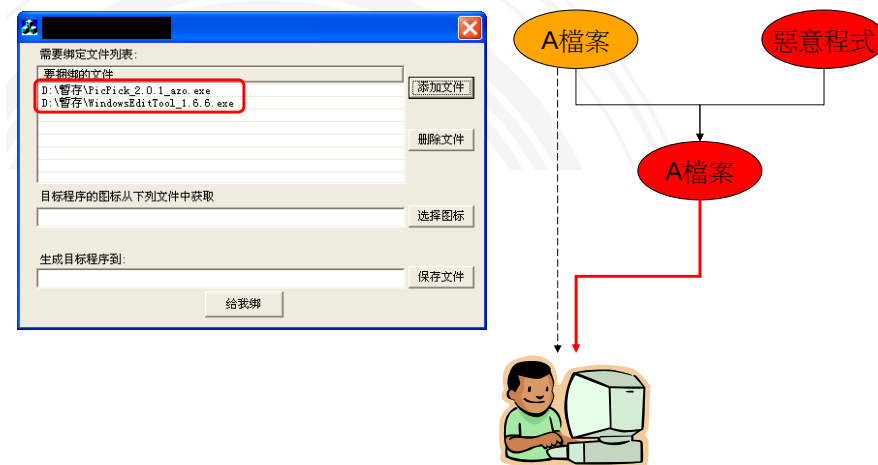
工具軟體嵌入惡意程式 (1/2)

惡意程式偽裝技倆解析 - 變更檔案圖示



工具軟體嵌入惡意程式 (2/2)

