台北海洋技術學院
Taipei College of Miritime Technology
103學年度資訊安全教育暨智慧財產權教育講座

時間:104年5月22日 下午13:00~16:00
地點:台北海洋技術學院士林校區行政大樓2F 202電腦教室
講師: 陳國輝 先生

資訊安全講座

—資訊攻擊與防護

主講人：陳國輝

「知己知彼，百戰不殆」

孫子兵法

攻擊者的類型

貪圖小利的傳統破壞者

- 他們尋找方法盜接有線電視或竊取密碼使用免費資源等。

惡作劇的年輕人

- 通常不具備技術能力，只會使用工具進行攻擊。

心有不滿的員工

- 未必有高明的技術，但因為身在組織內部，經常造成極大的傷害。

專業駭客

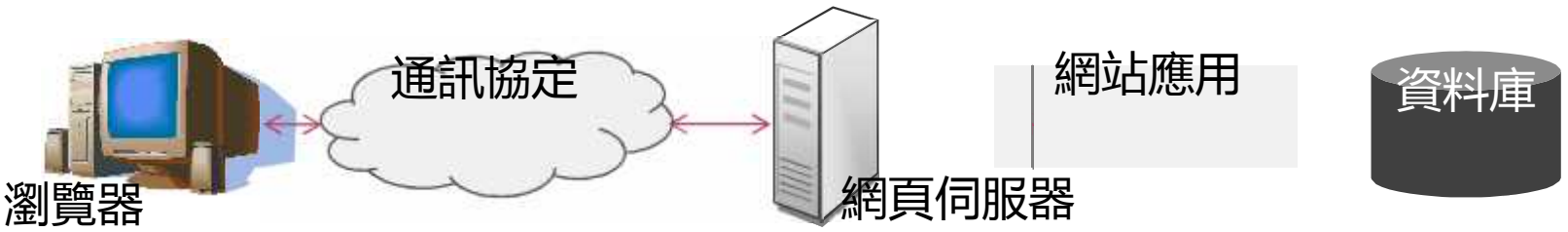
- 具備高級的技術能力，經常為經濟利益、意識形態、或自我炫耀而發起攻擊。

駭客分類

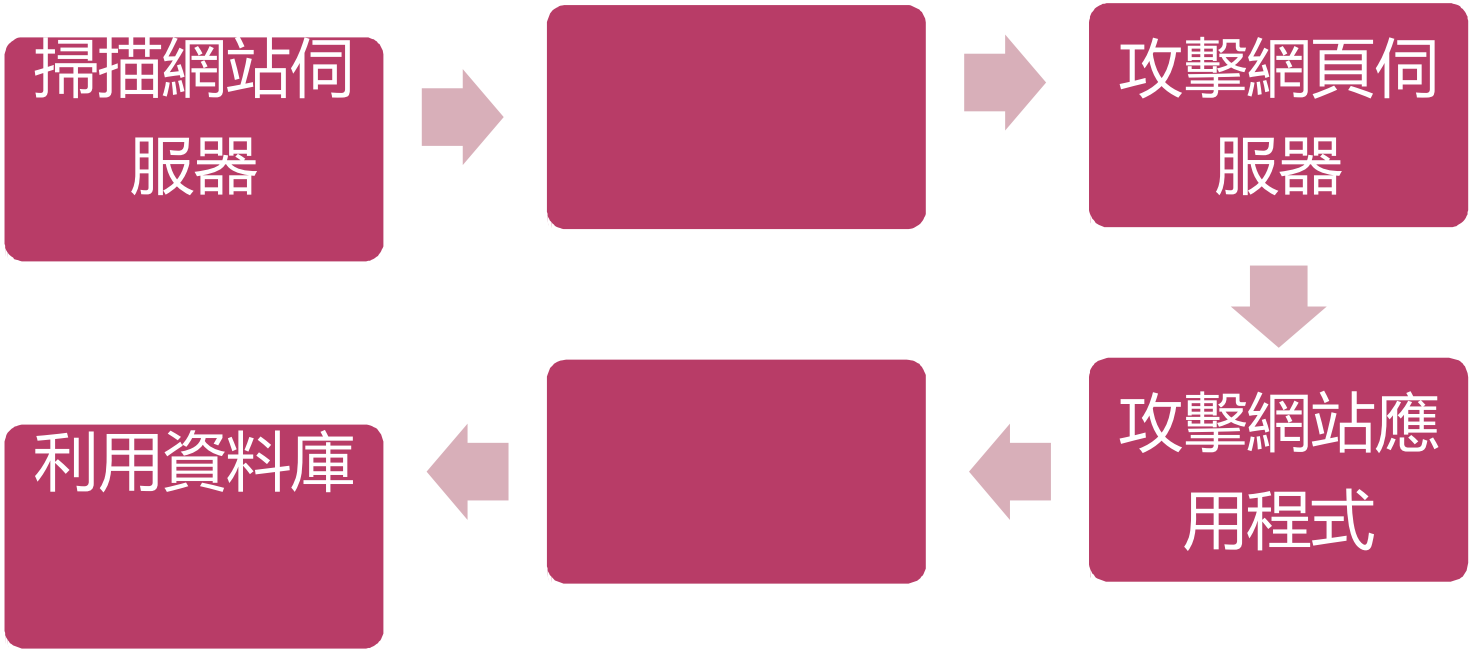
- Hacker 原指玩電腦的狂熱分子，但漸被用來指惡意攻擊電腦系統及網路的人。
- 指一些資訊安全專家，以類似駭客的手法檢驗系統與網路，協助公司或組織找到資訊安全漏洞。
- 指大多不違法，但又遊走法律邊緣常以類似駭客之手法便宜行事者。
- 指願意協助資訊安全人員瞭解駭客手法的駭客。

認識網站結構

- 瀏覽器 (browsers)：例如 Internet Explorer 或 FireFox 等
- 通訊協定 (transport protocols)：HTTP 或有加密功能之 SSL
- 網站伺服器 (web servers)：最常見的為以微軟為主的 IIS 和開放原始碼的 Apache
- 網站應用 (applications)：有 PHP 與 ASP 較常見。



