2013年4月12日 星期五

緩衝區溢位攻擊：第一章 - 預備環境與工具

<<< 前言
>>> 第二章 - 改變程式執行的流程
全書目錄

最一開始我們需要先預備環境和工具，從 Windows XP SP3 開始研究對初學者會比較容易，更早以前的 Windows 作業系統，像是 Windows XP SP2 或更早的作業系統，保護的措施做得不夠，如果你能夠了解本書的內容，自行應用到 Windows XP SP2 或者以前的作業系統應該不難，只是現在愈來愈少人使用以前的版本，像是 Windows 98 或者 Windows ME，它們的穩定性都不如 XP，再回頭研究舊版的系統意義不大，所以本書將只包含 Windows XP SP3 版本開始到之後新版的 Windows 系統。
以下是本書會使用到的工具，如果有寫版本編號，代表使用特定版本是需要的，如果沒有特別註明，則一般可以使用最新的軟體版本：

- VirtualBox
- Dev-C++ v4.9.9.2
- Visual C++ 2010 Express
- Visual C++ 2013 Express
- NASM
- OllyDbg
- WinDbg
- Immunity Debugger
- CFF Explorer
- HxD
- Process Explorer
- Metasploit

以下是本書所涵蓋的作業系統，唯一至少需要預備的只有 Windows XP SP3，其他都是選擇性的，等一下我們會提到如何取得 XP SP3 的測試環境：

- Windows XP SP3 x86
- Windows 7 x64
- Windows Server 2008 R2 x64
- Windows 10 x86/x64 (Technical Preview)

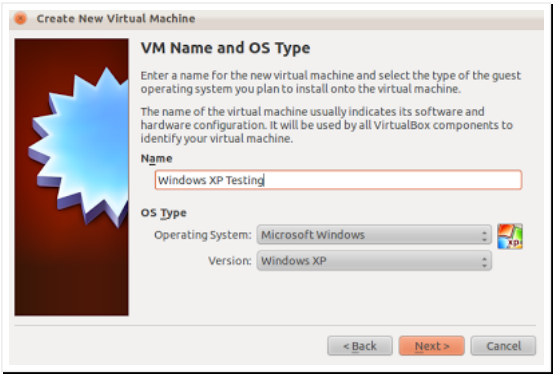
讀者或許會有疑問，為什麼我們需要那麼多的工具軟體？事實上一般駭客的攻擊行動用到的工具軟體可能更多，雖然不是每個行動都會用到所有的工具，但是預備好 自己的工具箱是很重要的概念，對初學者來說比較有挑戰性的是預備 Metasploit 的環境，因為我建議用一個 Linux 的環境來安裝 Metasploit，對沒有碰過 Linux 環境或者不熟悉的人可能會有點怕怕的，其實不用擔心，或者可以這麼看，網安的工作常常要面對未知的環境和問題，所以心臟要習慣練習地大顆一點，面對沒碰過 或者陌生的環境，學習面對心中的抗拒和那一點點潛藏的害怕，困難或未知的事物被理解清楚之後其實也不過就是那樣。

VirtualBox 以及 Windows XP SP3

本書使用的 Windows 是由 VirtualBox 所模擬的虛擬機器，VirtualBox 是免費合法的虛擬機器軟體，相當穩定且效率高，當然如果你有實體的 Windows 平台，或者其他的虛擬機器平台也可以，並不限制一定要用 VirtualBox。 筆者的作業系統為 Ubuntu 11.04，Ubuntu 官方提供的 VirtualBox 不是最新版，筆者建議直接到 VirtualBox 網站下載最新版安裝，安裝過程很直觀，按下幾個確定按鈕之後就完成了，在此不贅述。

如果讀者已經有 Windows XP SP3 的環境，可以跳過此段落，如果沒有，在 2011 年年底以前可以到 NVD (National Vulnerability Database) 網站下 載 Windows XP SP3 的 VHD (Virtual Hard Disk) 檔案，但是該網站在 2012 年以後不再提供 XP SP3 的檔案下載，現在除非是利用市面上買得到的 XP 光碟，或者是到微軟的網站下載，微軟提供 XP 以及 Internet Explorer 6 的測試環境，連結在此， 可以在該頁面找到 Windows_XP_IE6.exe 的檔案下載，大約 300 ~ 400 MB 左右的大小，請留意微軟會定期更新此頁面，並且提供有期限的 XP VHD 檔案讓人下載測試，有期限代表也許今天您下載了這個檔案，一個月過後期限到了就不能再使用了，期限都會註明在網頁上，這一點還請讀者留意，另外，如果未來 此頁面被拿掉了，可以試著用 Google 搜尋 "Microsoft Internet Explorer Application Compatibility VPC Image" 看看，希望微軟會持續提供測試的 XP 環境。

