

SoftIce-WinIce Tutorial

By CoRN2 [mE'97/C4N]

If you want to be able to read this, then NotePad with WordWrap on might be a very good idea.

Everybody asks the question, 'which debugger should I use?' The answer is usually SoftIce... The second question is 'how do I use SoftIce?!' This tutorial should hopefully cover the basic aspects of using SoftIce for our 'evil' needs!! ;)

I'm going to assume that you're using SoftIce/Win95 v3.0 or later. Once installed, SoftIce lives behind win until you need it... now the fun bit...

To access SoftIce you simply press <CTRL-D> unless of course you've changed this hotkey.

I'VE PRESSED CTRL-D, WTF IS ALL THIS STUFF!!!?!!??!

Although maybe daunting at first, its all pretty simple. You really do need to have a rough idea about ASM for me to be able to explain this properly. If not, get my tut, 'ASM For Crackers' (PLUG! PLUG!) from the mExeLITE'97 homepage. It should cover the basics.

Ok. Now you know what registers are, and hopefully what a chunk of assembly looks like.

The top three lines of the screen are dedicated to your computers registers, and their contents. This is fairly self explanatory.

EAX=whatever, EBX=whatever, and so on.

The second line at the far right contains 8 letters, these are your flags. Capital blue letters indicate that the flag is set, the flags are:

```

O D I S Z A P C
| | | | | | | |
| | | | | | | | +----- Carry Flag
| | | | | | | | +----- Parity Flag
| | | | | | | | +----- Auxiliary Carry Flag
| | | | | | | | +----- Zero Flag ( VERY USEFUL! )
| | | | | | | | +----- Sign Flag
| | | | | | | | +----- Interrupt Flag
| | | | | | | | +----- Direction Flag
+----- Overflow Flag
```

To be honest the only one I've ever looked at while cracking, is the Zero Flag (its looked for JZ/JNZ/JE/JNE commands)

Next we have another window underneath, this is your data window. It shows the value of any memory address you might need. As an example, type: d F9D2B --this shows the bytes at that address.

'd' is your display memory command.

Following this we have the code window. This contains the part of the program that we're looking at. Firstly you have the segment:offset of the code, then the opcode, then the asm commands we all love.

(NB you may have to type 'CODE ON' in order to see the opcode.

SoftIce-WinIce Tutorial

By CoRN2 [mE'97/C4N]

And finally at the bottom is your input/information window. In other words the bit you use to talk to SoftIce, and hears its' response.

BREAKPOINT ON EXECUTE

SYNTAX: `bpx <api function name>`

The main problem with cracking... umm.. sorry debugging (heh!) is to find yourself an entry point into the program. The easiest, and most effective way to begin is with breakpoints.

Basically all you need to do is to tell SoftIce when to 'break' into the program so you can see whats happening. The type of breakpoint that you would use depends upon the type of program you're trying to 'debug' ;)

To show this we'll take an example:

1. Switch to SoftIce (CTRL-D), and type 'bpx GetLocalTime'
2. The prompt should return, switch back to win (CTRL-D)
3. Double click on the win95 system clock (usually on your taskbar)

SoftIce should now pop up, at the start of the call to 'GetLocalTime', if you press F11 you will return to the part of the code that called the function.

Another function call to breakpoint on is useful when cracking serial number protections is 'GetWindowTextA' or 'GetDlgItemTextA'. This is done in exactly the same way.

1. Click your StartButton (good old MS :P) and click upon the 'RUN' button.
2. Type in any old crap, ie. 'lalalalalalalalaa' DON'T PRESS ENTER
3. Switch to SoftIce. (CTRL-D)
4. Type: BPX GetWindowTextA
5. Switch back to win, now press ENTER

SoftIce pops up at the Start of 'GetWindowTextA', so again press F11 to return to the calling code. GetDlgItemTextA isn't used as much in my experience, but worth trying if nothing happens on GetWindowTextA.

SEARCHING MEMORY

Simple one this. Say you've entered your registration info, and you're lost in the code somewhere, to help yourself along you can search in memory for your info (WOW! ;)

SYNTAX: `s <start> l <finish> '<string>'`

When searching you want to look for it everywhere, so I mainly use:

```
s 0 l ffffffff 'mystring'
```

Once found you'll get a nice prompt telling you where in memory it is, and the data window changes to that address.

To Search again just type: s

SoftIce-WinIce Tutorial

By CoRN2 [mE'97/C4N]

This will keep searching, beware though, that in my experience, any strings found around the 80000000+ and C0000000+ areas are either duplicates or bits of shite floating about due to Win95's amazing management of your ram.

BREAKPOINTING ON MEMORY ACCESS

SYNTAX: `BPM <address> R/W`

This is usually used in conjunction with the step above, searching. Once you've found your string, what use is it to you???

Say through searching, I got the prompt:

Pattern Found at 0157:0009AC2D

ok, this tells us that my string was found at the location 0157:0009AC2D (doh!). So to get SoftIce to monitor this we'd use:

BPM 0157:0009AC2D

The R/W tells SoftIce whether to pop up on a read or write operation to that address. The default is RW (read & write)

SOFTICE & The Net (The Internet/The Information Super-Highway ARRGGH!)

Some people (not me yet) have experienced a problem when cracking whilst logged on. This won't affect people who (like me) aren't lucky enough to get FREE LOCAL PHONE CALLS!! who have to pay £££'s for their phonebills... sorry.

Anyway, if you're logged on and you switch to SoftIce many people experience a loss in their connection (mainly to IRC) Apparently this is fixable by using the '/AWAY asuidsodj' command, but I dunno. Try it if you get stuck.

FINAL WORD

This tut should (hopefully, unless I totally messed it up) cover enough about SoftIce to allow the average newbie to get started. I know there is a shitload of stuff I haven't covered, there should be a more advanced tut arriving soon (watch this space | | ;)

If there is anything you else think ppl need to know to get started, or anything you think should be added, just mail me at CoRN02@hotmail.com and tell me. I can be reached on EFNET, in #Cracking4Newbies most of the time... someone will be able to help anyway....

Hope this helps anyone who wants to learn's task easier... I could have done with this when I started. Good Luck!