第八章

入侵網頁伺服器

網頁伺服器

- 常見的網頁伺服器：

（1）阿帕契（Apache）網頁伺服器

（2）微軟 IIS 網頁伺服器

（3）昇陽（Sun ONE）網頁伺服器

網頁伺服器的運作

1.瀏覽器分割網址（URL）成為三個部分：

（1）協定

（2）伺服器名稱

（3）檔案名稱

2.瀏覽器會先與名稱伺服器（DNS）通訊，轉換網址成為IP位址，因為網際網路的運作實際是以IP進行。

3.因為URL沒有指定目的地Port，依據預設，網頁伺服器的Port是80。

網頁伺服器的運作

4.接著瀏覽器會建立一個TCP的連接，這連結的目的地就是DNS轉換出來的IP位址，Port是80。

5.依據HTTP協定，瀏覽器會先送出一個需求給伺服器，這個需求對伺服器要求一個具有HTML格式的網頁檔案。

網頁伺服器的運作

6.伺服器依據需求，送回HTML格式的網頁文件給瀏覽器。

7.瀏覽器讀取HTML，並且依據HTML語法中的標籤（tags）來解譯網頁內容，並在瀏覽器的視窗中顯示此網頁。

網頁伺服器的威脅

（1）網頁伺服器的錯誤設定。

（2）網頁伺服器漏洞、弱點或臭蟲。

（3）網頁伺服器使用預設值進行安裝。

（4）安全政策或維護程序的缺失。

（5）網頁伺服器管理者的帳號被取得。

網頁伺服器的威脅

（6）阻斷服務攻擊（DoS）。

（7）SQL注入（Injection）。

（8）DNS或URL毒害。

（9）Cookie 被利用。

（10）使用Telnet或SSH入侵。

網頁伺服器出現過的弱點

- **Apache弱點**

- Win32的Apache 1.3.20，如果將一個較長的URL傳遞給Apache模組（mod_negative、mod_dir、mode_autoindex）會造成Apache列出路徑的內容。

- 例如： /cgi-bin ////////////// / // / / / / / // / / /

網頁伺服器出現過的弱點

- IIS弱點

- ::$DATA vulnerability
- showcode.asp vulnerability
- Piggy backing vulnerability
- Privilege command execution
- Buffer Overflow exploits（IIShack.exe）

常見的 IIS 弱點

（1）IIS的主要伺服器程序inetinfo.exe是依賴一堆的DLLs來共同執行工作，以提供多種不同的能力，例如提供server side scripting、content indexing、webbased printing等等功能。但是這樣的架構也提供了攻擊者能透過具有危害性的輸入，進行不同形式的入侵行為。

（2）另一個很有名的安全性弱點，是在ISAPI DLLs上的Buffer Overflow。這個ISAPI filter掌控了Internet Printing Protocol（IPP）列印檔案的支援。該弱點是當緩衝區塞入的字元接近420 bytes且被送到HTTP主機時發生，例如：

GET /NULL.printer HTTP/1.0
HOST: [buffer] ← 輸入 420 個 A

緩衝區溢位（Buffer Overflow）

- 緩衝區溢位是因為程式設計者在設計讀取輸入值時，忽略了要檢查輸入資料的長度。
- 在一般的程式中，輸入資料的緩衝區是一個固定長度的資料，如果使用者輸入了大於緩衝區長度的資料時，就會產生所謂的緩衝區溢位。
- 現在有相當多的漏洞都是因為緩衝區溢位造成的。

常見的 IIS 弱點

（3）IIS路徑追蹤（Directory Traversal）這個弱點起因於CGI scripts及ISAPI延伸名稱的拆解錯誤，例如“%c0%af”及“%c1%9c”對網址中?/?及?\?的網址表示法是過長的，如果把這資料當做需求，送給IIS網頁伺服器，將會有意想不到的後果。在GET後面接著%c0%af這樣的字串送給IIS，而且後面還下了任意的命令，結果可能造成這命令可透過IIS伺服器直接執行。

GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir=c:\ HTTP/1.0

常見的 IIS 弱點

（4）在Microsoft IIS 4.0及5.0曾發生Unicode的問題，ASCII中的逗點字元碼被換成Unicode碼的「%2E」。ASCII中斜線字元會被換成Unicode碼的「%c0%af」。Unicode 2.0允許每個字元有多種編碼的可能。例如：Unicode的「/」可以是2f, c0af, e080af, f08080af, f8808080af, ...。

- 過長的Unicode並不是畸形的，但是對一個正確的Unicode編碼器（encoder）與解碼器（decoder）來說，過長的碼卻是不允許的。惡意的使用這種過長的碼，可能會繞過IIS的過濾器，因為過濾器只檢查短的Unicode。

常見的 IIS 弱點

（5）WebDAV / ntdll.dll弱點，WebDAV的全名是「Web-based Distributed Authoring and Versioning」。

- 這是讓用戶端能發行及管理Web上的資源，使得使用者們得以經由網頁共同編輯整理檔案資料。IIS WebDAV元件在處理進入WebDAV的需求時，會使用ntdll.dll這個動態連結庫。
- 藉由送出一個特殊手法的WebDAV需求給IIS 5.0伺服器，攻擊者可以在系統上執行特定的程式碼，甚至取得系統的控制權。

常見的 IIS 弱點

（6）RPC DCOM弱點，這是一個重要的服務，被很多應用程式使用，它存在於Windows Component Object Model（COM） subsystem中。DCOM服務允許COM物件與另一個網路上的物件通訊。且在Windows NT、2000、XP及2003上預設都是開啟的。

攻擊者可以透過以下的Port存取COM的弱點：

- TCP及UDP ports 135（Remote Procedure Call）
- TCP ports 139及445（NetBIOS）
- TCP port 593（RPC-over-HTTP）
- 任何IIS HTTP/HTTPS port，如果COM的網際網路服務是打開的。

常見的 IIS 弱點

（7）ASN（Abstract Syntax Notation）是用來表現不同的二元資料型態，例如數字或文字檔的字串。主要是用於程式開發上的一個標準，很多的廠商在產品上的開發都是依循ASN.1標準。

- 攻擊者可以使用ASN.1的弱點執行一個能讓主機重新開機的程式，這樣形同造成阻斷服務攻擊。

常見的 IIS 弱點

（8）IIS Logs的資訊洩漏，IIS會記錄所有的訪客資訊在log檔中，只要沒有使用Proxy，訪客的IP就會被記錄下來，這個檔案是位於 <%systemroot%>\logfiles。

以下這個命令有可能會列出log檔：

http://目標主機網址
/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1

系統更新

- Hotfix是修正產品中錯誤的程式碼，使用者也許會經由不同的途徑，被廠商通知要安裝Hotfix。Hotfixes有時候是一堆修正軟體的集合，稱之為combined hotfix或service pack。

- Patch可以視為是程式問題的修補工作，可以立即提供給使用者的解決方案。

Patch management

- Patch management是用來確認適當的Patch是否正確的安裝在系統上的程序，其工作包含以下項目：

1. 選擇、核對、測試及套用Patch。
2. 在先前套用的Patch上套用最新的Patch。
3. 列出現在軟體上套用的Patch。
4. 指定及派送套用的Patch。

對策：網頁伺服器

- 使用防火牆。
- 改變administrator此帳號的名稱。
- 關閉預設的網站路徑及FTP。
- 移除伺服器不使用的應用程式。
- 在伺服器設定檔中，關閉從網頁進行網站目錄瀏覽與檢視的功能。

對策：網頁伺服器

- 檢查表單及查詢字串中的惡意輸入。
- 關閉遠端管理。
- 對作業系統與伺服器軟體套用最新的Patch、Service Packs、Hotfix。
- 在伺服器中放置對攻擊者的警告宣言。
- 在HTML中，將表單中內負責送資料給伺服器的GET敘述換成POST敘述。