惡意程式偽裝技倆解析 - 合併檔案



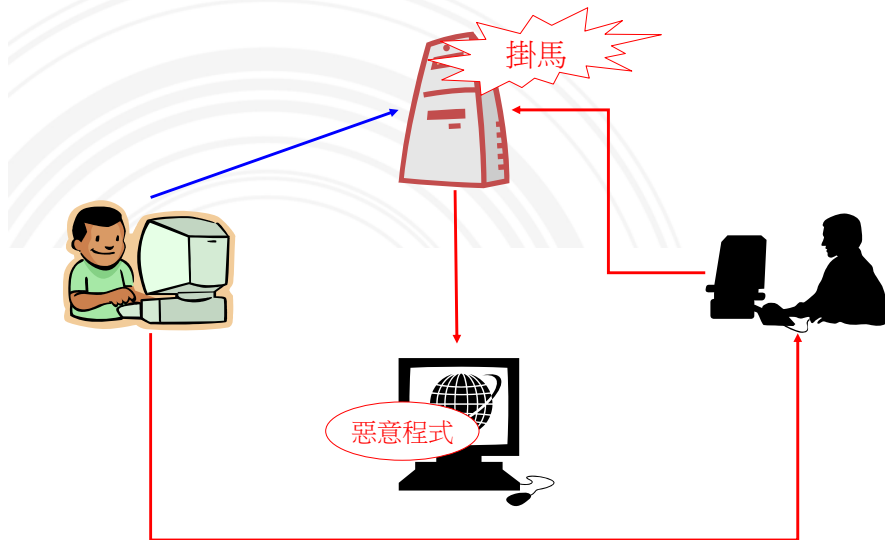
無名小站XSS攻擊事件～

在使用者瀏覽被植入惡意程式碼的頁面時，
資料會被竊取！

網路釣魚與網頁掛馬的差別

- **釣魚網頁**是設置一個以假亂真的網站，欺騙網路瀏覽
者上當
- **網頁掛馬**則是攻擊一個正常的網站，讓使用者在瀏覽
網站時連接到駭客的惡意程式網站

網頁掛馬攻擊模式



Page • 41

最新被掛馬網站

TW 網站滲陷資料庫 | 資安之眼 - Windows Internet Explorer

http://www.itis.tw/compromised

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

Google 搜尋 網頁註解 登入

TW 網站滲陷資料庫 | 資安之眼

事件	日期	主機	站名/抬頭	來源	作業系統	D
	2009-12-27	www.ifin.net.tw	網際焦點	Zone-h	Linux	2
	2009-12-27	service-learning.ncu.edu.tw	中央大學服務學習網	Zone-h	Win 2003	
	2009-12-27	osa-13.adm.ncu.edu.tw	中央大學服務學習網	Zone-h	Win 2003	
	2009-12-27	www.azoo.com.tw	AZOO水族網	PhishTank		
	2009-12-26	www.fords.idv.tw	海騰網頁設計工作室	Turkey-h		
	2009-12-25	www.rst.tw	伸鴻股份有限公司	Turk-h	4	
	2009-12-25	nurse.cgu.edu.tw	長庚護理	Turk-h	4	
	2009-12-23	necoast.cru.com.tw	東北角山海之戀	Turk-h		
	2009-12-22	www.tpce.org.tw	台北市土木技師公會	Zone-h_CN	7	
	2009-12-22	nurse.cgu.edu.tw	長庚護理	Turk-h	7	

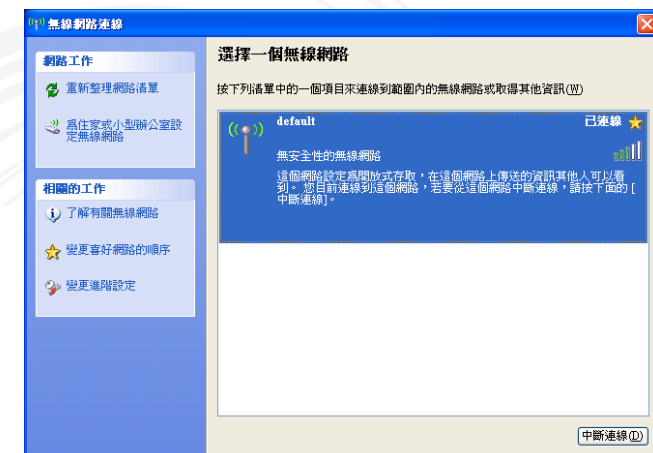
網路網路 100%

Page • 42

- 與您相關的資訊安全
- 您的駭客威脅
- 個人資訊安全須知
- 資訊安全工具
- 資訊安全案例
- 結語

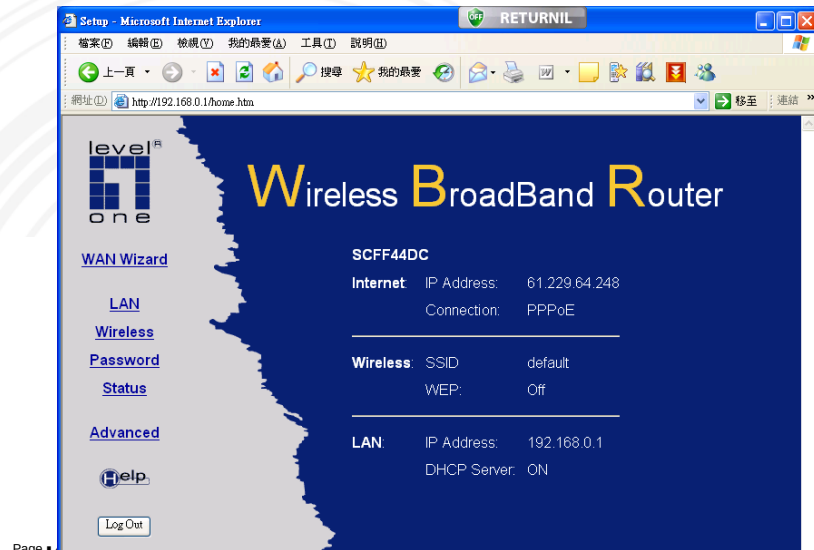
Page • 43

沒有加密無線網路...



