主機安全防護
與
駭客手法分析

新波科技
劉楨民
02-2331-0789
0932-212-913

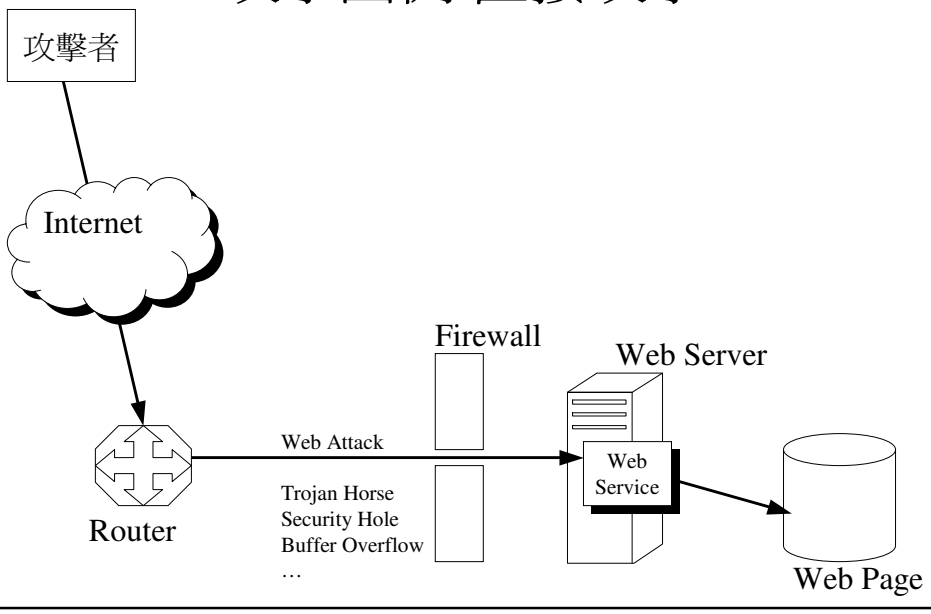
主機安全防護 與 駭客手法分析

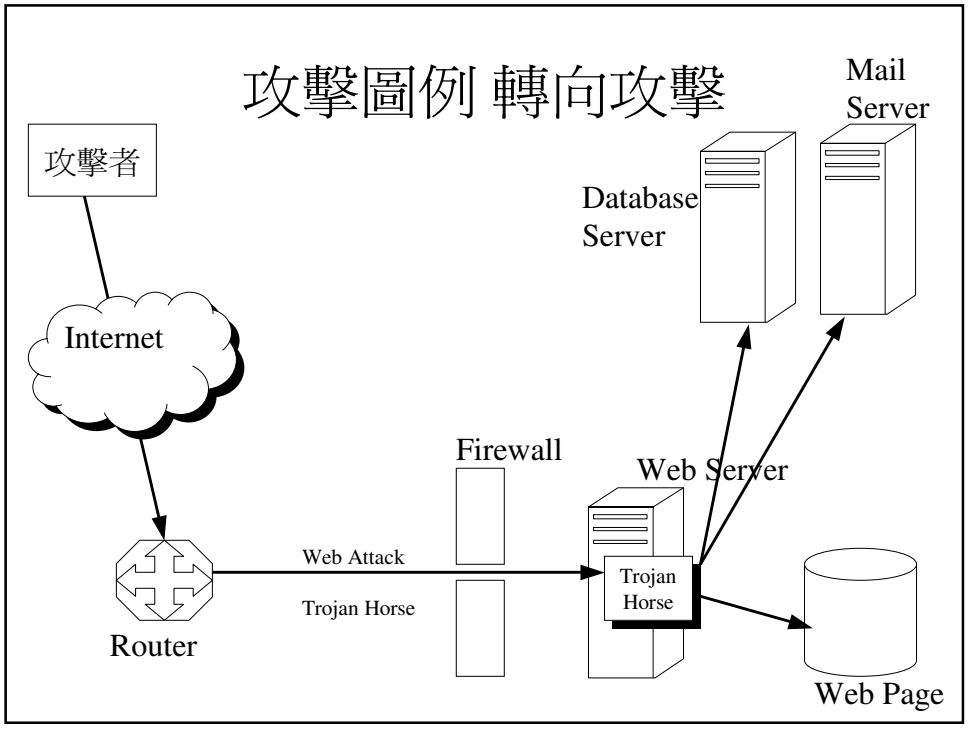
- **網路安全的重要觀念**
- **網路攻擊分類圖例**
- **網站面臨的網路攻擊手法分析**
- **安裝(設定)網站主機的步驟**
- **主機防護的檢核清單**
- **網站漏洞的範例介紹**
- **撰寫安全網頁程式碼的範例**
- **假設已知漏洞以外，還有未知漏洞**
- Q&A