網站攻擊步驟



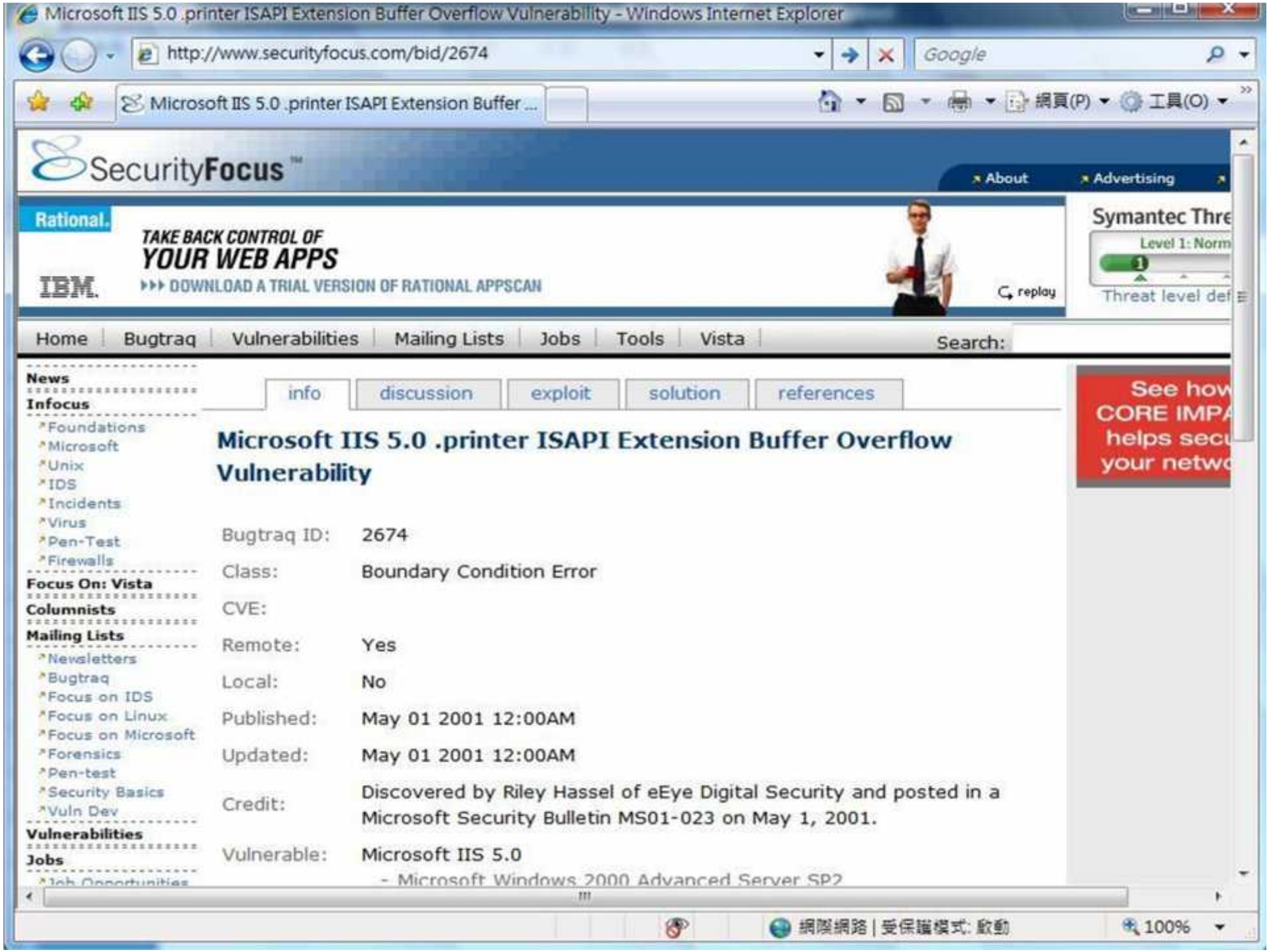
掃描網站伺服器

- 駭客常使用合法而免費的工具 (如 Nmap 或 Amap) 來尋找開放的電腦連接埠，或瞭解作業系統等。
- www.netcraft.com 是一個功能極強而不需安裝的工具，在它的 “What‘s that site running?...” 欄打上欲查詢之網站名，即可看到很詳細的網站資訊。
- 駭客也會使用簡單的通訊協定 (如 Ping 或 Telnet) 來測試網路結構，例如 Telnet 一個隨意網址，便能收集到以下資訊：

```
C:\>telnet www.anysite.com 80
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
```

瞭解網站與弱點

- 攻擊者查出網站伺服器的廠牌、型號後，便能進一步尋找該伺服器的已知弱點。
- 舉例說明，如果工具 (例如 Netcraft) 指出伺服器為 Microsoft IIS 6.0，則該系統使用 Windows 2003；若為 Microsoft IIS 5.0 則是 Windows 2000。
- 攻擊者可以在 www.securityfocus.com 或 http://nvd.nist.gov 等公開網站找出該系統的已知弱點。
  - 例如在 SecurityFocus 網頁的 vulnerabilities 輸入 “Microsoft IIS 5.0” 就能找到包括 “.printer ISAPI Extension Buffer Overflow” 等弱點，從 2000 年到 2007 年共 累計 76 項。微軟公司針對每一項弱點都已發行補丁，但若沒有依指示及時 安裝補丁，就易成為受攻擊的標的。


Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow Vulnerability - Windows Internet Explorer
http://www.securityfocus.com/bid/2674
Google
Microsoft IIS 5.0 .printer ISAPI Extension Buffer ...
網頁(P)
工具(O)
SecurityFocus
About
Advertising
Rational.
TAKE BACK CONTROL OF
YOUR WEB APPS
DOWNLOAD A TRIAL VERSION OF RATIONAL APPSCAN
IBM.
replay
Symantec Thre
Level 1: Norm
Threat level def
Home
Bugtraq
Vulnerabilities
Mailing Lists
Jobs
Tools
Vista
Search:
News
Infocus
Foundations
Microsoft
Unix
IDS
Incidents
Virus
Pen-Test
Firewalls
Focus On: Vista
Columnists
Mailing Lists
Newsletters
Bugtraq
Focus on IDS
Focus on Linux
Focus on Microsoft
Forensics
Pen-test
Security Basics
Vuln Dev
Vulnerabilities
Jobs
info
discussion
exploit
solution
references
Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow Vulnerability
Bugtraq ID: 2674
Class: Boundary Condition Error
CVE:
Remote: Yes
Local: No
Published: May 01 2001 12:00AM
Updated: May 01 2001 12:00AM
Credit: Discovered by Riley Hassel of eEye Digital Security and posted in a Microsoft Security Bulletin MS01-023 on May 1, 2001.
Vulnerable: Microsoft IIS 5.0
- Microsoft Windows 2000 Advanced Server SP2
See how
CORE IMPA
helps secu
your netwo
網際網路 | 受保護模式: 啟動
100%

攻擊網頁伺服器

- 網站伺服器偶而會被找出弱點，以下是 IIS 5.0 曾遭受攻擊的兩個弱點：
  - 緩衝區溢位 (buffer overflow)：2001 年 IIS 5.0 被發現有 .printer 檔案的緩衝區溢位，若連續被塞入 420 個以上的字元，緩衝區即滿溢。此時伺服器有可能會回覆給攻擊者一個 prompt，讓他有機會對主機直接下達指令。
  - 檔案系統橫越 (Unicode directory traversal)：IIS 5.0 對 Unicode 的檢查不夠嚴謹，若直接在 URL 欄填入長 Unicode，就可以騙過網站檢查。例如將 '/' 這個 符號輸入 URL 欄應該受到檢查，但若輸入這個符號的長 Unicode '%c0%af' 就 能不被檢查而直接接受。這讓 '../../../' (移往根目錄) 這種不該被接受的語句 能被插入 URL 欄，造成安全問題。2001 年的 Nimda 蠕蟲就是使用這個 IIS 弱 點。

攻擊應用程式

- 混淆 URL (URL Obfuscation)
  - URL 可以填入 IP 位址，例如 http://192.168.13.10。
  - 將這四個數字個別展開成 8 位的二進位數，再接成 32 位就成為：11000000101010000000110100001010，亦為十進制 3232238858。
  - 因此，http://3232238858 也會指向同一個網站，但以這種混淆的 URL 輸入法 有時可以騙過網站檢查，讀取一些不被允許的 IP。
- XSS 是駭客針對網站應用程式漏洞之攻擊手法，將 HTML 或 Script 插入 網頁中，造成其他人看網頁時受到影響。
  - 例如某位惡意的使用者，在一個網站填寫個人資料頁面時包含了以下這段文字：<script>alert('This is a pop!');</script>。當別的使用者瀏覽此人的個人資料，就有一個討厭的視窗彈出。

資料隱碼攻擊

- 部分網站程式將使用者輸入的資料直接交給資料庫處理，而未事先過濾可能有害的字元。讓駭客有機會在輸入的資料中夾帶 SQL 語言，進行資料隱碼攻擊 (SQL injection)。
- 此攻擊法並非透過病毒等手段，而是經由標準程序操作；因此為防火牆或防毒軟體所無法防範。唯有加強安全控管並建立良好的程式開發習慣。
- 資料隱碼攻擊有以下幾種方法，將在下幾頁中介紹。
  - 迴避授權查驗
  - 使用 SELECT 指令
  - 使用 INSERT 指令
  - 使用 SQL Server 程序

