Virtual PC 2007과 WinDBG를 이용한 가상 머신 디버깅

작성자 김희준 (<u>drost@naver.com</u>, <u>http://insidekernel.net</u>) 작성일 2007-02-09

이번 글에서는 마이크로소프트의 Virtual PC 제품을 이용하여 가상 머신을 구성하고, WinDBG를 이용하여 디버깅 환경을 셋팅하는 방법에 대해서 설명해 드릴 것입니다. 대부분의 과정은 기존 WMWARE를 이용하여 설정하는 방법과 전체적으로 유사하지만, 아주 약간의 차이가 있습니다.

우선 필요한 것들은 다음과 같습니다.

- Virtual PC 2007 (2004와 2007 beta 모두 무료로 다운로드 가능)
- WinDBG 6.6.0007 버전 이상
- Virtual PC에서 운영체제로 설치할 가상 머신의 이미지 (XP SP2)

Virtual PC 2007의 설치

Virtual PC 제품은 Microsoft의 Virtual PC 홈페이지에서 무료(!)로 다운로드가 가능합니다. 이 문서 에서는 2007 (beta) 기준으로 설명되어 있습니다.

http://www.microsoft.com/windows/virtualpc/default.mspx

Virtual PC에 운영체제 설치

OS 이미지 (ISO)를 활용하여 운영체제를 설치합니다.





가상 머신의 설정

Virtual PC에 운영 체제의 설치가 완료되면, 먼저 별도의 타겟 컴퓨터를 이용하여 디버깅 PC 셋팅 을 하는 것처럼, BOOT.INI 파일에 디버깅 모드로의 부팅 옵션을 추가해줍니다. 우리는 디버거 머 신의 COM 포트를 파이프를 이용해 redirection을 할 것이므로, /debugport=com1 /baudrate=115200 /debug 옵션을 적어 BOOT.INI 파일의 수정을 완료합니다.

S XP SP2 KOR - Microsoft Virtual PC 2007			
Action Edit CD Floppy Help			
시작 및 복구	2 🗙		
∼시스템 시작			
기본 운영 체제(<u>S</u>):	<u>? ×</u>		
"Microsoft Windows XP Professional" /noexecute=optin /fastde	e(💙 🛛 원격		
✓ 운영 체제 목록을 표시할 시간(<u>T</u>): 30 < 초			
· · · · · · · · · · · · · · · · · · ·			
시작 옵션 파일을 수동으로 편집하려면 [편집]을 클릭 편집([하십시오.			
↓스템 오류	S)		
▼ 시스템 로그에 이벤트 기록(₩)			
☑ 관리 경고 보내기(<u>N</u>)			
▼ 자동으로 다시 시작(표)			
디버깅 정보 쓰기	E E		
작은 메모리 덤프(64KB) 🔽	the state of the second		
작은 덤프 디렉터리:			
📮 boot - 메모장			
파일(F) 편집(E) 서식(<u>O</u>) 보기(<u>V</u>) 도움말(H)			
Windows XP Professional" /noexecute=optin /fastdetect Windows XP Professional" /noexecute=optin /fastdetect /debug /debugport=com1 /baudrate=115200			
	छि इत्रह		
	an A 漢窗 🛛 😳		
🛃 시작 📄 boot - 메모장	🖏 🕏 🎪 😏 오후 2:41		
🗇 🕀 🔜 🧰 🚣			

그 다음으로 Virtual PC의 COM 포트 설정을 변경해야 합니다. 메뉴에서, Edit->Setting 을 통해 가 상 머신의 Setting 창을 엽니다. 그리고 'Named pipe:' 항목을 선택한 후, 파이프네임을 아래 그림 과 같이 지정합니다(₩₩.₩pipe₩xpsp2).