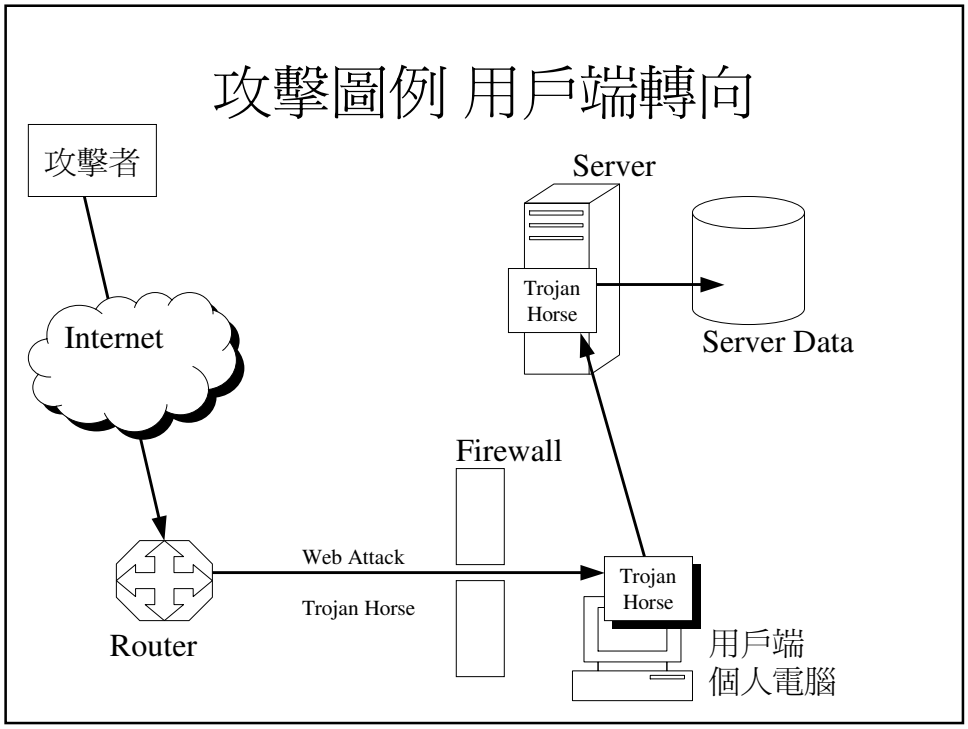
網路安全的重要觀念

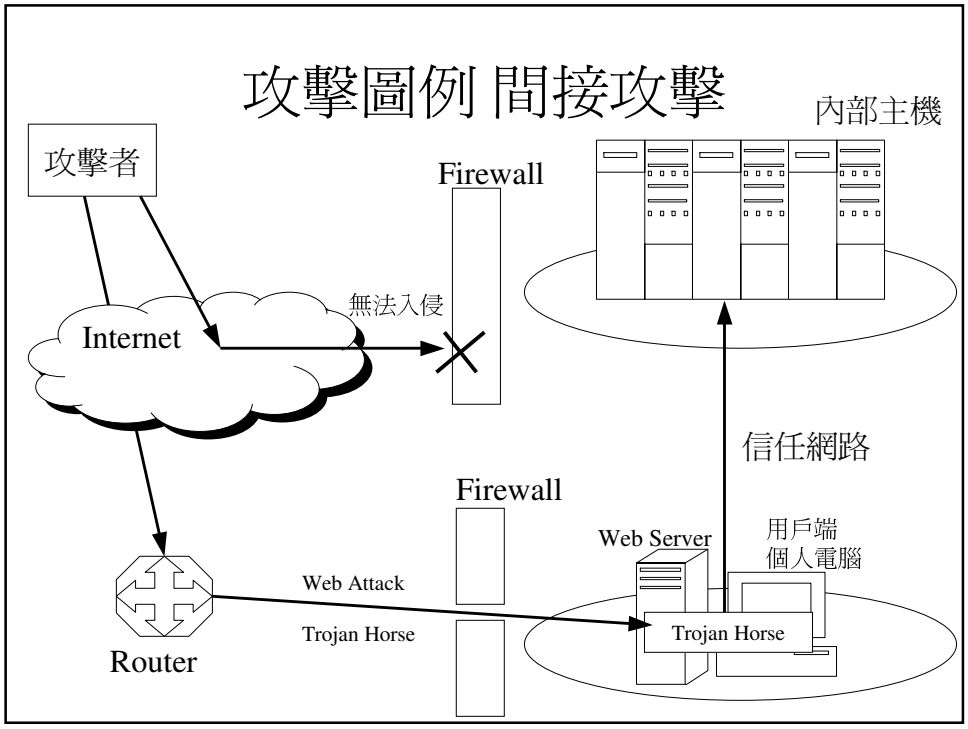
- 網路攻擊經常發生，這是常態。
- 已知的攻擊模式，可以有效地防護。
  - 防毒軟體，入侵偵測(IDS)，入侵防護(IPD)
- 未知的攻擊模式，無法完全被偵測。
  - 安全政策，Firewall政策，封包分析
- 『 主機端安全』與『用戶端安全』需兼顧。
- 沒有絕對安全的軟體，只有安全的設定。
- 『網路安全』與『網路便利』是天秤的兩端。
- 『中病毒』與『中木馬』的差異
  - 相同處：都是系統漏洞與安全問題
  - 差異處：自然感染與人為侵入

