静态逆向分析技术

1.静态分析：IDA Freeware
动态分析： OllyDbg：用户态的动态调试； WinDbg：内核态的动态调试（至少两个操作系统可用虚拟机）
2.IDA
IDA 除了支持PE文件格式，还支持ELF等文件格式；
IDA会自动识别处理器类型；
IDA是按区块装载PE文件的，例如.text(代码块)、.data(数据块)、.rsrc(资源块)等；
在默认情况下，IDA Freeware的反汇编代码中不包含PE头或资源节。
3.交叉引用
CODE XREF显示函数在什么地方被调用了
数据的交叉引用 DATA XREF
4.IDA默认命名规则：
局部变量（ local variable）：前缀: var_；后缀: 相对EBP的偏移值；偏移值为负值
参数（argument）：前缀： arg_；后缀：相对于EBP的偏移值；偏移为正值