執行 VirtualBox，在介面上按下按鈕 New，或者是按下 Ctrl+N 新增一個虛擬機器，名稱可以隨便取，Operating System (作業系統) 選擇 Microsoft Windows，Version (作業系統版本) 選擇 Windows XP，如下圖：

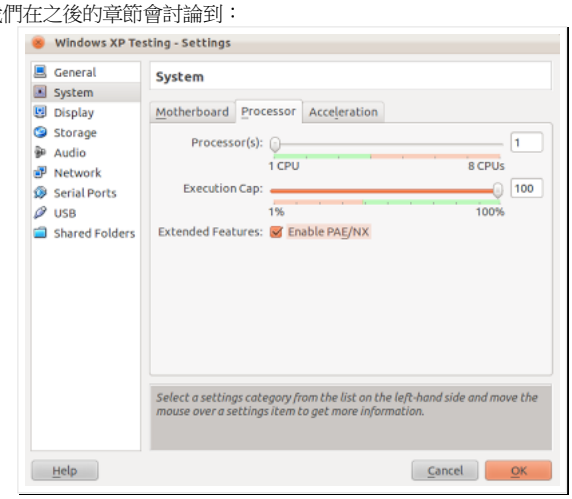


接下來選擇虛擬機器的記憶體大小，原則上 Windows XP 使用大約 512 MB 即可。

接下來要配置硬碟檔案，請選擇 Use existing hard disk，並且選擇您的 XP VHD 硬碟檔案，以下假設此硬碟檔案名稱為 "fdcc-xp Hard Disk.vhd"，如果讀者執行此步驟的時候跳出 UUID 已經重複的錯誤訊息，可以在電腦裡面或者 VirtualBox 的安裝資料夾下面找到執行程式 VBoxManage，並且執行下面指令來改變 UUID，'fdcc-xp Hard Disk.vhd' 是檔案名稱，請讀者依照自身的情況適當地修改：

```
VBoxManage internalcommands sethduuid 'fdcc-xp Hard Disk.vhd'
```

按下 Create 按鈕之後應該就完成了，唯一要注意的是，在真的執行虛擬機器之前，我們必須先修改一項虛擬機器的設定，在虛擬機器的設定選項裡面，找到 System | Processor 的相關設定，也就是中央處理器的相關設定，如下圖，請在 Enable PAE/NX 的地方打勾，這代表啟動硬體 DEP 功能，關於硬體 DEP 我們在之後的章節會討論到：



其他虛擬機器的相關設定請自行參考官方網站的文件，到這裡應該就可以使用這個 Windows XP 的測試環境了。

Dev-C++ v4.9.9.2

Dev-C++ 是相當「穩定」的 C 和 C++ 語言編譯器，雖然版本已經有很多年沒有更新了，但也因為這樣，所以沒有加入比較新的安全保護機制，很適合拿來作初學者的工具，另外它的消耗資源小，所以在我們的虛擬機器上面執行起來也滿順的，建議直接到其SourceForge網站下載 v4.9.9.2 版本，程式有中文介面，但是為了便於統一說明，本書使用其英文的介面，安裝方式也很容易，執行安裝檔案並且按下幾次的確定即可安裝完成。

針對學習程式設計，我並不是要推薦 Dev-C++，事實上 Dev-C++ 針對程式設計這個目的來說並不是一個合適的工具，因為它太「穩定」了，太久沒更新了，而且偵錯的介面容易出問題，即使是自己手動更換編譯器也是一件麻煩的 事，但是對於學習緩衝區溢位來說，Dev-C++ 是非常合適的解說工具，因為它編譯出來的東西比較單純，所以很容易解釋，當然在我們熟悉了基本觀念之後我們就會跳到比較時尚的 Visual C++，也會實際探討一些現實世界的例子，也就是當你連對方編譯器或者編譯參數是什麼都不知道的情況下，要怎麼掌握網路攻擊的資訊，這些都是我們會去探討的。

Visual C++ 2010 Express

Visual C++ 2010 Express 是微軟推出的免費程式編譯軟體，因為本書會講解如何突破編譯器所提供的保護機制，因此我們需要用一套能夠完整提供各樣保護機制的編譯器，在 Windows 的環境下，目前免費又最新的編譯軟體就是微軟本身所提供的 Visual C++ 2010 Express 了，可以到微軟的網站下 載並且安裝，可以選擇安裝中文版，不過為了統一解說方便，本書的範例是使用英文的介面，過程中可以選擇向微軟的網站註冊自己的電子郵件，並且微軟會依照所 註冊的電子郵件發送對應的註冊金鑰，Express 版本完全是免費的，所以只要註冊自己的電子郵件便可以無限期的使用這套軟體，如果不想註冊的話，在試用期限內也可以自由使用，安裝的過程很容易，也是直觀 的按下幾次確定按鈕即可，在此不贅述。

