Introduction

An insight on how to inject a dynamic library (DLL) into a 32 bit process in Windows Vista with the use of Remote Threads and taking into consideration the Address Space Layout Randomization (ASLR). The sample code used is written in assembly language (MASM32) using the WinAsm IDE. It should give you a better understanding on how dynamic libraries can be injected.

Tools

The tools used in this paper are the following:

- WinAsm Studio [http://www.winasm.net/]

Code

injectDLL.asm

```
.486
.model   flat, stdcall
option   casemap :none

include          injectDLL.inc

.code
start:
         invoke   GetModuleHandle, NULL
         mov      hInstance, eax
         invoke   DialogBoxParam, hInstance, 101, 0, ADDR DlgProc, 0
         invoke   ExitProcess, eax

DlgProc  proc hWin        :DWORD,
                  uMsg    :DWORD,
                  wParam  :DWORD,
                  lParam  :DWORD

         .if      uMsg == WM_COMMAND
                  .if      wParam == INJECT
                           invoke GetDlgItemText,hWin,PIDTXT,addr hProcIdb,5; Get PID from txtbox
                           invoke GetDlgItemText,hWin,DLLPATH,addr lib,512          ; Get dll pathname from txtbox
                           invoke InjectDll
                  .elseif  wParam == EXIT
                           invoke EndDialog,hWin,0
;////////////////////////////////////Open File Dialog//////////////////////////////////////////////////////////////
                  .elseif wParam == SELECT
                           mov ofn.lStructSize,SIZEOF ofn
                           mov ofn.lpstrFilter,offset strFilter
                           mov ofn.lpstrFile,offset lib
                           mov ofn.nMaxFile,512
                           mov
ofn.Flags,OFN_FILEMUSTEXIST+OFN_PATHMUSTEXIST+OFN_LONGNAMES+OFN_EXPLORER+OFN_HIDEREADONLY
                           invoke GetOpenFileName,addr ofn
                           .if eax==TRUE
                                    invoke SetDlgItemText,hWin,DLLPATH,addr lib
```