

今天打卡了嗎？手機上 網安全嗎？

行動設備攻防實錄

Benny

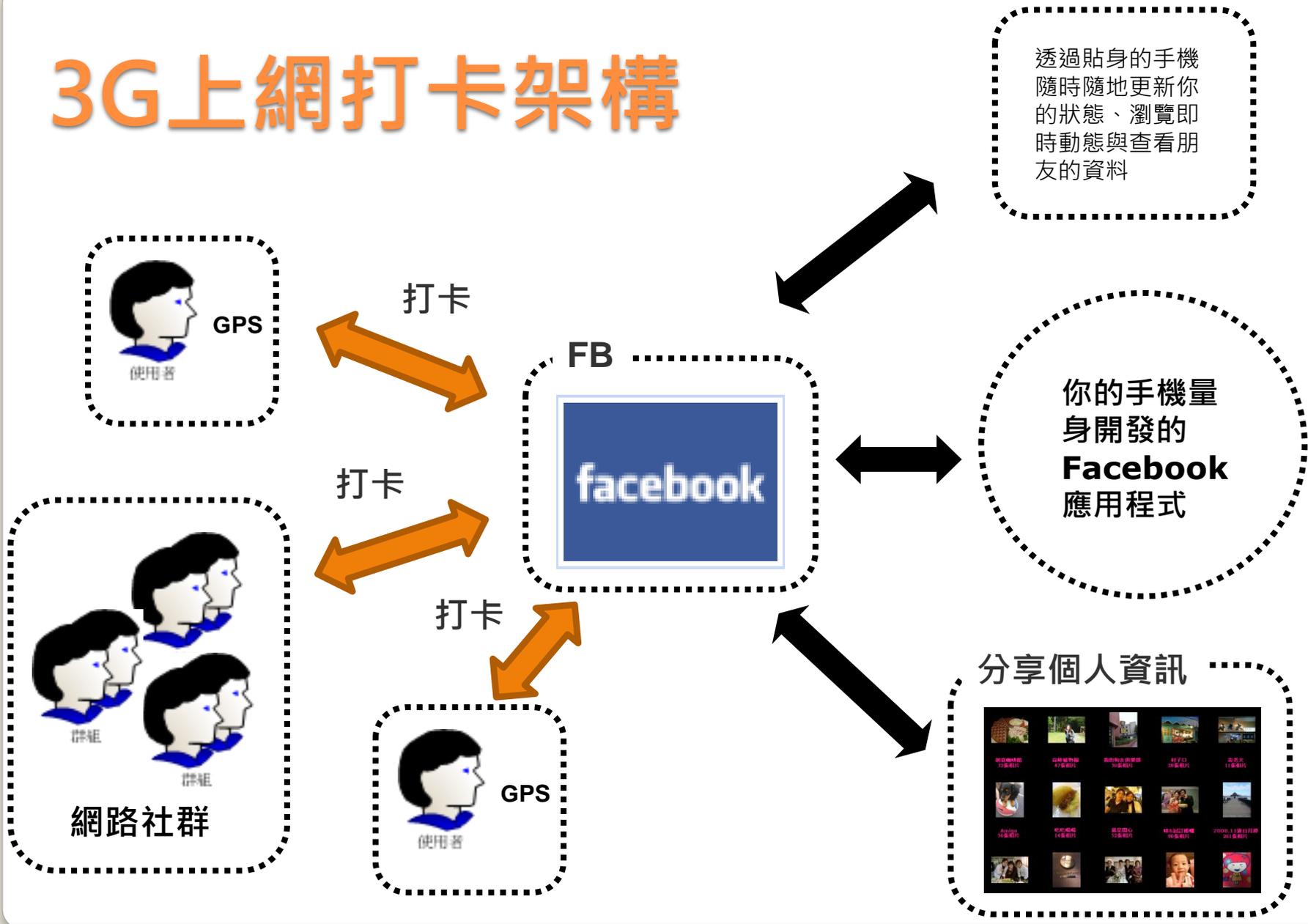
大綱

- 入侵網站伺服器實務(3G行動上網)
 - 隨時動動手指即拿下網站 (滑鼠版 & 手機版)
 - 人際互動安全問題 – 社交工程手法
 - 躲貓貓入侵攻擊(行動設備)
- 手機分享你的個人隱私資訊
 - 手機打卡留下什麼蛛絲馬跡
 - 利用網路人肉搜尋 (GPS定位追蹤)
 - 手機入侵手機實錄



手機上網安全問題

3G上網打卡架構





目前流行趨勢是什麼????