資料隱碼攻擊之防禦方法

對於字串的輸入加以過濾，並限制長度。例如單、雙引號都應排除。這種過濾應該被用在所有的應用軟體中，不光是網站。

加強資料庫權限管理，讓網站或軟體不以系統管理員的帳號連結資料庫。

GOOGLE HACKING

- 搜尋網站 (例如 Google) 的搜尋能力極為強大，往往會把敏感資訊公諸於世。Google hacking 是指使用搜尋引擎的連結侵入他人系統。
- Johnny Long 所著：“Google Hacking for Penetration Testers” 介紹許多 Google 駭客手法，也可上網站了解：http://johnny.ihackstuff.com。
- 如果在 Google 打入關鍵字 “Index of /admin” 可讓你連結到一些粗心網站的系統目錄內，而不需經過身分認證。
  - 打入“Index of /password” 或 “Index of /mail” 會有類似的結果。
  - 請注意：不可侵入他人系統，以免觸法。


Index of /admin - Google 搜尋 - Windows Internet Explorer
http://www.google.com.tw/search?q=Index+of+/admin&complete=1&hl=zh-TW&start=70&sa=N
Index of /admin
Index of /admin - Google 搜尋
網頁(P)
工具(O)
St. Louis City Dept. of Personnel Index to Admin. and Joint ... - [翻譯此頁]
... obtained from the Personnel Office at 1114 Market Street, Room 703, St. Louis, Missouri 63101. Administrative Regulations Index Joint Regulations Index ...
www.slpl.lib.mo.us/CityHall/Pers/data/reg.htm - 15k - 頁庫存檔 - 類似網頁
Index of /admin - [翻譯此頁]
Index of /admin. Parent Directory. Apache/2.2.8 (Unix) mod_ssl/2.2.8 OpenSSL/0.9.8g DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 ...
www.espantalagata.com.ar/admin/ - 1k - 頁庫存檔 - 類似網頁
Index of /admin/img/mag - [翻譯此頁]
Index of /admin/img/mag. Name Last modified Size Description. [DIR] Parent Directory 20-Oct-2005 14:57 -
www.fnss.com.tr/admin/img/mag/ - 1k - 頁庫存檔 - 類似網頁
Index of /admin - [翻譯此頁]
Index of /admin. Name Last modified Size Description. [DIR] Parent Directory 29-Feb-2008 12:58 - [TXT] featureadmin.jsp 06-Jun-2002 14:46 2k ...
www.merrywoodcottages.com/admin/ - 2k - 頁庫存檔 - 類似網頁
Index of /admin - [翻譯此頁]
Index of /admin. Icon Name Last modified Size Description. [DIR] Parent Directory - [ ] pancake.php 17-Jul-2007 21:49 795 [ ] ...
astral.zaptech.org/admin/ - 2k - 頁庫存檔 - 類似網頁
Index of /Admin - [翻譯此頁]
Index of /Admin. Icon Name Last modified Size Description. [DIR] Parent Directory - [DIR] awstats/ 30-Aug-2005 14:06 -
www.hellingeuroski.nl/Admin/ - 1k - 頁庫存檔 - 類似網頁
Lucene Index Search Admin - [翻譯此頁]
org.apache.lucene.index.FieldsReader. (FieldsReader.java:73) at ...
org.apache.lucene.index.IndexReader$1.doBody(IndexReader.java:110) at ...
search.fuwutong.asiaec.com/search?dir=news&index=TokenIndex&orderStyle=Score&q=%B0%B2%C3%DF... - 5k - 頁庫存檔 - 類似網頁
完成
網際網路 | 受保護模式: 啟動
100%

認識通關密碼

- 使用者名稱 (username) 與通關密碼 (password) 是時下電腦、系統、與網路身分認證最常用的方法。
- 破解通關密碼的手法不外以下幾種：
  - 以電腦重複去試各種可能的密碼，相關做法將於下幾頁詳細說明。
  - 以社交工程、網路釣魚、或使用中間監看工具來騙取密碼。
  - 由於許多使用者不願費心記憶密碼，所以用直覺或觀察法也甚為有效，例如：
    - 可以先試 “1111”, “1234”, “abcd”, “password” 之類的懶人密碼；或是輸入使用者名稱，許多人將這兩者設為相同。
    - 若有其私人資料，則試其配偶、子女之姓名拼音或生日，或以上合併。
    - 觀察當下環境裡是否有適合作密碼的字，例如網址、網名、廣告詞等。

窮舉攻擊法

- 假設通關密碼每個字元有 n 種選擇，而窮舉的密碼長度從 1 算到 i，那麼可能的密碼共有 Sum(n^1, n^2, …, n^i) 種。
- 舊式 ATM 規定的 PIN 為四位數字 (n=10, i=4)，共有 11,110 種選擇；現改為八位數之後，選擇增加了一萬倍。
- 電腦使用標準鍵盤，可以增加 n，例如數字 (n=10)，字母 (n=26)，大小寫分開 (n=26)，鍵盤符號 (n=33)。若以上都用，則 n=95。假設窮舉所有的八個位數的密碼，則有 6,704,780,954,517,120 種。
- 經過這樣的分析，我們得到兩點結論：
  - 由於運算時間過長，窮舉攻擊並不適合用來攻擊電腦的通關密碼。
  - 設計通關密碼時，較長的 n 和 i 可以有效的遏阻密碼攻擊。

字典攻擊法

- 字典攻擊乃基於一個假設：一般人設定的密碼大多可以在字典裡找到，或是可以用其他方法猜測與分類。這個假設甚為合理，因為幾乎沒有人能記得 (或願意去記) 一個隨機產生的八位元密碼。
- 網路上有許多字典攻擊工具，其中以 Cain & Abel 與 John the Ripper 較具知名度。這類工具是把兩刃劍：一方面可能幫助駭客攻擊別人的密碼；另一方面，若整合進身分認證系統，可幫助使用者挑選高強度之密碼。
- 通關密碼的選擇具有語言及地區性。英語系國家的使用者常選用英文單字；但華人使用者可能使用中文拼音。例如「小明」的拼音與四聲為：Shiao3Ming2，從英文看這個密碼很強，在台灣則未必。
- 許多人在研究密碼的規律性；而使用者設密碼時，應避免規律性。

通關密碼之政策

- CISSP 建議以下的通關密碼政策：
  - 至少六個字元長度，應包含數字、大小寫及特殊符號，不應為字典中的單字或與使用者名稱有關連。通關密碼需經常更換，並勿重複使用。應訓練使用者如何挑選及保護密碼，包括：不可與人分享密碼，避免易被猜中之密碼，並不可將密碼放置於未受保護之處。
- 每當幾次密碼輸入錯誤，系統可以暫時鎖住該帳戶數分鐘，可有效減低窮舉或字典等攻擊之速度。
- 在系統計算每個密碼的雜湊函數時，可以額外加入一個密值，讓駭客事先計算或下載的彩虹表失靈。這個作法稱為加鹽 (salted)。
- 可以在使用者設定新密碼時做簡單的檢查，例如要求輸入的密碼應含有數字、大寫、小寫、與特數符號四者中至少三種。

認識無線通訊技術與弱點

- 家用無線電話：早期（十數年前）家用無線電話沒有安全措施，若與鄰居使用同型機具，就能彼此聽到通話。目前的無線電話已安全許多，但若有適當的工具，仍然可以空中竊聽。
- 衛星電視：衛星電視節目經常遭到未付費戶的非法接收。2001 年美國衛星電視業者 DirectTV 使用動態碼結合智慧晶片，讓十萬台偽造的機上 盒一夕之間變成為廢物，情況方得控制。
- 行動電話：第二代數位電話開始具備加解密功能後，空中竊聽就非常困難；但在電信業者機房依然可以側錄。
- 藍芽 (Bluetooth)：藍芽有許多安全弱點；Bluejacking 攻擊能將資料塞進使用藍芽的機具；Bluesnarfing 攻擊能從機具中盜取資料。