Visual C++ 2013 Express

同上，Visual C++ 2013 Express 是微軟推出的免費程式編譯軟體，可以到微軟的網站查看新版的 Visual Studio Express，或者直接點這裡下載。請注意，下載必須有一個微軟的帳號，但是註冊是免費的。

本書使用英文的介面。安裝的過程很容易，也是直觀 的按下幾次確定按鈕即可，在此不贅述。

NASM

NASM 是 The Netwide Assembler 的簡稱，是一套免費的組譯器軟體，可以將組合語言組譯成為二進位碼檔案，即便讀者沒有學過組合語言也無所謂，在本書的第二章開始會陸陸續續講解所需要關於 組合語言的知識，在第三章以後我們會漸漸使用到 NASM，並且會附帶許多範例加以說明，NASM 可以在官方網站下載，本書的例子是使用 2.09.10 版本，但是如果後來有更新的版本也可以使用，建議在下載頁面進入 win32 資料夾，直接選擇 installer 檔案來安裝，安裝的過程也很直觀，在此不贅述，唯一值得一提的是，可以在安裝的時候，考慮把安裝路徑設在根目錄下的第一層目錄，例如 C:\nasm，這樣透過 Windows 的命令列模式視窗來下指令的時候會比較方便一點。

OllyDbg

OllyDbg 是一套偵錯軟體，也是免費的，可以在官方網站下載最新版，本書的範例使用的是 1.10 版本，更新的版本應該也可以，但是 1.10 版本是久經測試，被大眾廣泛使用的版本，如果沒有特別理由，建議還是使用 1.10 版，軟體沒有安裝程式，下載壓縮檔案下來之後，建議可以解壓縮放在 Windows 系統內的「我的文件夾」目錄下面，然後將執行檔案設立一個捷徑放在桌面上，一旦執行之後，OllyDbg 會在系統登錄檔案裡面註冊執行程式的路徑，所以建議執行之後就不要將檔案移動位置了。

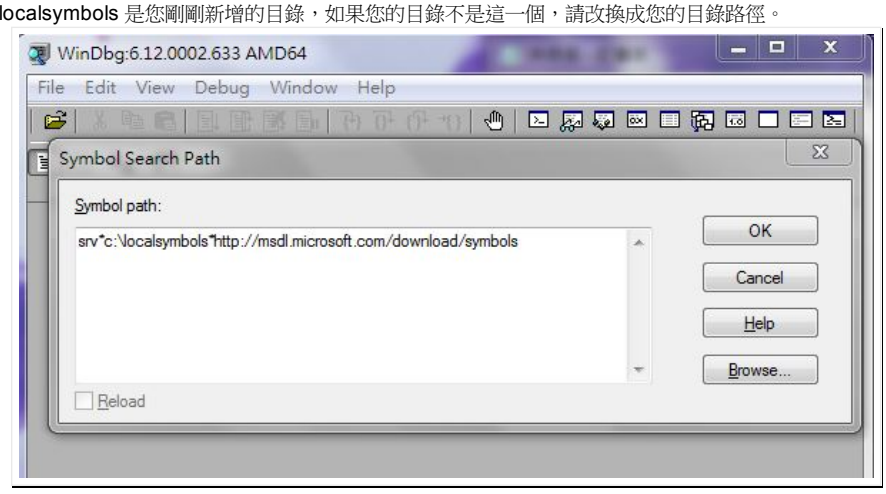
WinDbg

WinDbg 也是一套偵錯軟體，它是微軟內部普遍被使用的偵錯軟體，也是微軟所提供的官方偵錯程式，而且你或許不知道，WinDbg 目前並且相信在可見的未來都有為數不少的程式高手在負責維護並且更新它，WinDbg 的取得方式比較特別，因為微軟政策一直在改變的關係，以前 WinDbg 可以獨立下載安裝，後來被包在 DDK (Driver Development Kit) 裡面，最近又被包在 SDK (Software Development Kit) 裡面，可以在微軟的網站上找到，如果未來網頁的連結失效，讀者可以在微軟的官方網站 www.microsoft.com 搜尋關鍵字 WinDbg 並且找到最新的版本來使用，目前不管是 Windows XP、Vista、Windows 7、或者是 Windows 8，都可以使用 7.1 版的 SDK 裡面所提供的 WinDbg 來偵錯，安裝的時候，安裝程式會檢查是否有 .NET Framework 4.0，請忽略這項提示，因為我們不需要使用 .NET Framework 的功能，另外在選擇安裝項目的時候，請選擇 **Redistributable Packages** 項目下的 **Debugging Tools**，以及 **Common Utilities** 項目下的 **Debugging Tools for Windows**，這樣一來便會安裝完整 x86/x64 的 WinDbg，其他的安裝項目都不需要勾選，但是讀者可以根據自身的需要和喜好來決定是否安裝其他的項目。

