Portal World Domination Introduces:
VoXeL's Junior cracking tutorial

(This means your first real cracking tutorial)

You're First Crack?

Your probably wondering why there is a question mark after the title. Its simple, this could go well or be a disaster. If it turns out to be that latter don't be discouraged. I have, many times, read a tutorial that everyone else finds easy to follow and understand but became lost and disorientated. This may not be your style, but I understand that. Try to find one more your style. With that said let's get down to business. The first thing you need is a set of tools...good tools make the craftsman!

Tools!

For tools you need a minimum of debugger, disassembler, and hex editor. For a debugger and hex editor I use WinIce and Hex Works, respectively. As for a disassembler that really matters on what you're disassembling. For 32-bit windows files I recommend W32Dasm v5.4 or above and although W32Dasm works on 16-bit programs, Windows Source with Sourcer 6.51+ works best on 16-bit windows files.

Setting Up WinIce

When WinIce is installed out of the box, it is usually not set up to display the Hexadecimal values of instructions. The following sets this up in order to aid you. Ok, here is where things first get complicated. After installing all three(or four) programs you have to manually edit the Winice.dat file in the directory that installed WinIce.

Now the first thing you have to find is the line that reads:

INIT = "X;" and change it to **INIT = "CODE ON; X;"**

This will tell WinIce to display the Hex codes for the assembler instruction displayed in the code window.

Next find the lines that say:

; *** Examples of export symbols that can be included for Chicago *****
; Change the path to the appropriate drive and directory

and remove the ';' before every line AFTER that. *This tells WinIce to load the System functions.*
(The ';' comments out the lines that have been placed there by Nu-Mega)

Ok you know have to reboot. I'll wait...

Oh, you're back! Well then lets go...

Now, finally, you're really ready to get cracking! The first program was selected because of its simplicity. It's a date checker. It was meant as a demo that lasted until December 20 1996. Because this program has a constant date of termination, it simplifies cracking. One really helpful document to have handy is the Win32 API reference. It outlines most of the windows functions and how they return and accept values.

Lets review what we already know about this program. It checks the date to see if it's before Dec 20th. If its not it pops up a MessageBox and Exits. Hmmm, but where is it getting that damn date? Well a quick browse through our API reference reveals several possibilities:

- **GetCurrentTime** Returns elapsed time since Windows started
- **GetFileTime** Returns 64-bit file times
- **GetLocalTime** Returns local time and date
- **GetSystemTime** Returns system time and date
- **GetTickCount** Returns amount of time Windows has been running
- **GetTimeZoneInformation** Retrieves current time-zone settings

Just by using simple logic we can get rid of all except GetSystemTime and GetLocalTime. You may be wondering what is the difference between System and Local time. I have no clue but I do know that most programs call

GetSystemTime. So let's get that WinIce working...

WinIce

To enter and exit WinIce you have to press ^d (control d). Now you are faced with a nice text screen. You should have the registers along the top of the screen, just under that a hex readout of memory at a specific location, then the code window, and finally the command window. The code and command window is where you will spend most of your time.

Now you're in the code window so start by typing 'B', see the bottom of the screen? It lists all the commands that start with 'B'. With that said, lets set a breakpoint.

A breakpoint is a point that, when reached, halts execution and brings you to the debugger window. The one we will be using most is 'BPX', which stands for BreakPoint on eXecution. BPX breaks on any call to the function you tell it to. So you want get started on that crack? You feel lucky punk?

InstallSHIELD Express Professional Demo

After you install InstallSHIELD try running it at various dates. See the message box? Let's fix that bug!

- So now exit it and press ^d to go to WinIce.
- Type in 'BPX GetSystemTime' (remember that function?)
- Then press ^d to go back to windows.

Now you that you have set the breakpoint anytime an application calls it to get the time the debugger will pop up with the CALL in the code window. The next step is to just run the program...
Cool eh?

- OK now it broke at the entrance to the GetSystemTime code in the actual OS.
- THAT HAS ABSOLUTLY NOTHING TO DO WITH THE CHECK. First exit out with F11(this steps out of the code).
- Now you have the "call" to GetSystemTime and a bunch of CoMPares and MOVe's
- Those are just to place the actual time and date into the right place.
- Keep stepping (F10) until you RETurn to the calling function.
- Now you see an ADD and a CMP now look at what this compares... EAX to some weird looking constant!
- Something is telling you this is the place of the date check, look at the next line. a JLE (jump if less than or equal to) that would be the check I would use- "if the date is less than or equal to Dec 20 1996..." but how do we fix it?
- Well you want it to jump no matter what the date is, so your going to have to make the jump unconditional(just a JMP) write down the "CMP EAX, 32BAC2297". Then in WinIce, look to the left of the assembly instructions. That is the hex listing of the assembly instructions. Very useful.
- Write those down! You need them when you go to the hex editor. I would write down the ones for the CMP and JLE instruction(should be 8 bytes or 16 numbers).
- Go to the hex editor. Open the executable. Go to Edit->Find. Make sure the "Value" is set to Hex and "Direction" is down. Then do a search for that hex code you wrote down earlier. Put them together so search for both the CMP and JLE code. Make it one long number...
- Now that it found the instructions, find the byte for the JLE instruction(the JLE consists of two bytes, one is the instruction or type of jump and the other it the offset to where it jumps to)the first of the two bytes is the one your looking for.
- Now change that to EB (hex) EB is the byte for JMP and remember the goal was to change the conditional jump to unconditional.
- SAVE the edited file.
- Go back to WinIce and use BC * to clear your breakpoints.
- Go back to windows.
- Set your date ahead and run the program...IT WORKS!!!!

Now that you have cracked your first program are you ready for your second?

Typecaster BETA (a PhotoShop plugin)

At first this program might seem harder because it is a plugin and not a stand-alone program, but in truth

plugins are exactly like programs. The only real difference is who "owns" them. For regular programs the owner is the OS, but for plugins(which are really just DLL's) the owner is the program they plug into. With that said, Typecaster should be easy! Why? because it is also a date checker, exactly like before except it has three checks. Well what are you waiting for? Go do it!!!

How to contact us!

We're always looking for new members who really want to learn! See any of the senior members or Head members for membership! We can help you learn. If your ever on Undernet stop by #PWD. Or look for our members scattered around the world. Here is a list:

First the two founding (Senior) Members and the best of our group:

- DiM
- StarFury

Then the Head Members, those of us that cracked something:

- _Lasher_ / Imajix
- B_Spline
- Kratz
- VoXeL

Finally those valuable Members that are there to help and learn:

- BigD_
- Cyah
- DrmWEaver
- EvilAngel
- Fouton
- Goa
- IcedFire
- Locote
- Maug
- |No_One|
- Quequog
- Slvrmoon
- TimbrWlf
- Tungsten

VoXeL