Page • 44

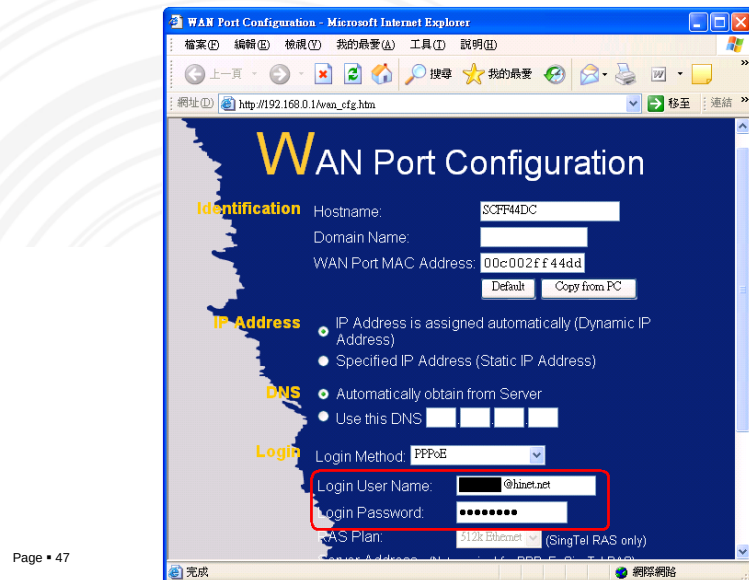
嘗試連線基地台...



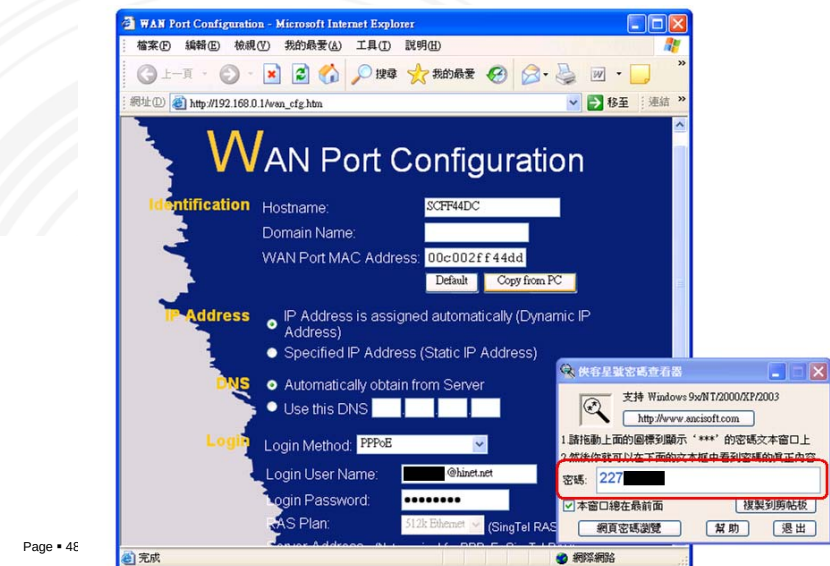
沒有設定基地台密碼...



Configuration頁面



破解得到連線密碼...



駭客入侵無線網路的問題

- 內部網路安全問題
 - 駭客與您的電腦處於同一區域網路，可能利用資源共享進行攻擊
- 外部網路安全問題
 - 駭客進行犯罪，基地台擁有者成了代罪羔羊

Page • 49

無線網路防護(一)