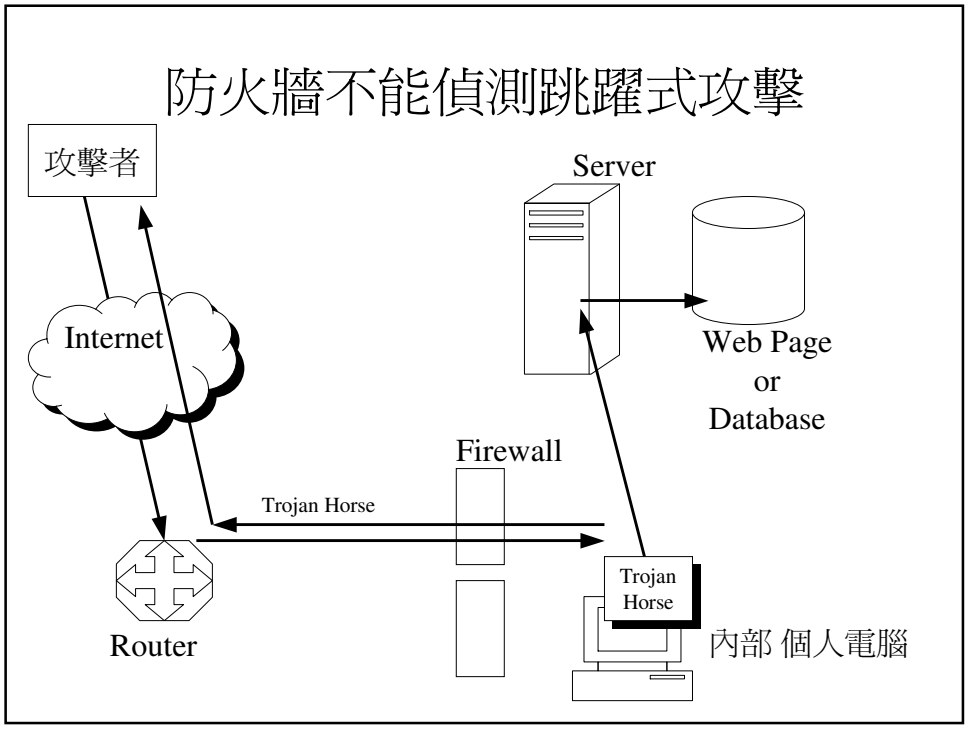
攻擊圖例 直接攻擊











網站面臨的網路攻擊手法分析 1

- Password Attack
  - 後台管理介面，暴力式或字典式密碼攻擊。
- SQL-Injection
  - 資料庫命令碼隱藏在網頁參數後，傳回網站。
- Cross-Site Script
  - JavaScript或其他HTML-Script，隱藏在網頁參數後，傳回網站。
- Directory Traversal
  - 網站服務設置錯誤，造成用戶端可以直接從網站主機，讀取目錄檔案的清單列表。
- HTTP Service Exploit
  - 網站服務的內部漏洞，通常是Buffer-Overflow, 緩衝溢出。
- Cookie/Session Hijacking
  - 用戶端自行修改Cookie或Session值，欺騙主機，取得他人權限。
- DDoS of HTTP service
  - 同時間向網站主機傳送大量讀取網頁，或連接要求。
- XML-Injection, HTTP-Injection

網站面臨的網路攻擊手法分析 2

- Password Attack
  - 後台管理介面，暴力式或字典式密碼攻擊。
- SQL-Injection
  - 取得後台管理身分，置換網頁，傳送木馬程式，修改資料庫內容，執行DOS指令等等。
- Cross-Site Script
  - 誤導用戶端，執行錯誤網頁內容，進行假網站的中間人攻擊。
- Directory Traversal
  - 取得網站目力資訊與後台管理程式碼。
- HTTP Service Exploit
  - 傳送木馬程式，感染網路蠕蟲，置換網頁。
- Cookie/Session Hijacking
  - 偽裝用戶端，取得個人敏感資料，或是取得後台管理身分。
- DDoS of HTTP service
  - 網站服務癱瘓，或是網路通訊緩慢。
- XML-Injection, HTTP-Injection

網站漏洞的範例介紹 1

- 漏洞名稱 : SQL-Injection
- 漏洞範例 (ASP 程式碼)

0 . 直接使用前端輸入的資料，沒有過濾檢查其內容，是否有異常資料。

```
1 . strUserInput=request.form(“UID")
2 . SqlCmd="select password from usr where UserID='"& strUserInput &"'"
3 . set rs1=cn.execute(SqlCmd)
    :
    :
    :
```