Get與Post的差別

1、Get會將表單中的資料，按照「？變數1=值&變數2=值」的格式，附加到URL後面。而Post是將表單中的變數與資料放在表單的本體中，按照變數和值相對應的方式，傳遞到Action所指的URL。

2、Get是不安全的，因為在傳輸執行過程中，資料被附加在URL上，這樣就可能會有一些隱私的資訊被看到。Post的所有變數則都是不可見的。

3、Get能夠傳輸的資料量很小，主要是因為受限於URL的長度限制，而Post可以傳輸大量的數據，所以如果要上傳檔案，只能使用Post。

4、Get會限制Form表單的變數值必須為ASCII字元，而Post無此限制。

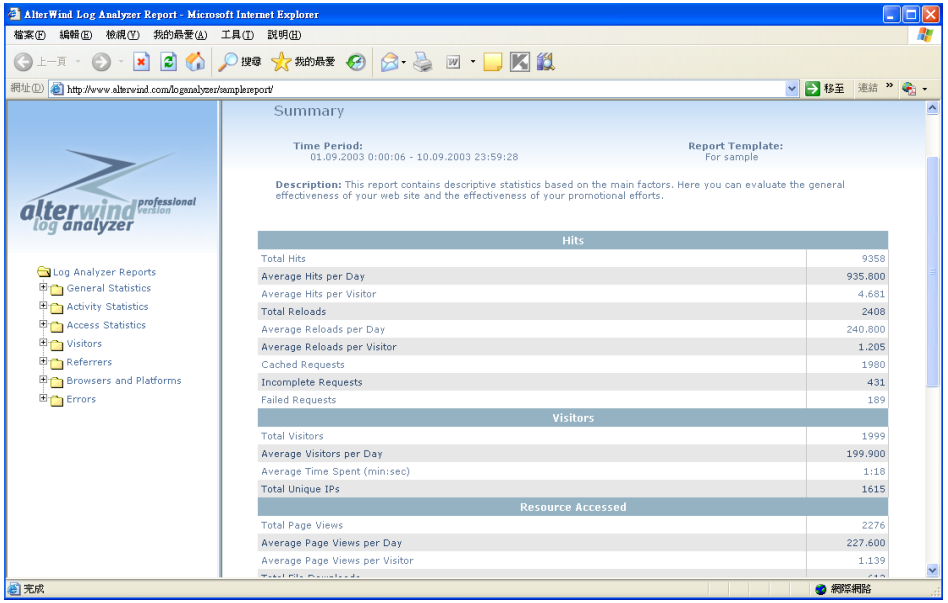
對策：檔案系統追蹤

1. 微軟建議設定NTFS ACL只在cmd.exe及幾個重要的執行檔案上才給予管理者等級的系統控制權限。
2. Sample檔案必須被移除。
3. 監督log檔。
4. 經常性套用微軟的patches及hotfixes。

工具

- **AlterWind Log Analyzer**

- 可以抓取web server的logs同時建立圖形化的報表，包括使用統計、流量...等等，可透過網頁的方式查詢，並提供了一個包含了數百個搜尋引擎的資料庫。



工具程式

- **CleanIISLog**

- CleanIISLog能夠很容易的清掉在IIS的W3SVC下的日誌檔案中指定的IP項目，和其他工具相比有以下不同點：

1、可以清除指定的IP連接記錄，保留其他IP記錄。

2、當清除成功後，CleanIISLog會在系統日誌中將本身的記錄清除。

CleanIISLog

- CleanIISLog <LogFile>|<.> <CleanIP>|<.>

<LogFile>：指定要處理的日誌檔，如果指定為「.」，則處理所有的日誌檔（注意：處理所有日誌檔需要很長的時間）。

<CleanIP>：指定要清除的IP記錄，如果指定為「.」，就是清除所有的IP記錄。

工具程式

- **cacls.exe**

- Windows 2000內建的cacls.exe可以全面性的設定存取控制清單（ACLs）的權限。可改變所有可執行檔的權限為System:Full，Administrators:Full，讓管理者擁有所有檔案的權限。

