## 逆向工程——汇编基础（一）

汇编语言

一种最接近计算机核心的编码语言。

处理器（cpu）

认识处理器：汇编语言被编译为机器语言，cpu执行机器语言。

典型处理器功能

从内存获取机器语言指令，译码，执行。

根据指令代码管理寄存器。

根据指令或自己的需要修改内存内容。

响应其它硬件的中断请求。

寄存器

寄存器位于cpu中，保存特定长度的数据。寄存器可以被装入数据，可以在不同寄存器之间移动这些数据，或者做类似的事情，如四则运算、位运算等操作。

通用寄存器

EAX：32-bit。常用于①进行运算，②保护模式中作为内存偏移指针（此时，DS作为段寄存器或选择器）。

EBX：32-bit。常用于①内存偏移指针（DS是默认的段寄存器或选择器）②保护模式中和EAX相同。

ECX:32-bit.常用于①用于特定指令的计数②保护模式中和EAX相同

EDX: 32-bit。常用于①在一些运算中作为EAX的溢出寄存器（eg：乘除）②保护模式中和EAX相同

ESI: 32-bit。常用于①内存操作指令中作为源地址指针使用②可被装入任何数值制、但通常不用作寄存器。DS作为寄存器或段选择器

EDI:32-bit。常用于①内存操作指令中作为目的指针使用。

EBP: 32-bit。常用于①指针寄存器，通常，它被高级语言编译器用以建造堆栈帧来保存函数或过程的局部变量。②ss是它的默认段寄存器或选择器。

注意：这三个寄存器没有对应的8-bit分组。但可以通过SI、DI、BP分别访问他们的低16位。

段寄存器和选择器

实模式下的段寄存器到保护模式下，摇身一变就成了选择器。不同的是，实模式下的段选择器是16-bit的，而保护模式下的选择器是32-bit的。