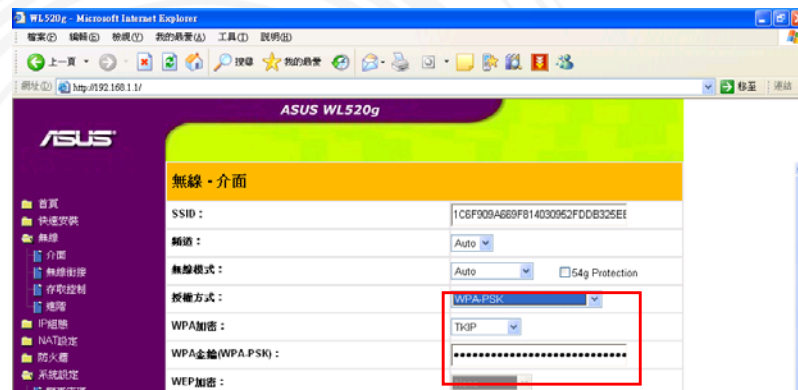
- 設定基地台管理密碼
 - 預設值常是admin/1234
 - 修改無線基地台的預設登入帳號密碼



Page • 50

無線網路防護(二)

- 設定WPA2加密傳輸



Page • 51

無線網路防護(三)

- 鎖定網路卡MAC位址
 - 所有網路卡都有唯一ID，稱為MAC
 - 設定允許連線的MAC位址



Page • 52

查詢網路卡MAC...

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Blake>IPCONFIG /ALL

Windows IP Configuration

Host Name . . . . . : NB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter 區域連線:

Media State . . . . . : Media disconnected
Description . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
Physical Address. . . . . : 00-13-D4-67-A3-B6

Ethernet adapter 無線網路連線:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/Wireless 2200BG Network Connection
Physical Address. . . . . : 00-12-F0-9C-0C-6D
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
Lease Obtained. . . . . : 2007年10月23日 上午 10:06:44
Lease Expires . . . . . : 2007年10月24日 上午 10:06:44