C:\>cacls.exe c:\myfolder*.exe /T /G System:F Administrators:F

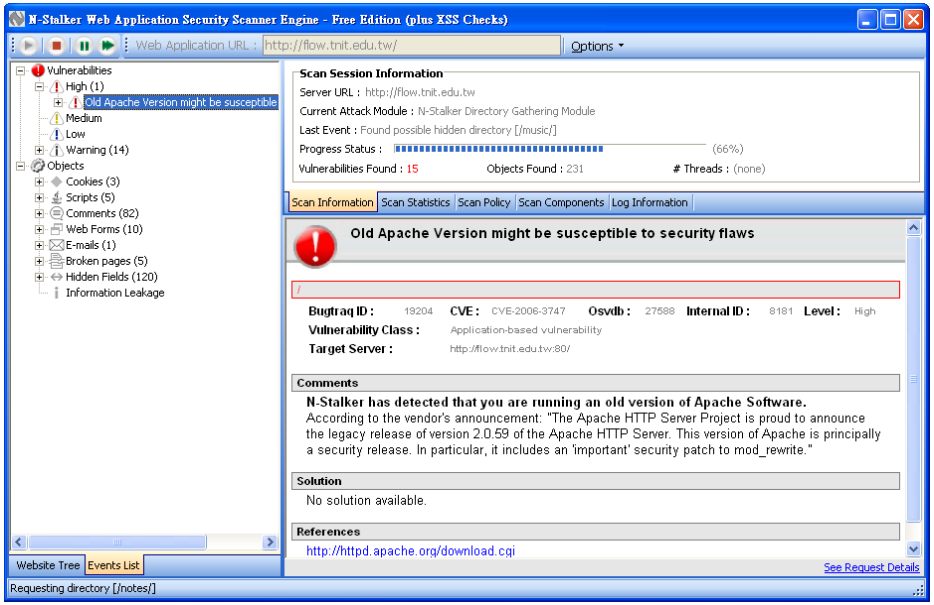
工具程式

- **N-Stealth HTTP Scanner**

- N-Stealth是一個功能完整的Web弱點掃描軟體，能在Windows XP/2003系統下正常地運行，幾乎可掃描所有的伺服器，檢測超過35000個有關HTTP及HTTPS的安全性議題，包含服務應用程式（如CGI、ColdFusion、ASP、Lotus Domino、FrontPage、PHP等）。

N-Stealth HTTP Scanner

- 能避開IDS（入侵測試系統）捕捉的功能，把掃描結果寫入一個HTML、文字檔或PDF格式的報表中，也可以使用電子郵件進行警告通知（正式版功能），N-Stealth通常被用來做為對網頁伺服器進行弱點稽核及滲透測試。



工具程式

- **IISLockdown**

- IISLockdown可以限制匿名（anonymous）帳號存取系統及寫入Web目錄的能力，也可以關閉WebDAV，並且會安裝URLScan ISAPI的過濾程式。

工具程式

- **URLScan**

- URLScan是一個安全性的工具，能基於管理者設定的規則，將Server所有的進入需求進行過濾。

練習

1. 下載N-Stealth HTTP Scanner免費（Free）版本。（可能需要填寫資料）
2. 安裝N-Stealth HTTP Scanner。
3. 更新偵測資料庫，並重新啟動。
4. 選擇一台適當的網頁伺服器（單位或組織內的）。
5. 偵測這台網頁伺服器。
6. 依據N-Stealth HTTP Scanner報表，說明這台伺服器有哪些弱點，以及如何補強這些弱點。