Settings for XP SP2 KOR	
Setting Current Value Image: File Name XP SP2 KOR Image: Memory 256 MB Image: Hard Disk 1 XP SP2 KOR Hard Disk.vhd Image: Hard Disk 1 XP SP2 KOR Hard Disk.vhd Image: Hard Disk 1 XP SP2 KOR Hard Disk.vhd Image: Hard Disk 1 XP SP2 KOR Hard Disk.vhd Image: Hard Disk 2 None Image: Hard Disk 3 None Image: CD/DVD Drive Secondary controller Image: Floppy Disk Auto detected Image: COM1 Named pipe: WW.W Image: COM2 None Image: COM2 Not available Image: Comage: Close Show message	COM1 None Physical serial port: Wait for modem command to open port Named pipe: \WW.\Wpipe\Wxpsp2 Text file: Browse You can select a serial port on the physical computer, a named pipe, or a text file to connect to the COM1 port on the virtual machine. If the COM1 port is used for a modem, select the Wait for modem command to open port check box. OK Cancel

호스트 WinDBG의 설정

WinDBG를 실행하고, 메뉴에서 'Kernel Debugging'을 선택합니다. 'Baud Rate'를 확인하고, 'Pipe' 항목을 체크합니다. 그리고 'Port:' 항목에는 이전에 Named Pipe로 설정해 두었던 파이프네임을 지정하고, OK를 클릭하면 하나의 컴퓨터에서 Virtual PC와 WinDBG를 사용한 가상 머신의 커널 디버깅이 시작됩니다.

Kernel Debugging	? 🔀
COM 1394 USB : Kemel debugging over	2.0 Local a COM port or virtual serial device
Baud Rate: 115200 Port:	Pipe
₩₩.₩pipe₩xpsp2	Resets:
	OK Cancel Help

🖉 Kernel 'com:port=\\\pipe\xpsp2,baud=115200,pipe,reconnect' - WinDbg:6.6.0007.5				
File Edit View Debug Window Help				
Disassembly	Locals			
Offset: nt ! IoCreateDevice Previous Next	Typecast Locations			
805a2df8 8b4508 mov ebp.esp 805a2df8 8b4508 mov eax.dword ptr [ebp+8] 805a2df8 8b4508 and dword ptr [eax+8].0 805a2df8 8b4508 and dword ptr [eax+8].0 805a2df8 8b4508 pop ebp 805a2df8 8b4508 pop ebp 805a2e03 5d pop ebp 805a2e04 c20400 ret 4 805a2e07 90 nop 805a2e09 90 nop 805a2e09 90 nop 805a2e08 8bf1 nov 805a2e17 8bec mov 805a2e17 8bec mov 805a2e17 8bec mov 805a2e17 8bec mov 805a2e17 8bef08 mov 805a2e17 8bef08 mov 805a2e17 8bef08 mov 805a2e17 8bef08 mov 805a2e18 8bef08 mov <t< td=""><td>Name Value</td></t<>	Name Value			
805a2e22 8985/411111 mov dword ptr [ebp=80.h], eax 805a2e28 8b4510 mov eax, dword ptr [ebp+10h]				
Disassembly fltop_rw.c	< >			
Command	<u>2</u>			
<pre>Microsoft (R) Windows Debugger Version 6.6.0007.5 Copyright (c) Microsoft Corporation. All rights reserved. Opened \.\pipe\xpsp2 Waiting to reconnect Connected to Windows XP 2600 x86 compatible target, ptr64 FAISE Kernel Debugger connection established. Symbol search path is: srv#D:\symbols*http://msdl.microsoft.com/download/symbols Executable search path is: D:\public\TheForce\projects\VFVsys\objchk_wxp_x86\i386 Windows XP Kernel Version 2600 (Service Pack 2) UP Free X86 compatible Product: WinNt, suite: TerminalServer SingleUserTS Built by: 2600.xpsp_sp2_rtm.040803-2158 Kernel base = 0x804d9000 PsLoadedModuleList = 0x8055cb20 Debug consist time: Ext Each 0 1E:22:22 751 2007 (CWT:0) kd></pre>				
Ln 197, Col 23 Sys 0:KdSn	v:S Proc 000:0 Thrd 000:0 ASM OVR CAPS NUM			

예) 위의 과정을 통하여 BreakPoint를 잡은 모습

이로써 Virtual PC 2007과 WinDBG를 이용한 가상 머신 셋팅 방법에 대해서 알아보았습니다. 감사 합니다.