認識無線區域網路

- 無線區域網路 (wireless LAN or WLAN) 的標準為 802.11 系列，由 IEEE 在 1997 年制定。
- 802.11 技術持續在演進中，較常使用的 2.4GHz 標準包括過去的 802.11b (11Mbps) 和現在的 802.11g (54Mbps)。802.11n 預計在 2009 年 通過標準，傳輸速率可達數百 Mbps，距離也較遠。
- 802.11 使用以前軍方的 spread spectrum 技術，可以降低雜訊干擾並且可隨訊號品質調整傳輸速率 (訊號品質好就能提高速率)。
- 802.11b/g/n 將頻寬切分為 14 個互有重疊的通道 (channels)，每個通道 距離 5MHz。但每個國家有不同的頻寬限制，台灣與北美相同只能用
  11 個通道，大部份歐洲國家可以用 13 個。

WLAN 的安全問題－WEP

- 無線網路比有線網路更難保障傳輸安全，有鑑於此，一種加密傳輸方法 Wired Equivalent Privacy (WEP) 被設計並廣為應用，然而此法已被完全被攻破。
  - WEP 使用 RC4 對稱式加密法，但裝置的方式有漏洞。
  - WEP 的初始值 (initialization vector, IV) 會被重複使用，收集夠多的封包後，就可以解開密鑰。
  - 此外，WEP 沒有將整個傳輸加密，表頭和表尾皆為明碼。
- Wi-Fi Protected Access (WPA) 被提出以修補 WEP 的問題。
  - WPA 使用修正的 RC4 (TKIP) 並增加金鑰長度，IV 由 24 bit 增至 48 bit；進階的 WPA2 更使用 AES 加密。

無線網路攻擊

無線網路的竊聽攻擊

- 竊聽攻擊是無線網路的基本問題，任何在射頻範圍內的機具都可以接收到訊號。
  - 將無線 NIC 卡設定在隨意模式 (promiscuous mode)，就可以接收所有的封包，而不僅限於自己的 IP 位址。
  - 使用強化天線，可以接收更遠的訊號。一個簡易的 cantenna 有機會收到三百公尺外的 WLAN 訊號。
  - 相當多的無線網路沒有啟動最基本的安全設定，因此被竊聽的資料是以明碼傳輸。而 FTP 與 SMTP 等協定在傳輸使用者名稱與通關密碼時，也都是使用 明碼。
  - 如前所述，即使以 WEP 加密傳輸，仍可輕易的以工具破解。
  - 相關資訊及工具可參考 www.wardriving.com。

開放身分認證

- 大部分的無線網路設備 (如基地台) 在出廠時的設定都是 open systems authentication，也就是不論任何人或系統，都可以不經身分認證地自由使用。許多旅館、咖啡館、餐廳提供的無線網路都處於開放身分認證的狀態。
  - 惡意使用者可以經由這個網路的連結做不法的事，卻隱藏自己的 IP。
  - 開放身分認證的狀態讓連結上來的使用者都冒著遭人竊聽的風險。
  - 大部分使用者上網後的第一件事就是查電子郵件，開放身分認證這個狀態讓使用者與郵件伺服器間的 ID 與密碼被暴露在公共場合。
  - 這種狀態也讓連結上來的主機有被安裝後門的風險。一旦這些被侵入的主機遭受駭客挾持，就可能在未來被用作攻擊別人的傀儡機器 (zombies)。

欺騙的無線基地台

- 在無線網路世界裡，駭客未必扮演中間攻擊者，也可能是一個基地台，稱做欺騙基地台 (rogue access point) 或孿生惡魔 (evil twin)。
  - 若你在公共場合急著上網，可能會隨意選擇任何能夠上網的無線網路，卻連結到了一個駭客所設置的基地台。
  - 駭客基地台可能取了一個足以亂真的名字，例如 WiFi-Service，假裝成收費網路服務，向使用者要信用卡號及驗證碼。
  - 基地台的角色也讓駭客可以攔截機密資料，如網路銀行密碼等。
  - 有時駭客會在公司附近安裝無線基地台，如果一台公司內的電腦同時連結公司內部有線網路 (intranet)，又連結了駭客基地台，那麼駭客就有機會經此路徑侵入公司內部網路。
  - 有的 WLAN 卡會自動連結訊號最強的無線網路，而未徵詢使用者。

無線網路的拒絕服務攻擊

- 身分認證洪水攻擊 (authentication flood attack) 是指駭客對基地台不斷發出身分認證的要求，讓認證伺服器無法回應其他使用者的正常要求。
- 解除授權洪水攻擊 (deauthentication flood attack) 是相反的，由駭客偽裝伺服器，不斷的向某個使用端電腦發出解除授權信號，該電腦意欲重新連線，則繼續用解除授權來阻斷。
- 無線干擾攻擊 (network jamming attack) 是使用高能量的電波發送機對預干擾的區域發射，一台 1000 瓦的發送機可以在一百公尺外干擾一個 小型辦公室的無線網路。
- 更高功率的電波發送機若以天線對準基地台發射脈衝波，有機會永久性損毀基地台的電子元件。

無線網路的安全措施

將資料加密，所以未經授權的人無法取得機密。

設定存取權限，沒有必要之人就不應享有權限。

徹底保護硬體設施如門禁、主機、與基地台等。

使用高強度的身分認證，確保進入網路者是合法使用者。

在各個防禦層次設定安全控制；萬一某層被攻破，仍能控制損害。

惡意程式的種類

- 較為眾人熟悉的惡意程式是病毒、蠕蟲和木馬程式，這三者也經常在媒體報導上被彼此誤用。下圖顯示三者間的差異。
- 惡意行動碼與追蹤 cookies 主要是在網站瀏覽過程中入侵。
- 攻擊工具是指後門程式、rootkits 與鍵盤側錄等，本身不造成損害，而是植入後可供駭客使用的工具。

特徵	病毒	蠕蟲	木馬	惡意行動碼	追蹤 cookie	攻擊工具
可否自行存在？	否	是	是	否	是	是
可否自行複製？	是	是	否	否	否	否
擴散方法為何？	使用者互動	自行擴散	使用者不知情的網路下載、電子郵件附檔、或由惡意者植入			

病毒

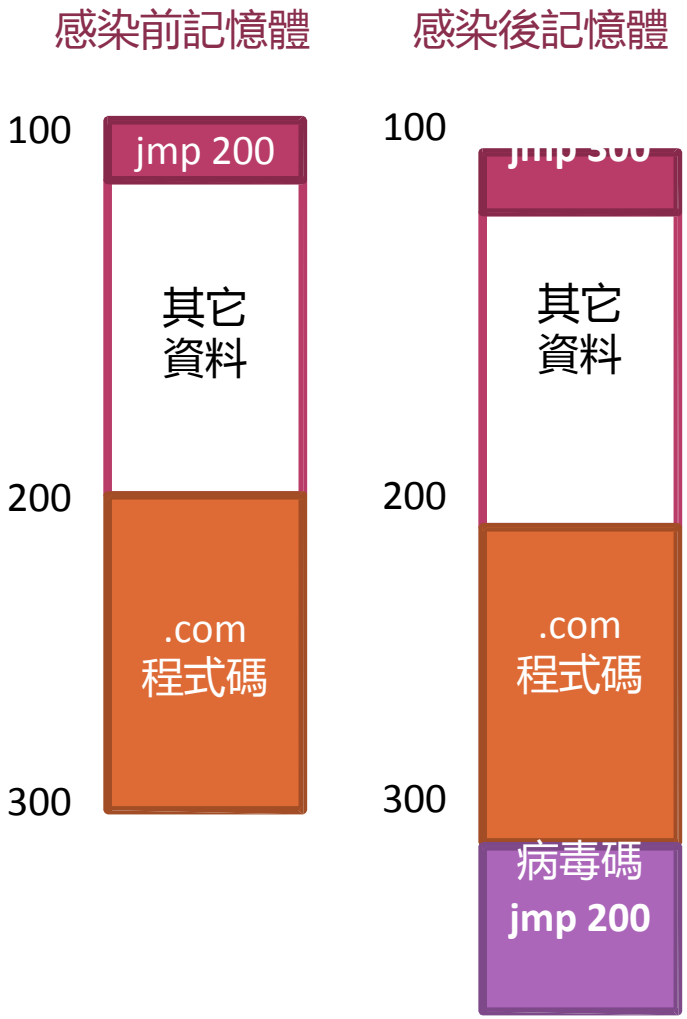
- 病毒 (virus) 複製自己並擴散到其它的檔案、程式或電腦上。
- 每種病毒有自己的擴散方式，例如寄生在檔案或程式上再經由使用者下載、拷貝後感染。
- NIST SP800-83 將病毒分為兩大類：
  - 編譯病毒 (compiled viruses) 是經過編譯的程式，可以在作業系統上直接執行。
  - 直譯病毒 (interpreted viruses) 則靠應用程式執行。兩種主要類型為巨集病毒 (macro viruses) 與指令碼病毒 (scripting viruses) 。