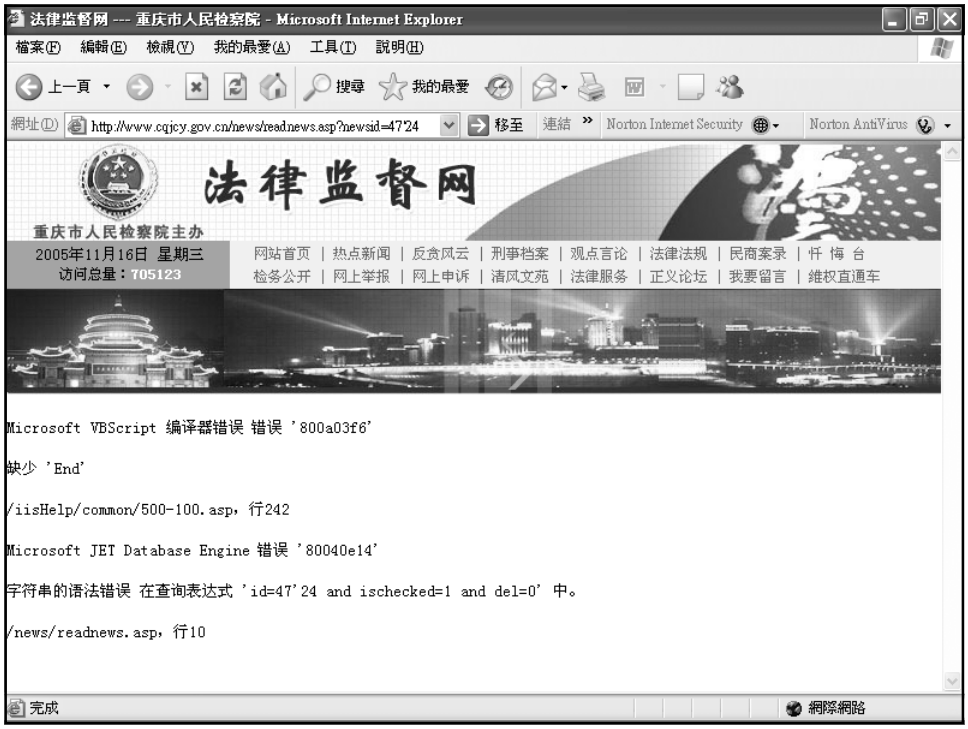
網站漏洞的範例介紹 1

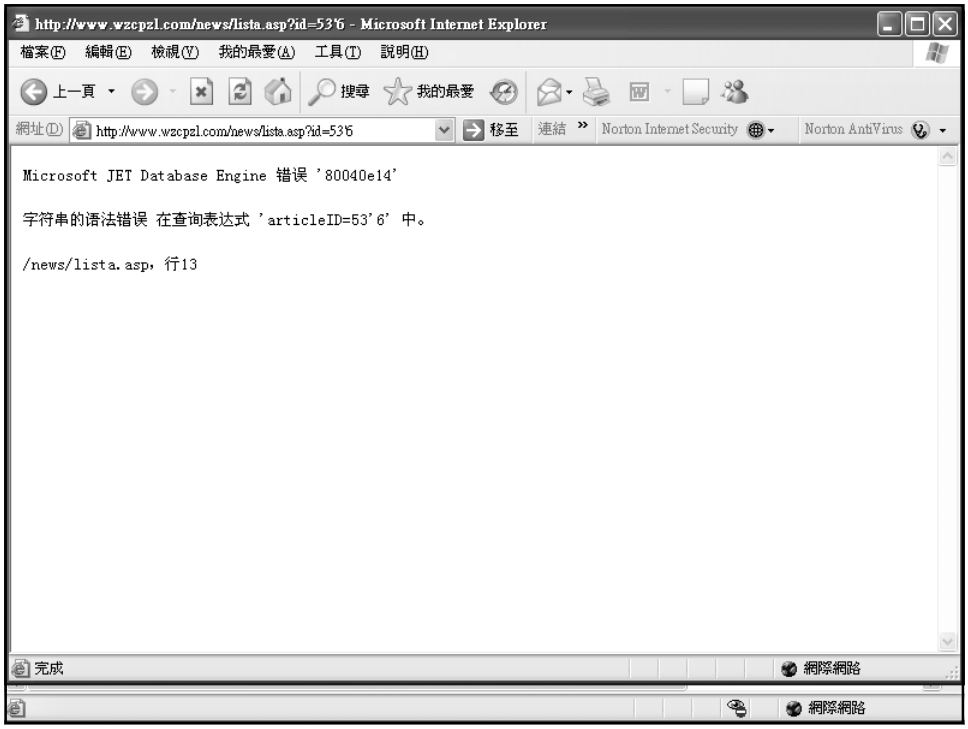
- 漏洞名稱 : SQL-Injection
- 漏洞範例 (ASP 程式碼)

```
1 . <!--#include file=conn.asp-->
2 . <%
3 . username=request.form("username")
4 . password=request.form("password")
5 . sql="select * from my_webUser where userCode='"&username&"' and
    userPassword='"&password&"' and userType=1 "
6 . set rs=conn.execute(sql)
    :
    :
    :
```