10大新聞

cti 中天新聞

- 珍檢心臟血管最嚴重
- 中監拒收扁嫂責付兒
- 女扒手傘戳孩趁機偷
- 肩痛灸腎病患控性侵
- 首創！行李遲到賠客

主播 張心宇

月19日週六

25H



no1speed2002, 您好!
會員登出 | 帳號資料

新聞 網頁

Search bar with magnifying glass icon and 搜尋 button

新聞首頁 政治 社會 地方 國際 財經 科技 運動 健康 教育 藝文 影劇 旅遊 生活 影音新聞

資訊3C 科學發展 自然環境 照片故事 專輯 民調中心 雜誌 網路趨勢 新版體驗 瘋電玩

2011/08/08(星期一) 農曆(辛卯)七月初九日

新聞首頁 > 科技 > 資訊3C > 聯合

寄給朋友 | 友善列印 | 字級設定: 小 中 大 巨 | 分享

拍照就知道個資 恐侵犯隱私



更新日期: 2011/08/08 10:05 編譯賴美君 / 綜合外電

想像自己坐在酒吧，只要對著人們拍照，很快就能得知他們的身分、居住地點、喜歡的音樂類型，甚至社會安全號碼。

或者瀏覽約會網站，光看照片就能得知大家的身分。這種科技相當駭人，

Google 曾經研發出來，但隨即選擇放棄，因為前執行長史密特 (Eric Schmidt) 認為問世的危險性過高。

卡內基梅隆大學教授阿奎斯蒂 (Alessandro Acquisti) 在拉斯維加斯的黑帽駭客會議 (Black Hat) 表示，這種科技銳不可擋。

阿奎斯蒂運用現成的臉部辨識軟體與簡單的網路資料探勘技術，證明只要透過臉部照片，就可以查出大多數人的身分，而且誰都辦得到。

換句話說，人臉成了身分標幟，在每目動輒有數十億張照片流傳網路的世

廣告

100年免費電腦培訓課程

名額有限，立即洽詢!!

3DMax動畫設計班	0元
建築室內設計CAD班	
Office全能整合班	
Dreamweaver動態網頁設計班	
Photoshop平面設計班	

我要申請 · 免費課程

快加入國軍的行列



Y! 民調中心

時事投票

前期投票

台股跌不停，你認為政府應該如何因應？



A Division of Cisco Systems, Inc.

Wireless

Wireless-G

Setup Wireless Security Re

Basic Wireless Settings | Wireless Security

Wireless Network

Wireless Network Mode:

Wireless Network Name (SSID):

Wireless Channel:

Wireless SSID Broadcast: Enable Dis


Status: SES Inactiv

Upgrade Network Scanner

Hosts in Scan
4 minutes ago Network: Free Public WiFi

 **192.168.1.1**
Cisco-Linksys LLC
192.168.1.1

 **iPhone-2**
Apple, Inc.
192.168.1.118

 **William 的 iPhone**
Apple, Inc.
192.168.1.120

 **192.168.1.122**
Apple, Inc.
192.168.1.122

 **Carrie-Wong-mato-iPhone**
Apple, Inc.
192.168.1.123

 **Leung-Cheuk-Lum**
Apple, Inc.
192.168.1.124

Internet 共享

群組 所有聯絡資訊 +

13 劃

- 1 ●
- 4 ●
- 7 ●
- 10 ●
- 13 ●
- 16 ●
- 19 ●
- A ●
- E ●

14 劃

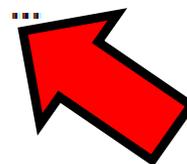
- I ●
- M ●
- R ●
- V ●
- Z ●
- # ●

[歡迎來到Facebook](#) ☆

Facebook 是一個聯繫朋友、工作伙伴、同學或其它社交圈之間的社交工具。你可以利用Facebook 與朋友保持密切聯絡，無限量地上傳相片，分享轉貼連結及影片，還可以幫助你 ...

[中文\(香港\)](#) - [忘記密碼](#) - [Find Friends](#)

[zh-tw.facebook.com/](#) - [頁庫存檔](#) - [類似內容](#)



社交網路平台 (FaceBook)

Demo

Facebook_ClickJacking (聲東擊西 ~ ~ 看馬非馬)



聲東擊西 似真非真的 ClickJacking連結(範例)

新訊息!