病毒躲避監視的手法

- 千面人 (polymorphism)：病毒藉著與不同的金鑰加密來改變外形，以躲避防毒偵測；啟動攻擊前再自我解密。病毒的內容在變形過程中並沒有實質改變。
- 變體 (metamorphism)：病毒不是靠變形來躲避監視，而是實質地改變自己的內容。例如在原始碼中加入多餘的程式或調整程式順序後重新編譯，就產生變體病毒。
- 隱藏 (stealth)：病毒利用各種技巧隱藏自己，例如有的隱藏病毒可以修改作業系統顯示的檔案大小，讓人無法察覺被寄生檔案的改變。
- 加殼 (armoring)：病毒使用特殊的程式碼保護自己，使防毒軟體或清毒專家更難偵測、分解與瞭解病毒碼。
- 通道 (tunneling)：病毒建立通道來攔截低階的作業系統呼叫與中斷，以削弱防毒軟體的偵測功能。

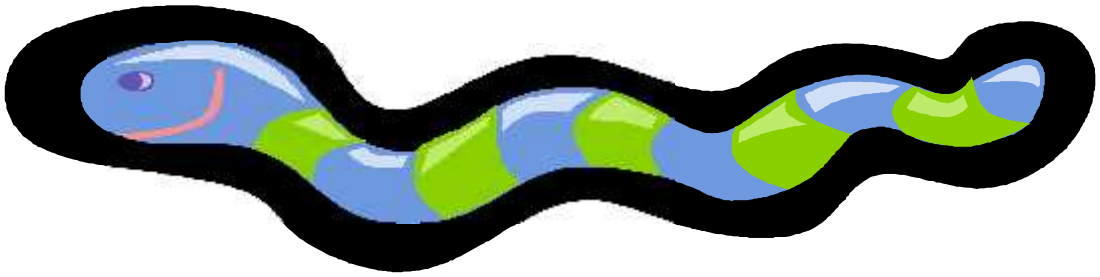
早期病毒的範例

- 作業系統從位址 100 開始執行這個程式；第一行直接跳到 (jump) 可執行程式碼的第一個指令位址 200，開始執行這個程式。
- 病毒將病毒碼寫在 .com 程式後面，並將位址 100 的內容改成 “jmp 300” 跳到病毒碼的位址。
- 執行病毒碼的結果可能包括再去感染別的 .com 程式，或在某種條件下發動惡意攻擊。
- 病毒碼執行完之後，再跳回 200 執行原程式碼，避免受到注意。



蠕蟲

- 病毒需要寄居體，而蠕蟲則相當獨立：它可以自行存在、自行複製、自行擴散。因此蠕蟲可以在短時間內快速擴散，形成全球性事件。蠕蟲利用網路或系統的已知弱點來進行攻擊與擴散。
- 網路服務蠕蟲 (network service worms) 利用網路服務中有弱點的作業系統或應用程式進佔主機；再繼續掃描其它相同弱點的主機，作為攻擊目標。由於蠕蟲擴散不需要人的參與，所以擴散極快。
- 大量郵件蠕蟲 (mass mailing worms) 與郵件病毒相仿，只是蠕蟲不需要寄居在其它檔案上。郵件蠕蟲感染一台電腦後，繼續使用受害者的通訊錄將自己再大量的寄出。



木馬

- 木馬程式可以自行存在，但不以複製或擴散為目的。它看似好的程式，卻暗藏惡意。
- 偵測木馬程式有時並不容易，因為它執行起來像是一個正常的應用程式。此外，較新的木馬程式也會使用躲避監視的手法。
- 不同於病毒或蠕蟲只會產生破壞，木馬程式可能為攻擊者帶來利益，因此木馬攻擊似有凌駕前兩者的趨勢。
- 可以使用木馬程式來散播間諜軟體；也可以用木馬進行未經授權的存取。

惡意行動碼

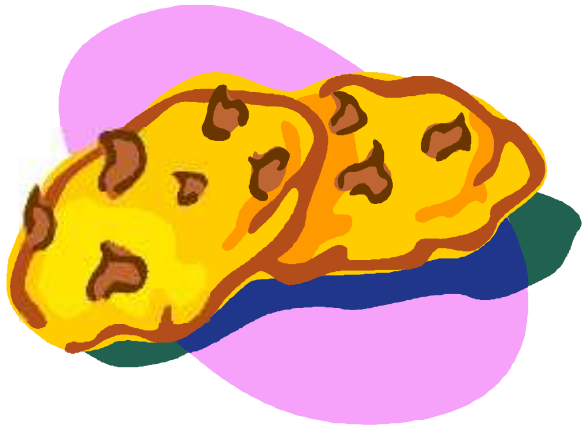
- 網路時代開始後，大家開始撰寫跨平台行動碼 (mobile code)，在不同的作業系統、不同的瀏覽器及電子郵件閱讀器上都能順利執行。
- 行動碼可以從遠端系統傳來在本地執行的軟體，通常行動碼的下載不需要使用者的允許。
- 雖然行動碼大多是善意的，但惡意行動碼可以攻擊系統，並傳送病毒、蠕蟲及木馬。
- 惡意行動碼與病毒及蠕蟲等頗有不同，它不感染檔案或企圖擴散，也不利用特定的弱點。惡意行動碼是靠本地主機所授予行動碼的權限。
- 行動碼最常使用的語言是 Java, ActiveX, Java Script, VB Script 等。
  - 2001 年造成巨大傷害的 Nimda 即是使用 Java Script 寫成的惡意程式。Nimda 是 admin 倒過來寫，至今作者不詳。

混合攻擊

- 混合攻擊 (blended attack) 是一個惡意程式使用多種感染與傳輸方法，Nimda 惡意程式就使用了四種擴散方式：
  - 電子郵件：當一個主機有弱點的使用者打開了被感染的電子郵件附件，Nimda 感染主機，並找出郵件通訊錄將自己大量的寄出。
  - 視窗的資源分享：Nimda 掃描設定不當檔案分享的主機，利用 NetBIOS 傳輸來感染主機上的檔案。當使用者執行被感染的檔案，就會啟動 Nimda。
  - 網站伺服器：Nimda 掃描網站伺服器，尋找微軟 IIS 的已知弱點 (同一弱點在 2001 年稍早被 Code Red 蠕蟲利用，造成全球三十餘萬台電腦被感染)，若找到弱點，就感染該伺服器及其檔案。
  - 網站客戶端：如果一台有弱點的網站客戶端瀏覽了被 Nimda 感染的網站伺服器，則客戶端主機也被感染。
- 除了以上方法，混合攻擊也可以利用 IM 或 P2P 做為擴散管道。