網站漏洞的範例介紹 1

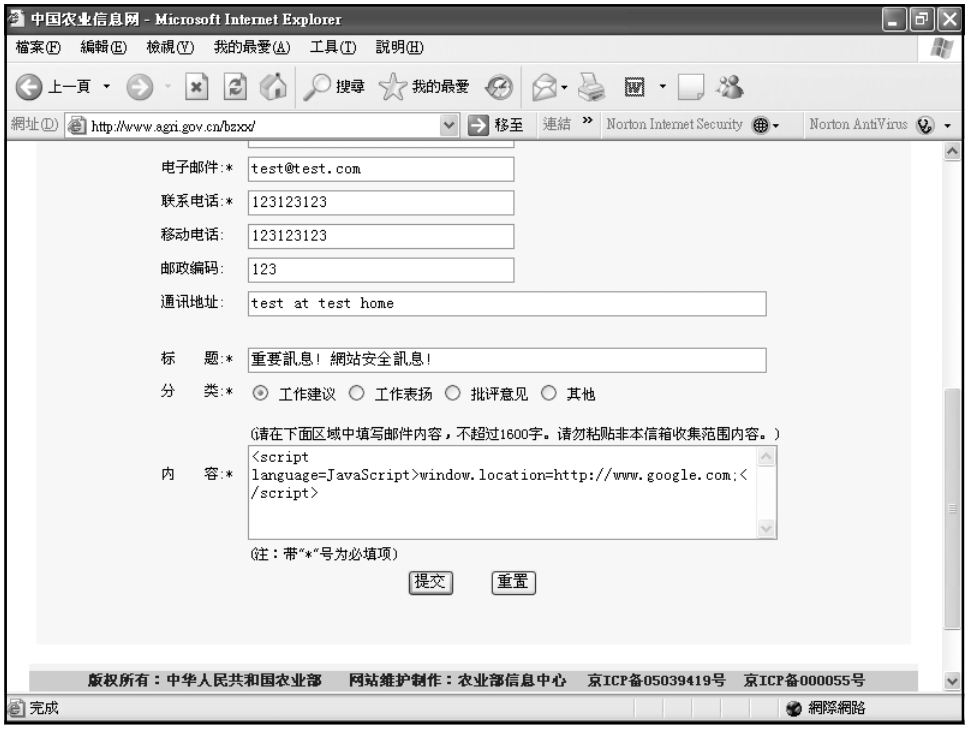
- 漏洞名稱 : SQL-Injection
- 漏洞範例
  - http://www.abc.gov/admin/login.asp?UID=admin&PWD=test1234
  - http://www.abc.gov/admin/login.asp?UID=admin&PWD=‘ or ‘’=‘
  - http://www.abc.gov/ShowNews.php?Item=2&Detail=100
  - http://www.abc.gov/ShowNews.php?Item=2&Detail=100’ ;-- Select * from user where UID=‘admin’





網站漏洞的範例介紹 2

- 漏洞名稱 : Cross Site Script
- 漏洞範例
  - http://host/phpmyadmin/index.php?pma_username=&pma_password=&server=1&lang=en-iso-8859-1&convcharset=\"><script>alert(document.cookie)</script>
  - http://host/phpmyadmin/index.php?pma_username=&pma_password=&server=1&lang=en-iso-8859-1&convcharset=\"><h1>XSS</h1>



網站漏洞的範例介紹 3

- 範例：某網站同時有SQL-Injection與XSS
- http://demo.siteenable.com/content.asp?contenttype=%3Cscript%3Ealert(document.cookie)%3C/script%3E
- http://demo.siteenable.com/content.asp?do_search=0&keywords=contact&page_no=2&sortby=;SELECT%20* FROM blablabla--

網站漏洞的範例介紹 3

- 範例 : SonicWall SOHO/10, Firmware: 5.1.7.0 , ROM-Version: 4.0.0

- GET 攻擊方式, 在 IE 輸入下列URL資料
  - http://192.168.168.168/<script>alert("Its not magic... its a sonicWall")</script>
- POST 攻擊方式

```
POST 192.168.168.168:80/auth.cgi HTTP/1.0 ↓
Accept: */* ↓
Referer: http://192.168.168.168/auth.html ↓
Accept-Language: de ↓
Content-Type: application/x-www-form-urlencoded ↓
Proxy-Connection: Keep-Alive ↓
User-Agent: BadGuy ↓
Host: 192.168.168.168 ↓
Content-Length: 160 ↓
Pragma: no-cache ↓
 ↓
uName=</TD><script>alert("Its not magic... it's a
    sonicWall")</script>&pass=NiceTry&Submit=Login&
clientHash=bbe63bb858b02e741d2d12023ee350a1 ↓
```