收件人: 魯明明 ×

主旨: 台中警紀崩盤/角頭賭場 刑警1把1萬底(YAHOO新聞)

訊息: YAHOO新聞

連結 ×

<http://news.pchome.com.tw/society/libertytimes/20100> 附件

傳送 取消

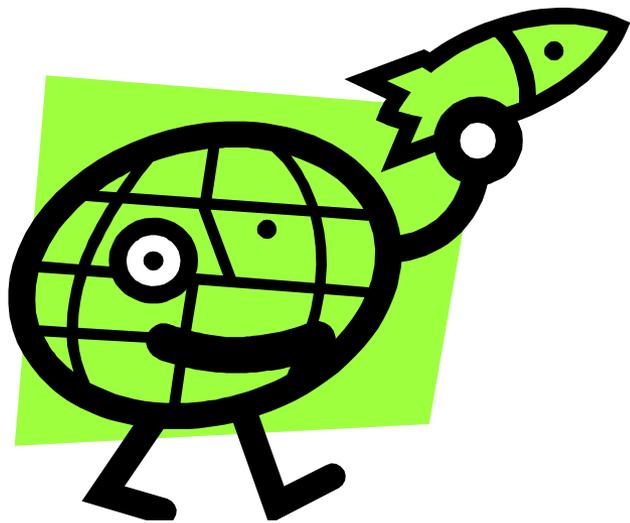
選擇: 全部, 已閱讀, 無



你
6月18日 12:02

台中警紀崩盤/角頭賭場 刑警1把1萬底(YAHOO新聞)
YAHOO新聞

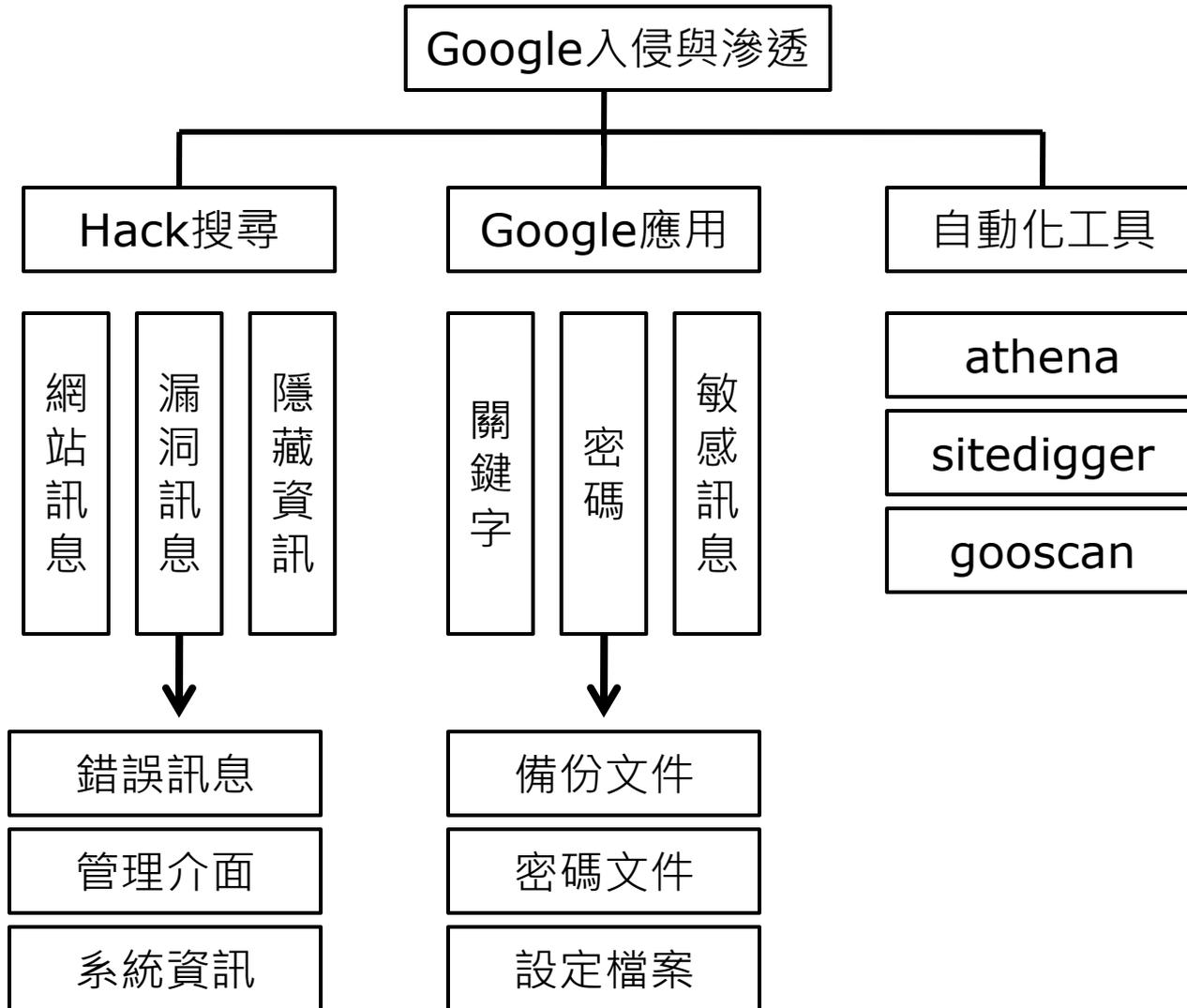
系統入侵實錄



系統入侵實務-滑鼠版

- 入侵環境條件：
網站同意Google機器人造訪你的網站!!
主機檔案及目錄設定不良

Google入侵拓撲圖



基本語法與關鍵字

- site: (搜尋特定網址)
- inurl: (搜尋特定連結)
- intext: (搜尋網頁內文字)
- intitle: (搜尋網頁標題)
- filetype: (搜尋特定檔案格式)
- link: (搜尋互相連結的網頁)
- "index of" (搜尋開放目錄瀏覽)
- cache: (顯示網頁在google中的暫存資料)

進階語法與關鍵字

- "access denied for user" "using password"
- "Index of /backup"
- allinurl: admin mdb
- inurl:passlist.txt
- " -FrontPage-" ext:pwd inurl:(service | authors | administrators | users)
- "ASP.NET_SessionId" "data source="
- "AutoCreate=TRUE password=*"
- "Index of /" +password.txt
- "Index of /password"
- "mysql dump" filetype:sql
- "pcANYWHERE EXPRESS Java Client"
- "VNC Desktop" inurl:5800
- "phpMyAdmin MySQL-Dump" "INSERT INTO" -"the"
- "phpMyAdminMySQL-Dump" filetype:txt
- "phpMyAdmin" "running on" inurl:"main.php"