追蹤 COOKIES

- Cookie 是特定網站在客戶端建立的一個小資料檔。
  - 會談 cookie 是暫時的，只在一次網站拜訪中有效；
  - 長期 cookie 則長期存在客戶端電腦中，在每次拜訪該網站時，讓網站得以識別該使用者。網站可以藉以記錄使用者的喜好。
- 然而長期 cookie 可被利用做為間諜程式，在使用者不知情下，追蹤他的瀏覽器活動。
  - 例如一家行銷公司在許多網站上都放廣告，卻在使用者主機上都用同一個 cookie，就可以追蹤這位使用者在每個網站的行為。



攻擊工具 (I)

- 攻擊工具 (attacker tools) 主要是幫助攻擊者不經授權地存取被感染的系統。攻擊工具可以藉由蠕蟲或木馬等惡意程式送進系統；再被用來進行下一步的攻擊。
- 後門程式 (backdoor) 泛指專門聽 TCP 或 UDP 埠的惡意程式。後門程式通常包含客戶端與伺服器兩個部分，前者在入侵者的遠端電腦上，後者在受感染的系統內。兩者連線後，入侵者就可以存取受感染系統的檔案或下指令。
  - 殭屍程式 (zombie) 是一種後門程式，植在一個系統內讓它去攻擊別的系統。DDoS 攻擊就是利用許多的殭屍系統同時對一個受害者發動攻擊。

攻擊工具 (II)

- 鍵盤側錄 (keylogger) 監視並記錄鍵盤的使用，可能包括受害者鍵入的密碼、郵件、信用卡帳號等私密訊息。
- Rootkit 是一個或一組的惡意程式可以幫助入侵者控制系統並躲避偵測，成功地植入 rootkits 可以讓入侵者擁有管理員的權限。
- 瀏覽器嵌入軟體 (web browser plug-in) 可被用做間諜程式；一旦嵌入後，可以監視使用者的瀏覽器活動，包括上過的網站與瀏覽的網頁。
- 攻擊者工具包 (attacker toolkits) 可以一次植入各種工具到受害者的電腦裡面，讓攻擊者立即或日後監控受害者。
  - 攻擊者工具包裡可能有：封包監視器 (pocket sniffers)，連接埠掃描器 (port scanners)，弱點掃描器 (vulnerability scanners)，通關密碼破解器 (password crackers)，遠端登入程式 (remote login programs) 以及可以發動 DoS 之類攻擊的攻擊工具 (attacks)。

網路釣魚

- 網路釣魚 (phishing) 是一種欺騙攻擊，它可能是一個看似有公信力的惡意網站，或是冒名的電子郵件要受害者連結到惡意網站。
  - 下圖是一封釣魚郵件，惡意者冒用匯豐銀行之名，要求收件者上釣魚網站填寫一張網路銀行的表格。該信已被過濾為垃圾郵件。


寄件者: HSBC [cservice.refXS2828576385481LZ.bib@hsbc.com]
寄件日期: 2007/12/15 (星期六) 上午 01:0
收件者: Hansonlai
副本:
主旨: (HSpam?) HSBC Bank: Urgent Message! (mess_id: T0415090806335)

Dear HSBC Bank business customer,

HSBC Customer Service team requests you to complete Business Internet Banking Online Form (BIB Online Form).

This procedure is obligatory for all HSBC Bank business customers.

Please select the hyperlink and visit the address listed to access BIB Online Form.

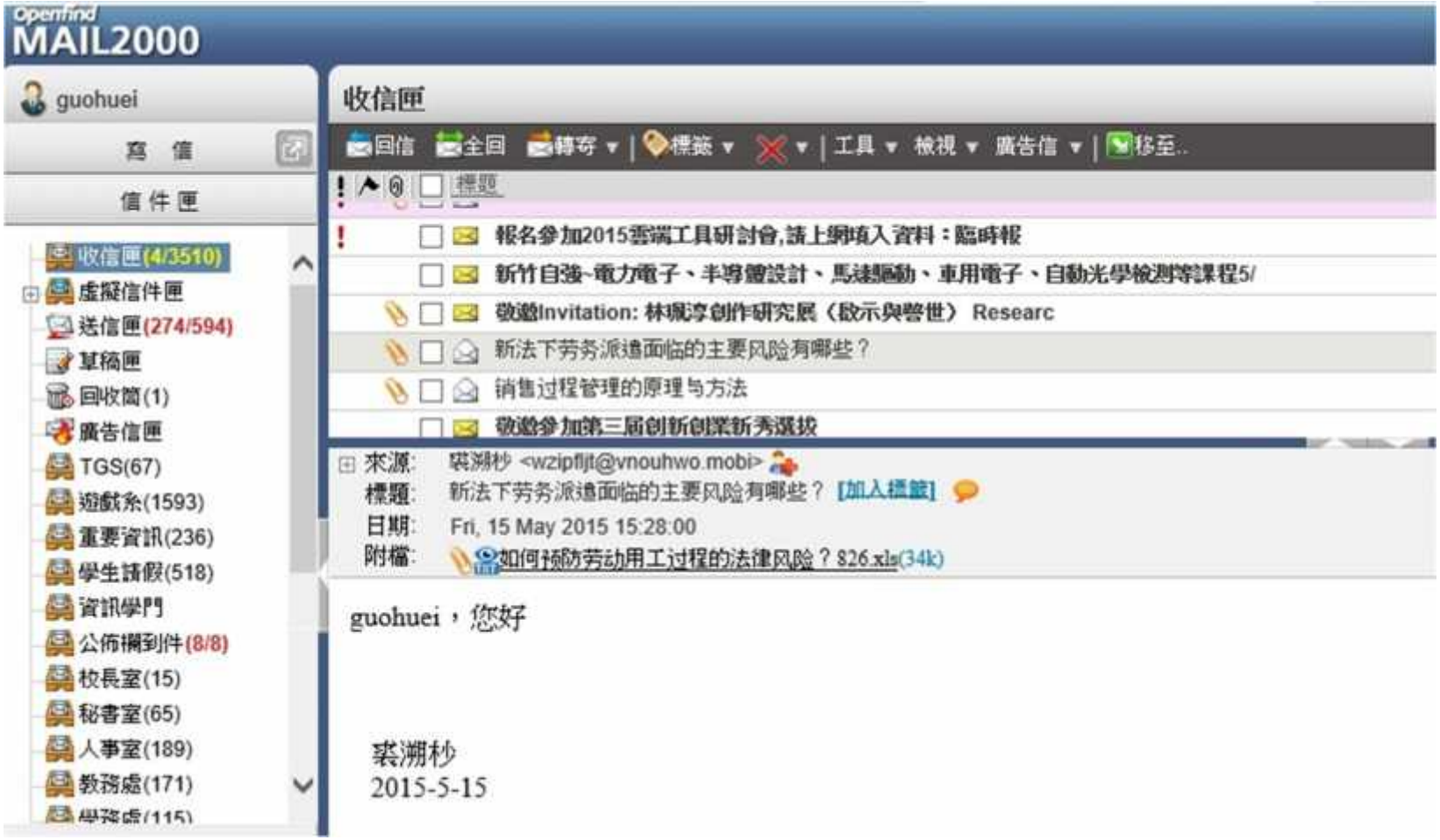
http://business-internet-banking.hsbc.com/bibauth/formStart?partnerid=HBEU22413151214098571004036083082372845987804958845991049

Please do not respond to this email.

.....

© Copyright hsbc.com, inc 2007. All rights reserved.