資安防護建議

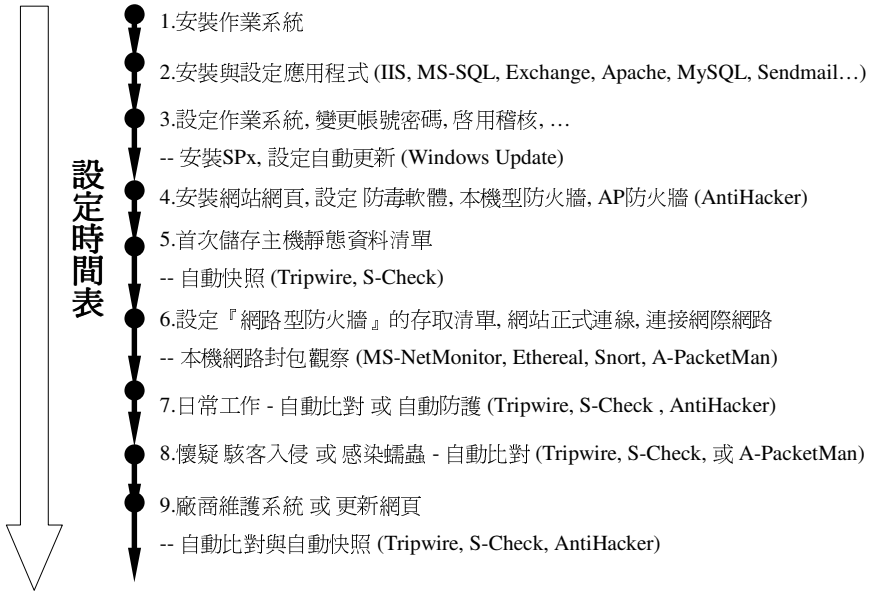
撰寫安全網頁程式碼的範例

- 1. 在ASP/PHP程式碼中，過濾參數字串
  - strData = replace([\&;\`'\\\|"*?~<>^\(\)\[\]\{\}\$\n\r])/\\$1/g;,"")
  - strUsername = replace(trim(request.Form("UID")),"'","")
  - strPassword = replace(trim(request.Form("PWD")),"'","")
- 2. 如果是數值，請先轉換爲 cint(字串)
- 3. 如果要儲存前端資料(留言版或是討論區)，請使用替代字元。
  - ‘ 轉換爲 &squo;
  - “ 轉換爲 "
  - < 轉換爲 <
  - > 轉換爲 >
  - & 轉換爲 &
  - ? 轉換爲

撰寫安全網頁程式碼的範例

- 4. 小心後台管理介面的帳號密碼，不要使用簡單密碼，尤其高階主管。
- 5. 網站主機要區分管理權限，維護權限與資料權限。
- 6. MS-SQL的任何帳號，密碼需爲6位以上。
- 7. 對外主機應停用網路芳鄰，遠端遙控(VNC, pcAnywhere, TerminalService, 等等)
- 8. 對外主機一定要裝設防火牆(本機與網路兩種)
- * . ASP網頁記得要關閉RecordSet (與安全無關)
  - rs.close
  - Set rs = nothing