- "robots.txt" "Disallow:" filetype:txt
- intitle:"Remote Desktop Web Connection" inurl:tsweb
- intitle:"Welcome to Windows 2000 Internet Services"
- inurl:"printer/main.html" intext:"settings"
- intitle:index.of administrators.pwd



進階搜尋

[搜尋說明](#) | [Google 完全手冊](#)

查詢

包含全部的字詞

10 項結果

Google 搜尋

包含完整的字句

包含任何一個字詞

不包括指定字詞

語言

查詢網頁語言是

任何語言

區域

尋找網頁位於：

任何地區

檔案類型

只在 尋找指定的檔案類型

所有的檔案類型

日期

傳回下列時間內所檢視的網頁：

字詞位置

查詢字詞位於網頁的

網域

只在 以下的網址或網域

使用權

傳回以下結果

安全搜尋

 未篩選
 使用 [「安全搜尋」](#) 過濾查詢結果。

所有的檔案類型

Adobe Acrobat PDF (.pdf)

Adobe Postscript (.ps)

Autodesk DWF (.dwf)

Google 地球 KML (.kml)

Google 地球 KMZ (.kmz)

Microsoft Excel (.xls)

Microsoft Powerpoint (.ppt)

Microsoft Word (.doc)

RTF 格式

Shockwave Flash (.swf)

搜尋特定網頁

類似網頁

搜尋類似以下網址的網頁

搜尋

例如：www.google.com/help.html

Demo

Google 實務應用

1. 滑鼠點擊入侵
2. 進階變化入侵





加入 Google 智慧型搜尋框

Google 開始

下載 Google 工具列

Google 搜尋 好手氣

進階搜尋
使用偏好
語言選項

- 所有網頁
- 中文網頁
- 繁體中文網頁
- 台灣的網頁

傳統首頁 | [iGoogle: 台灣首頁](#)

[廣告服務](#) - [Google 完全手冊](#) - [Google.com in English](#)

©2009 - [隱私權政策](#)