釣魚信範例(一)


Openfind
MAIL2000
guohuei
寫 信
信件匣
收信匣(4/3510)
虛擬信件匣
送信匣(274/594)
草稿匣
回收筒(1)
廣告信匣
TGS(67)
遊戲系(1593)
重要資訊(236)
學生請假(518)
資訊學門
公佈欄到件(8/8)
校長室(15)
秘書室(65)
人事室(189)
教務處(171)
收信匣
回信 全回 轉寄 標籤 工具 檢視 廣告信 移至..
標題
報名參加2015雲端工具研討會,請上網填入資料：臨時報
新竹自強~電力電子、半導體設計、馬達驅動、車用電子、自動光學檢測等課程5/
敬邀Invitation: 林珮淳創作研究展（啟示與警世） Researc
新法下劳务派遣面临的主要风险有哪些？
销售过程管理的原理与方法
敬邀參加第三屆創新創業新秀選拔
來源: 裘溯杪 <wzipflit@vnouhwo.mobi>
標題: 新法下劳务派遣面临的主要风险有哪些？ [加入標籤]
日期: Fri, 15 May 2015 15:28:00
附檔: 如何预防劳动用工过程的法律风险？826.xls(34k)
guohuei，您好
裘溯杪
2015-5-15

惡意程式的防禦

- 安全政策應說明惡意程式之防禦責任，做為建置各項防禦措施之基礎。

- 建立並維持所有人對惡意程式的認知，並加強資訊人員對惡意程式防禦的教育訓練，可以有效降低人為錯誤所造成的資訊安全事件。

- 補強系統及網路的弱點可以降低惡意程式的攻擊動力。

威脅防禦

- 建置多重的威脅防禦措施 (如防火牆與防毒軟體) 可以避免惡意程式成功的攻擊系統或網路。

安全政策

- 如果沒有惡意程式防禦的相關政策，組織就不會貫徹執行防禦措施。以下為部分範例，可做為惡意程式防禦政策之參考：
  - 外部進入組織的任何儲存媒體都要通過惡意程式掃描後才能使用。
  - 所有電子郵件附件都要先存入本地磁碟並通過掃描後才能開啟。
  - 禁止以電子郵件送出或接收某些種類的檔案，如 .exe 檔。
  - 限制或禁止使用可能傳輸惡意程式的軟體，例如 P2P 或沒有公信力的 IM。
  - 一般使用者不該有管理員的權限。
  - 要求系統與應用軟體更新並安裝補丁。
  - 限制使用可移除的儲存媒體，如 USB 碟；尤其在公共區域或安全區域。
  - 指明各系統應該安裝的防禦軟體，並指導軟體的設定方式。
  - 規定只能使用組織認可的方法與其它網路通訊。

教育訓練

- 組織的資訊安全教育訓練中，應該加強惡意程式防禦的認知，以下是部分宣導重點：
  - 不開啟可疑之郵件或附件，即使熟識寄件者。
  - 不開啟某些種類的檔案 (如 .exe 與 .com 等)。
  - 不回應要求提供財務或個人資料的電子郵件。
  - 不點選可疑網站的彈出視窗。
  - 不瀏覽任何可能含惡意內容的網站。
  - 不任意關閉安全防禦機制，如防毒軟體與個人防火牆等。
  - 一般系統操作時，不使用管理員等級之帳號。
  - 不下載來路不明的程式。

弱點補強

補丁管理

- 安裝補丁是作業系統與應用程式最常用的弱點補強。
- 新的弱點被公布而補丁未安裝前，是系統最脆弱的時候。

最小權限

- 最小權限原則是在不影響工作的情況下，只提供最小的使用權限給使用者、程式和主機。

強化主機

- 主要的原則還是關掉或移除不需要的服務、排除不安全的檔案共享、建置身分認證機制並勤於更換夠強的密碼。

防毒軟體

- 掃描系統最重要的部分，像是啟動檔。
- 注意系統上可疑的活動，例如當系統接收或傳送電子郵件時掃描附件。
- 監視應用程式的行為，例如郵件軟體、瀏覽器和 IM 等。在應用程式執行有風險的動作前(例如下載行動碼)，防毒軟體應提醒使用者。
- 掃描檔案檢查已知病毒。應該設定防毒軟體固定時間掃描整個硬碟，同時也要掃描其它儲存媒體。
- 識別惡意程式的種類，像是病毒、蠕蟲、木馬、行動碼、鍵盤側錄等。

防毒偵測的準確性

- 防毒軟體對惡意程式的偵測方式仍是以比對特徵 (signatures) 為主；這種方法對識別已知惡意程式相當有效，對已知病毒的變形、變種也有很好的偵測效果。
- 特徵比對乃針對已知的威脅；要偵測全新的惡意程式則使用探索方式 (heuristic method)，包括在程式裡搜尋可疑的邏輯順序，或是先在虛擬機器 (virtual machine) 上執行程式來檢查可疑活動。
- 偵測新威脅的探索方式容易造成誤殺 (false positive)，也就是把好的檔案誤判為惡意程式。因此，商用防毒軟體通常會讓使用者自己調節偵測的敏感度，在安全性和方便性之間做取捨。
- 主要的防毒軟體廠商通常在重要攻擊事件發生幾小時內，就要完成惡意程式分析、編寫攻擊特徵、測試之後連同說明文件下載給用戶。

間諜程式的偵測與移除

- 防毒軟體主要在處理惡意程式；而間諜程式偵測與移除工具則同時針對惡意程式及非惡意程式形態的間諜程式。它常見的功能包括：
  - 監視最有可能帶進間諜程式的應用程式，像是瀏覽器與電子郵件軟體等。
  - 經常性的掃描檔案、記憶體與設定檔，尋找已知間諜程式。
  - 識別幾種間諜程式類別，包括惡意行動碼、木馬程式與追蹤 cookies 等。
  - 防止幾種間諜程式的下載方法，包括網站的彈出視窗、追蹤 cookies、瀏覽器嵌入等。
  - 監視網路及作業系統的核心，以及啟動程式。
  - 隔離或刪除間諜程式。

惡意程式事件的處理

- 組織本身的事件反應能力，是處理惡意程式攻擊的基礎。第二章我們曾介紹事件反應的程序包括分類 (triage)、調查 (investigation)、隔離 (containment)、分析 (analysis) 與追蹤 (tracking)。
- 負責處理惡意程式事件的人應熟悉事件反應程序及以下的知識領域：
  - 惡意程式感染方法。處理惡意程式攻擊的人要清楚了解主要惡意程式種類的擴散方法。
  - 惡意程式偵測工具。處理惡意程式攻擊的人需要熟悉防毒軟體、入侵防禦系統、防火牆、間諜程式偵測與移除工具等。
  - 電腦鑑識 (computer forensics)。如第二章 30 頁所介紹的，電腦鑑識是調查惡 意程式攻擊所需要具備的專業。
  - 廣泛之資訊技術。廣泛的知識才能讓一位資訊安全專業人士正確評估惡意程式攻擊對組織造成的衝擊，並對隔離及復原程序做精準的建議。
  - 程式設計。程式設計經驗有助於分析惡意程式的行為。

惡意程式事件的徵兆

- 網路伺服器當機。
- 使用者在網際網路上存取主機速度變慢、系統資源被用盡、磁碟機變慢、系統啟動速度變慢等。(將 CPU 與記憶體使用率置於桌面隨時監視是個好方法。)
- 防毒軟體偵測到主機被感染並發出警訊。
- 系統管理員看到檔案名稱出現不正常字元。
- 主機記錄到稽核紀錄的設定值遭到變更。
- 電子郵件管理員看到大量內容可疑的退回信件。
- 許多主機上都出現防毒軟體被關閉的現象。
- 網路管理員注意到不正常的網路流量。

惡意程式隔離 (I)

