

反汇编(逆向工程)

贺利坚 主讲



汇编语言程序设计
Assembly Language

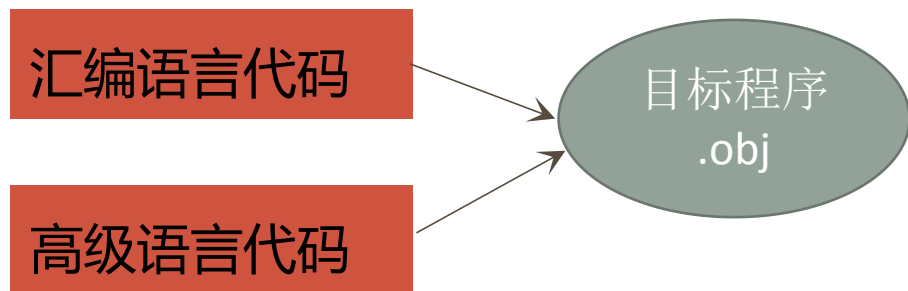
反汇编(逆向工程)

💻 把目标代码转为汇编代码的过程，即，把机器语言代码转换为汇编语言代码，由低级转高级。

💻 常用于软件破解（例如找到它是如何注册的，从而解出它的注册码或者编写注册机）、外挂技术、病毒分析、逆向工程、软件汉化等领域。

💻 学习和理解反汇编，对软件调试、漏洞分析、OS的内核原理及理解高级语言代码都有相当大的帮助，在此过程中我们可以领悟到软件作者的编程思想。

💻 总之一句话：软件一切神秘的运行机制全在反汇编代码里面。



用Debug反汇编

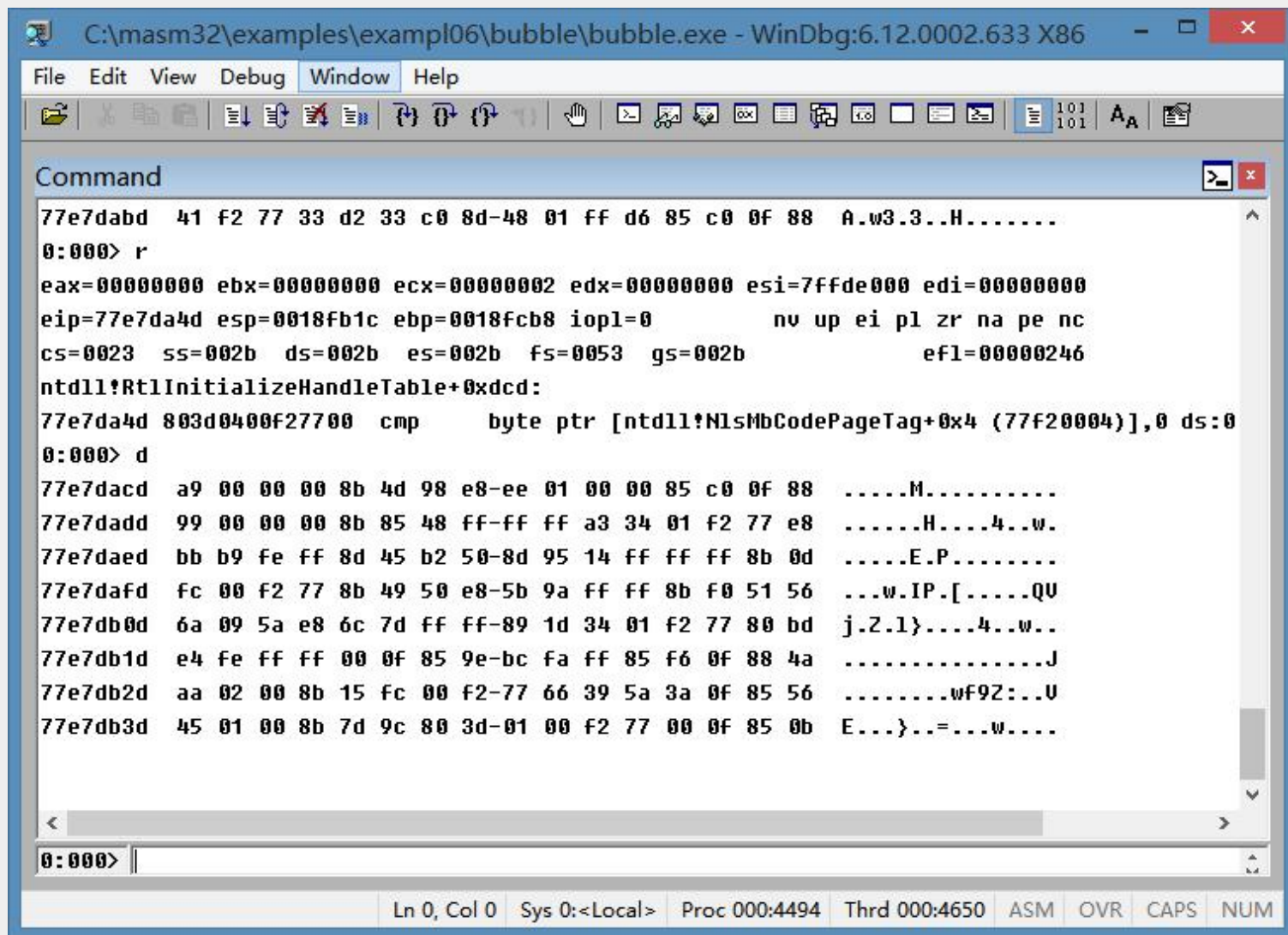
```
C:\>debug ptest.exe
```

```
-u
```

076A:0000	B86D07	MOV	AX,076D
076A:0003	BED8	MOV	DS,AX
076A:0005	B80000	MOV	AX,0000
076A:0008	BD360000	LEA	SI,[0000]
076A:000C	B90500	MOV	CX,0005
076A:000F	0304	ADD	AX,[SI]
076A:0011	46	INC	SI
076A:0012	46	INC	SI
076A:0013	E2FA	LOOP	000F
076A:0015	A30A00	MOV	[000A],AX
076A:0018	B80000	MOV	AX,0000
076A:001B	BD360C00	LEA	SI,[000C]
076A:001F	B90900	MOV	CX,0009

```
-
```

windbg——windows下的Debug



The screenshot shows the WinDbg 6.12.0002.633 X86 interface. The title bar indicates the file path: C:\masm32\examples\exampl06\bubble\bubble.exe. The menu bar includes File, Edit, View, Debug, Window, and Help. The toolbar contains various icons for file operations, debugging, and viewing. The Command window shows the following commands and output:

```
Command
77e7dabd 41 f2 77 33 d2 33 c0 8d-48 01 ff d6 85 c0 0f 88 A.w3.3..H.....
0:000> r
eax=00000000 ebx=00000000 ecx=00000002 edx=00000000 esi=7ffde000 edi=00000000
eip=77e7da4d esp=0018fb1c ebp=0018fcb8 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
ntdll!RtlInitializeHandleTable+0xcd:
77e7da4d 803d0400f27700 cmp     byte ptr [ntdll!NlsMbCodePageTag+0x4 (77f20004)],0 ds:0
0:000> d
77e7dacd a9 00 00 00 8b 4d 98 e8-ee 01 00 00 85 c0 0f 88 .....M.....
77e7dadd 99 00 00 00 8b 85 48 ff-ff ff a3 34 01 f2 77 e8 .....H....4..w.
77e7daed bb b9 fe ff 8d 45 b2 50-8d 95 14 ff ff ff 8b 0d .....E.P.....
77e7dafd fc 00 f2 77 8b 49 50 e8-5b 9a ff ff 8b f0 51 56 ...w.IP.[.....QU
77e7db0d 6a 09 5a e8 6c 7d ff ff-89 1d 34 01 f2 77 80 bd j.2.1}>...4..w..
77e7db1d e4 fe ff ff 00 0f 85 9e-bc fa ff 85 f6 0f 88 4a .....J
77e7db2d aa 02 00 8b 15 fc 00 f2-77 66 39 5a 3a 0f 85 56 .....wF92:...U
77e7db3d 45 01 00 8b 7d 9c 80 3d-01 00 f2 77 00 0f 85 0b E...}>...=...w....
```

The status bar at the bottom shows: Ln 0, Col 0 Sys 0:<Local> Proc 000:4494 Thrd 000:4650 ASM OVR CAPS NUM.