安裝完之後，我們要設定偵錯符號檔案，請先決定一個存放下載偵錯符號的目錄名稱，舉例來說：c:\localsymbols，如果此目錄之前不存在，請先 新增它，然後在程式集裡面找到 WinDbg 執行，執行後選擇 File | Symbol File Path ...，或者直接在程式中按下 Ctrl + S 叫出符號設定視窗，輸入：

```
srv*c:\localsymbols*http://msdl.microsoft.com/download/symbols
```

如下圖，請留意 c:\localsymbols 是您剛剛新增的目錄，如果您的目錄不是這一個，請改換成您的目錄路徑。



按下 OK 後結束離開，這樣偵錯符號就設定完成了，之後我們對 WinDbg 的操作都需要連線到微軟的網站，也就是到剛剛輸入的網址 (http://msdl.microsoft.com/download/symbols)去下 載相對應的系統符號，剛剛的設定會讓這些動作自動完成，我們只需要確定操作的時候有網際網路連線就可以了。

Immunity Debugger

Immunity Debugger 也是一套免費的偵錯軟體，因為它整合了 Python 語言的功能，所以有相當方便的外掛程式以供使用，在官方的下載網頁，只要填一些資料便可以下載到程式，資料的填寫並沒有特別檢查正確性或者是格式，所以要求並不嚴格，如果你願意，可以詳細填寫正確的資料，如果不願意，可以隨意填寫任意字串，填完按下 Download 的按鈕就可以下載程式了，安裝的過程也相當簡單，在此不贅述。

CFF Explorer

CFF Explorer 是一套免費的工具軟體，可以用來查看 EXE 檔案的內部格式，讀者可以在官方的網站，選擇下載 CFF Explorer (x86 Version, stand-alone, Zip Archive) 即可，一樣解壓縮完之後便可以直接執行使用，所以建議可以放置在一個固定的資料夾內，然後在桌面

上安置一個捷徑來執行。

HxD

HxD 是以 16 進位格式來讀取或者修改檔案的工具，可以在官方網站找到更多資訊，或者直接到下載頁面下載，對本書而言這項工具是選擇性的，可以考慮安裝，是一套方便的工具軟體。

Process Explorer

Process Explorer 也是免費的工具軟體，可以從 Windows Sysinternals 的網站下載最新版，下載完解壓縮之後，只要執行檔案就可以使用，沒有獨立的安裝程序，所以也是建議固定放置在某處資料夾，並且在桌面上設立一個捷徑方便執行，對本書涵蓋的內容而言，Process Explorer 也是選擇性的不一定要使用。

Metasploit

Metasploit 是一套適合安裝在 Linux 環境的軟體，我們實際要使用的其實是 Metasploit Framework，雖然它也有提供 Windows 的版本，但是建議還是預備一個 Linux 的環境，不管是實體機器，或者是用虛擬機器來運行都可以。
安裝 Metasploit Framework 的話，建議是使用 Git 的方式，Git 的方式會取得目前在開發中的版本，因此也會是最新的版本，因為 Metasploit Framework 開發過程中常常會加入新的資料。所以安裝開發中的版本，並且時常更新，可以確保取得最新的資料。
詳細安裝細節，請參考我寫的一篇教學。

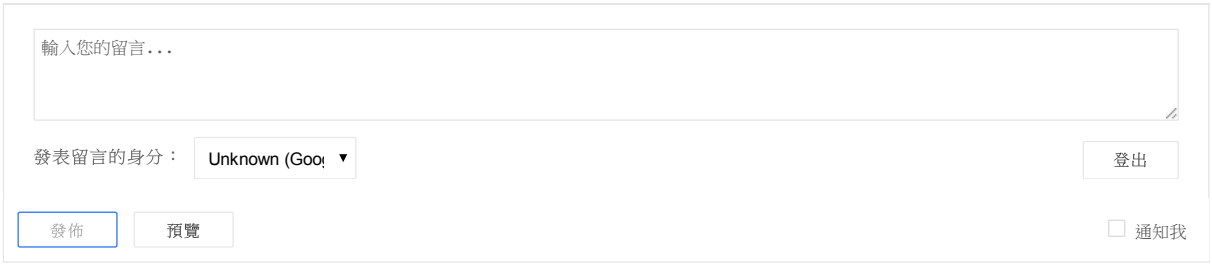
到此為止，我們初步的實驗環境可以說已經預備完成，讀者您準備好了嗎？請翻閱下一章，讓我們一起窺探網路攻防的秘辛...

<<< 前言
>>> 第二章 - 改變程式執行的流程

於 下午7:55 G+1 +2 在 Google 上推薦這個網址
標籤： 網路安全實務, 緩衝區溢位

沒有留言:

張貼留言



較新的文章 首頁 較舊的文章

訂閱： 張貼留言 (Atom)