C:\Documents and Settings\Blake>
```

無線網路安全注意事項

- 修改無線基地台的預設帳號密碼
- 使用WPA2 連線加密 / 鎖定網路卡MAC
 - 多一層防護多一層入侵的障礙
- 啟用日誌 (Log)，定期查看

不明來源的
沒有加密無線網路，
亦可能是駭客的陷阱...

沒加密的公用無線網路，
避免使用登入帳號密碼
的服務！

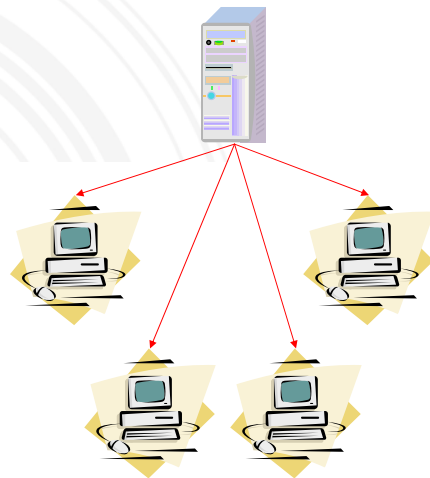
常見的P2P程式

- 即時通訊軟體
- eDonkey
- eMule
- Foxy
- BitTorrent / BitComet
- Clubbox / GOGOBOX
- Kuro / ezPeer

分享加速式檔案下載

傳統伺服器下載

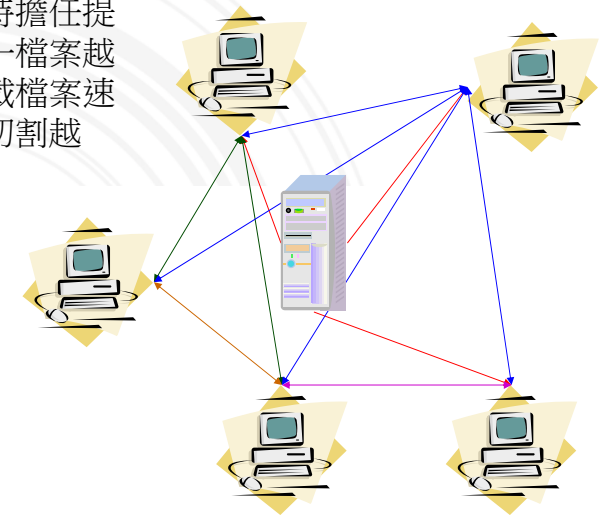
- 使用者由伺服器下載檔案，多使用者同時下載檔案時會因頻寬分用，下載檔案速度會變慢



Page • 57

P2P網路下載

- 每一個使用者同時擔任提供檔案角色，某一檔案越多的人下載時，下載檔案速度會因檔案分段切割越多，速度越快



Page • 58

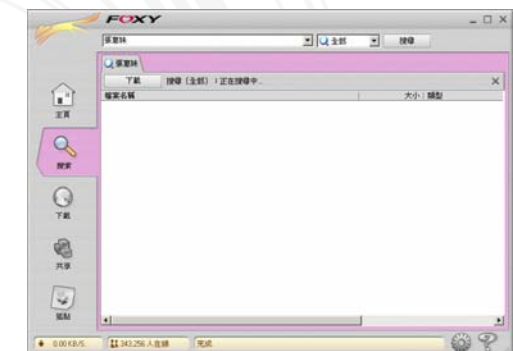
使用P2P軟體可能衍生的問題

- 任意使用各種P2P軟體下載盜版軟體、電影與音樂等
- 使用不當造成電腦內資料外洩
- P2P網路上散播的惡意程式造成電腦中毒
- 佔用區域網路連外頻寬

Page • 59

關於Foxy

- 該軟體在分享資料夾的設定上容易讓使用者誤設為整台電腦全部分享
- 該軟體亦容易被植入木馬，資料外洩情況最嚴重



Page • 60

Foxy資料外洩事件

- 2007年4月，警察機關因員警違規使用P2P分享軟體，導致內部筆錄外洩
- 在新聞熱潮下，部分以「刑案筆錄」等文字為檔名的假檔案藉機散播

→ 檔名與實際內容不符的假檔案在P2P網路上相當常見

2010年，美國《紐約時報》一篇報導指出，
網路安全公司Imperva公布了一份統計資料，
分析了被駭客入侵竊取的某網站會員帳號密碼，
在三千兩百萬個密碼中，

最多使用者使用的密碼是「123456」，
有高達1%的會員使用！

• 第二至十名

- 2)12345
- 3)123456789
- 4)password
- 5)iloveyou
- 6)princess
- 7)rockyou
- 8)1234567
- 9)12345678
- 10)abc123

• 第十一至二十名

- 11)nicole
- 12)daniel
- 13)babygirl
- 14)monkey
- 15)jessica
- 16)lovely
- 17)michael
- 18)ashley
- 19)654321
- 20)qwerty

這些容易記憶的簡單數字密碼，就是「**懶人密碼**」

雖然方便記憶，卻也容易遭駭客破解！

常見的懶人密碼除了簡單數字外，還包括：

- 1)自己的英文名、生日、電話等個人資料
- 2)與帳號相同
- 3)簡單的連續英文字元，例如aaaa
- 4)簡單的英文字元加數字，例如abc123
- 5)電腦鍵盤上的連續字元，例如asdf、qwerty
- 6)單字或簡單詞語，例如上述的password與iloveyou

正確的密碼設定

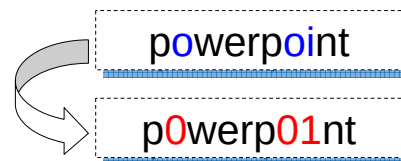
- 1) 不使用個人資料
- 2) 不使用有意義的單字
- 3) 結合大小寫英文、數字和特殊符號

越長的密碼長度當然亦越難被破解，
建議密碼最少為八個字元。
包括大小寫英文、數字和特殊符號的