設定時間表



安裝(設定)網站主機的步驟

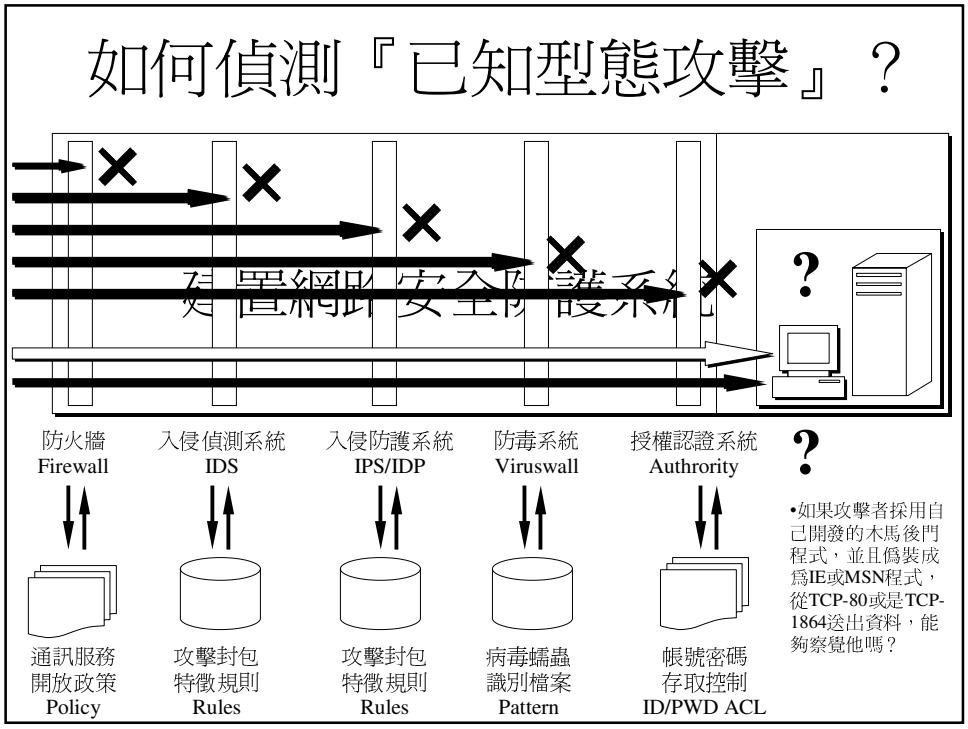
- **訣竅 1：不要採用安裝預設值**
  - administrator, sa, 目錄, …。
- **訣竅 2：請假設系統有漏洞，防衛系統失效**
  - 逐層防衛設定，啟動系統稽核，損害分析控制
- **訣竅 3：分層安全防護，團隊討論回報**
  - 網路安全防護，主機安全防護，應用程式防護
  - 制定系統設定紀錄單(病歷表)，填寫網站異動
- **訣竅 4：請假設網頁參數有錯誤(不安全)**
  - 過濾網頁參數內容，減少網頁參數傳送
- **訣竅 5：請假設網路已遭入侵或攻擊**
  - 檢查主機存取操作紀錄，事件檢視紀錄，
  - 檢查網路封包通訊，有無異常網路通訊。

主機防護的檢示清單

- 這部主機的功能用途？
  - Web？Mail？DNS？Database？
- 它應該提供的網路服務？
  - HTTP(TCP-80)
  - SMTP/POP3(TCP-25,TCP-110)
  - DNS(UDP-53,TCP-53)
- 它所提供網路服務的對象？
  - LAN？DMZ？WAN？單獨對象的IP位址？
- 主機資料維護方式？
  - FrontPage？FTP？Terminal Service？
  - pcAnyWhere？WinVNC？
- 主機資料備份方式？
  - Data-Backup？Disk-Backup？

假如 已知漏洞以外，還有未知漏洞

- **未知型態攻擊的來源**
  - 1.內網用戶自行安裝(下載)軟體
  - 2.內網用戶蓄意破壞(非法建置網站)
  - 3.某種未知攻擊模式正在蔓延...
- **防護方式1: 入侵偵測與防毒軟體**
  - 採用負面表列偵測方式，需要快速更新攻擊特徵檔案(病毒碼)。
- **防護方式2: 防火牆與網頁存取限制**
  - 採用正面表列方式，限制可以存取的網路服務有哪些項目。
- **訣竅 4 :防護方式3: 定時定期，隨機抽樣監控網路封包現況，觀察有無異常通訊。將該通訊阻斷，並且從電腦移除異常程式。**



如何進一步學習封包分析技巧與累積經驗?

- 異常網路封包的危害判斷準則
  - 先排除所有已知的標準通訊協定, HTTP/SMTP/POP3/DNS/CIFS/MSN…
  - 內網或外網 (通訊雙方的IP位址是否爲Internet位址?)
  - 允許或開放 (這類網路服務是否可以執行?)
  - 單向或雙向 (通訊雙方有無互相傳送資料?)
- 異常通訊的蒐證與分析步驟
  - 標示 (標示位址或是標示封包內容)
  - 複製 (將已經標示顏色的封包, 複製到 特殊封包視窗)
  - 顯示 (切換顯示畫面爲 特殊封包視窗)
  - 統計 (option, 如果要進一步瞭解攻擊來源或是受害對象)

Q&A

新波科技
劉楨民
0932-212-913