- 惡意程式的隔離有兩個主要部分：阻止惡意程式的擴散與防止它進一步地傷害系統。幾乎所有惡意程式事件都需要進行隔離。
- 隔離方法可被分為四個類別：使用者參與、自動偵測、暫停服務與阻止某些網路連結。
- 使用者參與的隔離方法
  - 讓使用者參與是惡意程式隔離的重要部分，尤其當事件規模大的時候。
  - 要指導使用者如何識別感染現象，如果受感染要如何求助，例如聯絡資訊服務台，切斷網路連結或是關機。
  - 資訊能力較強的組織 (例如資訊公司) 可以指導使用者如何處理惡意程式，像是更新防毒軟體的病毒特徵，進行系統掃描，或是取得並執行特製的惡意程式處理工具。
  - 雖然使用者參與有助於惡意程式事件隔離，組織不能依靠這個方法。不論隔離指導給的多麼清楚，很難讓使用者都瞭解並且貫徹地執行。

後頁續

惡意程式隔離 (II)

- 自動偵測的隔離方法
  - 防毒軟體是最適用的惡意程式偵測及隔離工具。當發生大規模事件而防毒軟體無法識別惡意程式時，就應該使用其它資訊安全工具進行隔離，直到防毒程式的病毒特徵檔案得以建立。
  - 這些輔助方法包括以電子郵件伺服器與垃圾郵件過濾器來攔阻特定郵件，或是以 IDPS 過濾特定特徵的訊息。
- 停止服務的隔離方法
  - 惡意程式通常會依靠某種網路服務來擴散，因此停止該服務可以快速隔離惡意程式。例如電子郵件常是傳染的媒介，關閉電子郵件伺服器是一種有效的隔離手段。
- 停止連線的隔離方法
  - 同樣的，暫時停止網路連線也是快速有效的惡意程式隔離手段。

移除惡意程式

- 組織可以先使用工具或手工識別受感染的主機，以安裝補丁等方式修補弱點，最後再以防毒軟體等工具移除感染 (如下圖)。
- 如果作業系統被惡意程式做大幅變動或遭到太多惡意程式同時攻擊，就必須重建整個系統。

系統復原

- 惡意程式事件的復原工作包含兩方面：一為恢復受感染系統的功能與資料；另一為移除暫時隔離的措施。
- 一般惡意程式事件不需要做系統復原，例如只感染了幾個檔案，而且已被防毒軟體清除。但有的惡意程式嚴重地傷害系統或大量的檔案，或清除部分或全部的硬碟，就需要重建整個系統或從可靠的備份上還原，並且強化系統安全讓惡意程式無法攻擊相同的弱點。
- 在處理大型惡意程式事件過程中，決定何時解除暫時隔離的措施是一個困難的決定。
  - 例如，一個組織暫時關閉了電子郵件系統避免惡意程式的擴散，但是修補弱點、安裝補丁、到完全清除感染需要幾天甚至幾周的時間。電子郵件系統不能關閉那麼久，因此處理事件的人需要在風險可以控制的情況下恢復郵件系統。

事件後的檢討

- 處理重大惡意程式事件花費巨大的時間與精力，一個組織應該從過程中檢討、學習。可能的檢討結果包括：
  - 修正資訊安全政策避免類似事件再發生。例如 .scr 種類的電子郵件附件造成了病毒的擴散與攻擊，就修改政策禁止同類附件進入。
  - 改變認知教育訓練，強化使用者對事件的回報與處理能力。
  - 重新調整作業系統及應用程式的設定，來因應安全政策的修正。
  - 若事件發生的原因是惡意程式偵測與防禦工具不足，應該加強相關軟體的佈建。
  - 重新調整惡意程式偵測軟體，例如：
    - 增加軟體及病毒特徵碼的更新頻率。
    - 提高偵測準確性 – 降低誤放機率 (同時誤殺機率也相對地提高)。
    - 增加監視範圍，例如監視更多傳輸協定與檔案。
    - 修正當偵測到惡意程式時的反應。

問　　答

問答 1：

- 以下哪一種惡意程式無法自行存在？
  A. 病毒 Virus
  B. 蠕蟲 Worm
  C. 木馬 Trajan Horse
  D. 追蹤紀錄 Tracking Cookie

問答 2：

- 駭客會利用 Line 或 Facebook 進行詐騙與攻擊，所以應該養成哪一項正確的使用習慣？
  - A. 不接收與執行不明人士傳來的檔案
  - B. 不點擊不明人士分享的不明網址
  - C. 不點擊朋友突然傳送的不明網址
  - D. 以上皆是

問答 3：

- 為了避免電腦淪為駭客可操控的殭屍電腦，應該安裝哪項最基本的防護軟體？並定期更新
  - A. 分享軟體
  - B. 反垃圾郵件軟體
  - C. 防毒軟體與防火牆
  - D. 網頁過濾軟體

問答 4：

- 馬航失蹤班機的新聞也淪為駭客散播病毒的工具，所以平時應該如何防範電腦中毒
  - A. 安裝防毒軟體並定期掃毒
  - B. 注意發信來源及電子信箱是否正確
  - C. 定期更新作業系統與軟體修補程式
  - D. 以上皆是

問答5：

- 收到銀行寄來的電子郵件，內容是立即點選連結網址更新個人資料，可得一萬點紅利點數，這時應該如何處理？
  - A. 立即點選更新個人資料以獲取紅利點數
  - B. 可能是網路釣魚郵件，不要點選郵件中的網址，應自己輸入正確網址
  - C. 只要確認與該銀行有往來，即表示這封電子郵件沒問題
  - D. 連結郵件中的網址，檢視網頁是否顯示為該銀行，再進行個人資料更新

謝謝聆聽

敬請指教

活動寫真

簽到單

台北海洋技術學院
103學年度資訊安全暨智慧財產權教育講座

活動時間：104年5月22日下午1點至4點
活動地點：士林校區 行202電腦教室
主辦單位：圖資中心網路組、資訊組　　參加人數：　　人

序號	單位	姓名	簽名	備註
1	時尚系	徐珮清		
2	環安衛組	郭正中		
3	運休系	黃致豪		
4	輪機工程系	張靜怡		
5	圖資中心	蔡慧貞		
6	食品系	李嘉展		
7	海觀系	江[illegible]潔		(室代)
8	航海系	鄧純敏		
9	輪機系	歐陽寬		
10	運休系、	邱玉惠		
11	食品系	林雅惠		
12	餐管系	黃世浩		
13	課註組	李瑜		
14	餐管系	戴德和		
15	食品系	任曉晶		

序號	單位	姓名	簽名	備註
16	食品系	林雪良	林雪良	
17	食品系	吳雅蓉	吳雅蓉	
18	海觀系	童宜淳	童宜淳	
19	海觀系	簡明亭	簡明亭	
20	食品系	張恭銘	張恭銘	
21	食品系	林玉惠	林玉惠	
22	食品系	胡秀媛	胡秀媛	
23	進修部	邱宣蓉	邱宣蓉	
24	健照系	沈仲銘	沈仲銘	
25	課指組	劉品伶	劉品伶	
26	數遊系	陳國輝	陳國輝	
27	餐管系	田侑傑	田侑傑	
28	海觀系	蔡承賢	蔡承賢	
29	〃	張佳蓁	張佳蓁	
30	〃	江秀英	江秀英	

序號	單位	姓名	簽名	備註
31	航海系	李宏丰	李宏丰	
32	〃	梁雨薇	梁雨薇	
33	教務處	蔡昊婧	蔡昊婧	
34	主管室	徐軍蘭	徐軍蘭	
35	~~通識部~~	~~邱宏基~~	~~邱宏基~~	離職
36	總務處	林金保	林金保	
37	輪訓中心	陳怡如	陳怡如	
38	航海系	李海清	李海清	
39	輪訓中心	林百銘	林百銘	
40	輪訓中心	洪銘澤	洪銘澤	
41	圖資中心	王漢狄	王漢狄	
42				
43				
44				
45				