八個字元以上密碼，
即稱為「強式密碼」

如何設定一個容易記憶的強式密碼，
這裡介紹一個最簡單的小技巧，
叫做「替換」。

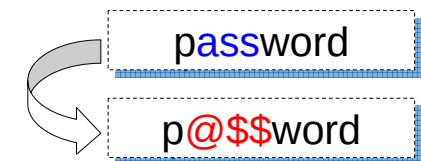
替換(一)

- 1) 選擇一個單字，例如「powerpoint」
- 2) 設計替換原則，例如：
英文「o」→數字「0」
英文「i」→數字「1」
- 3) 產生出結合英文和數字的密碼



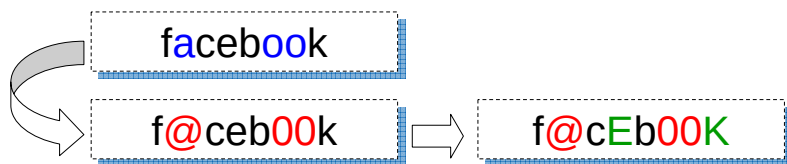
替換(二)

- 1) 選擇一個單字，例如「password」
- 2) 設計替換原則，例如：
英文「a」→符號「@」
英文「s」→符號「\$」
- 3) 產生出結合英文和符號的密碼



替換(三)

- 1) 選擇一個單字，例如「facebook」
- 2) 設計替換原則，例如：
英文「o」→數字「0」
英文「a」→符號「@」
- 3) 將偶位數的小寫英文字元→大寫英文字元
- 4) 產生包括大小寫英文、數字和符號的強式密碼



Page • 69

不要只用一組密碼，
至少使用兩至三組密碼，

可設定不同重要群組的使用密碼，例如：

- 1)低重要性群組的密碼：論壇、網站會員…
- 2)中重要性群組的密碼：郵件、網路空間…
- 3)高重要性群組的密碼：網路銀行…

Page • 70

- 與您相關的資訊安全
- 您的駭客威脅
- 個人資訊安全須知
- 資訊安全工具
- 資訊安全案例
- 結語

Page • 71

監控網路連線工具

- TCPView
 - 監控電腦上各個通訊埠連線情況
 - <http://download.sysinternals.com/Files/TcpView.zip>

Page • 72

工具管理員軟體

- Process Explorer

- 監控系統內正在運行的各個執行程序
- <http://download.sysinternals.com/Files/ProcessExplorer.zip>

免費的磁碟 / 資料加密軟體

- TrueCrypt

- 在硬碟上新增一個加密磁區，使用時只需將要加密的檔案移入
- 綠色軟體
- <http://www.truecrypt.org/downloads.php>

- 與您相關的資訊安全
- 您的駭客威脅
- 個人資訊安全須知
- 資訊安全工具
- 資訊安全案例
- 結語

ICO國際著作權機構事件

- 之前在PTT上有人爆料，在日本有一個叫作「ICO」(International Copyright Organization)的網站，竊取並公佈了大量電腦使用者的個人資料，其中包括了許多台灣的玩家。
- 這些人的資料之所以遭竊取公佈，是因為安裝某些盜版遊戲軟體

- 不應違法使用盜版軟體
- 不隨意由網路論壇、不明網站等下載軟體，軟體之下載最好由官方網站下載
- 網路上的免費軟體、共享軟體，可能附帶廣告軟體，或隱藏惡意人士之陷阱，最好清楚安全無虞方可使用
- 不管是安裝任何軟體，皆應確實閱覽「授權使用同意書」，確認無損害隱私權益之情況；如有疑慮，即應取消安裝
- 軟體安裝過程中預設附加之其他程式、工具列等，應仔細查看到底是什麼程式；非必要或有廣告軟體等疑慮之程式，請取消其安裝勾選，千萬不可只是盲目地按「下一步」鍵完成安裝

- 與您相關的資訊安全
- 您的駭客威脅
- 個人資訊安全須知
- 資訊安全工具
- 資訊安全案例
- 結語

Page • 78

資訊安全須融入日常生活方能久遠維護
觀念認知 → 習慣養成

簡報完畢，敬請指教！

姓 名：邱瑩青
e-mail：blake@nii.org.tw
電 話：(02)25082353-110
NII產業發展協進會