目標

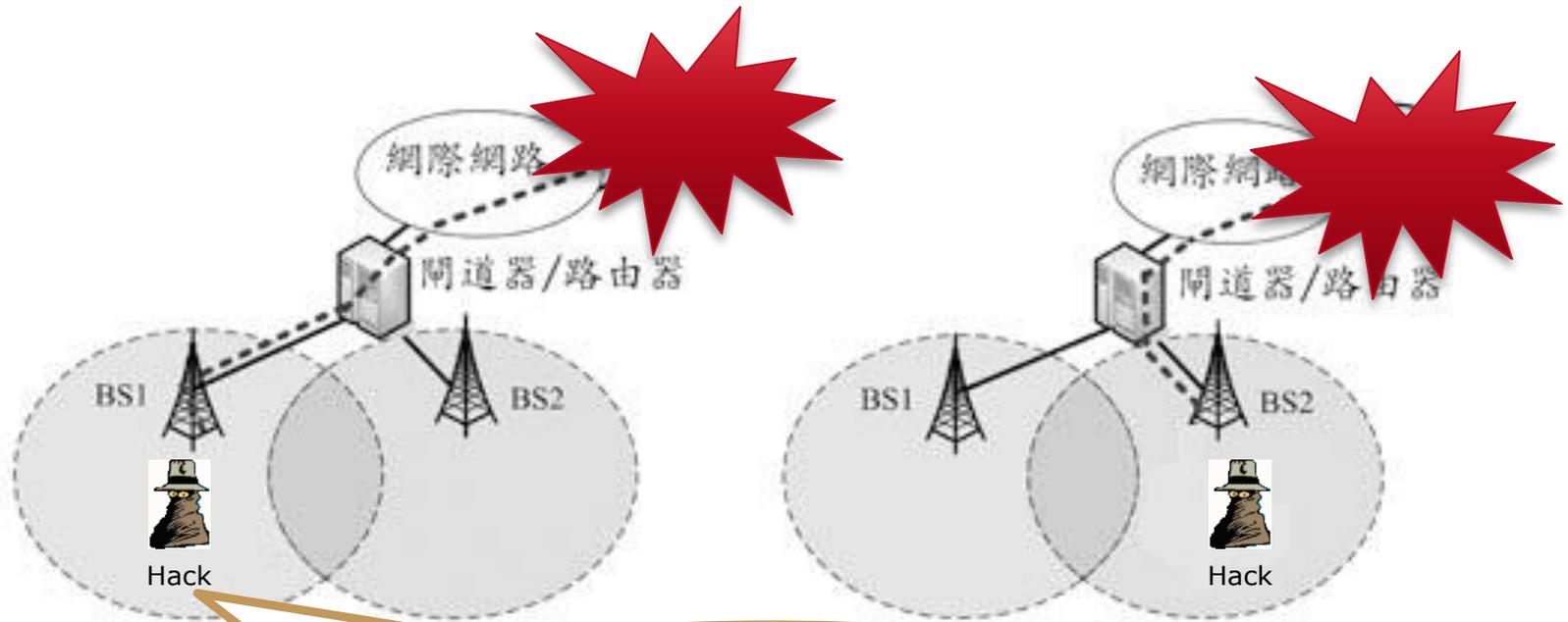
<http://www.1c188.cn/manage/Login.asp>

I

系統入侵實務 -- 躲貓貓入侵攻擊

- 躲貓貓入侵攻擊(行動設備) 入侵流程圖
- 目前阻擋難度高又不異追蹤
- 目前阻擋設備的方式
- 行動設備功能上限制

行動式設備入侵流程圖



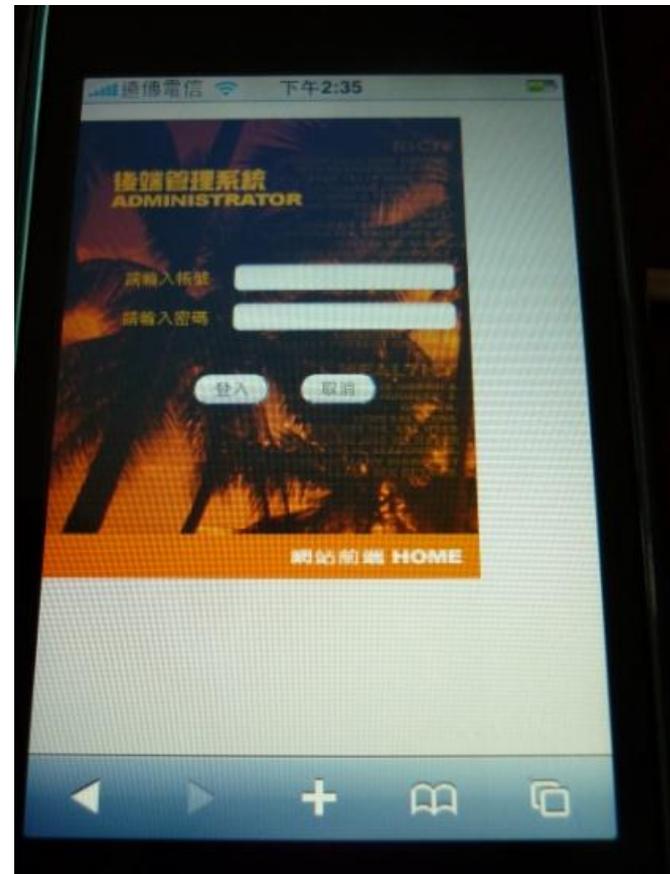
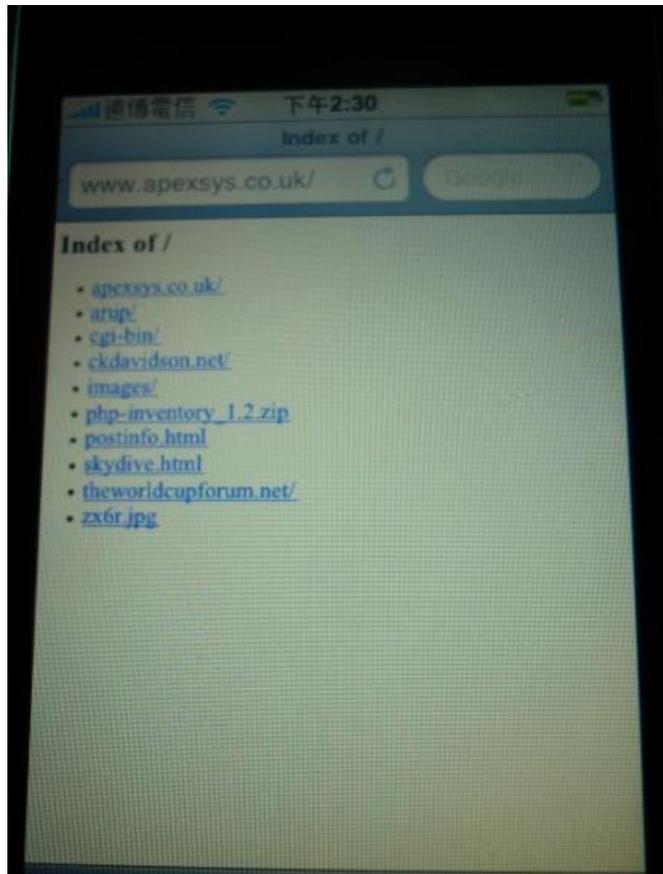
利用一般常見入侵手法(SQL Injection、弱密碼等)

Demo

系統入侵實務 - 手機版



行動式設備入侵伺服器



五招判斷手機惡意程式

- **Android**上的惡意程式數量爆增，數量從80個增加到至少400個，還有許多是還沒被偵測出來的。五招判斷讓你的手機免受惡意程式影響。
- 第一招：注意星級及評等數
- 第二招：觀察使用者評論
- 第三招：留意**APP**的功能及介紹
- 第四招：查看**APP**存取權限
- 第五招：留意開發者的其他**APP**

手機安全防護重點事項

- 1.確實使用Android平台提供的基本手機防護：設定pin碼或是開機密碼等可以讓手機與資料受到基本保護。
- 2.盡量避免使用Wi-Fi自動連線功能：連上開放性的網路服務，如Wi-Fi，看似相當便利，但此類網路的開放特質如同雙面刃，會讓使用者手機中的資料暴露在輕易被有心人士竊取的風險中。
- 3.在下載來自第三方應用程式商店的APP前請審慎考慮。
- 4.當有程式或網頁請求授權時，請詳細閱讀其請求授權的內容。
- 5.安裝具有信譽且有效的智慧型手機防毒軟體：可有效阻擋惡意程式入侵手機平台，保護Android裝置免受惡意程式威脅。



**THE
END**