这一章看完会很崩溃，为什么呢？

因为前面学习的各种技巧全被微软修复了，比如经典的栈溢出，微软加入了GS编译技术，SEH等等也添加了相应的保护机制，看着看着......

也就明白了为什么前面用的都是windows XP和windows 2000，而不是用windows 7

下面来总结一下微软的安全机制：

(1)使用GS变异技术，在函数返回地址之前加入了Security Cookie，在函数返回前首先检测Securit Cookie是否被覆盖，从而把针对操作系统的栈溢出变得十分困难

(2)增加了对S.E.H的安全校验机制，能够有效地挫败绝大多数通过改写S.E.H而劫持进程的攻击

(3)堆中加入了Heap Cookie，Safe Unlinking等一系列的安全机制，为原本就困难重重的堆溢出增加了更多的限制

(4)D.E.P（Data Execution Protection）将数据部分标记为不可执行，阻止了栈，堆和数据结中攻击代码的执行

(5)ASLR（Address space layout randomization，加载地址随机）技术通过对系统关键地址的随机化，使得经典堆栈溢出手段失效

(6)SEHOP（Structured Execution Handler Overwrite Protection，S.E.H覆盖保护）作为对安全S.E.H机制的补充，SEHOP将S.E.H的保护提升到系统级别，使得S.E.H的保护机制更为有效

那么看完这些内心当然是崩溃的 (╯‵□′)╯︵┻━┻

但是，道高一尺，魔高一丈，总会有新的手段可以绕过windows的安全机制，虽然现在我还不能独立研究出绕过windows防护机制的方法，但是以后可以啊！！！！！！