**第一次习题（教材第1章+逆向）**

1. **什么是软件缺陷和软件漏洞？软件缺陷和软件漏洞有何区别？软件漏洞是否有可能转变为软件后门，为什么？**

答：

1. 软件缺陷是指计算机软件或程序中存在的某种破坏正常运行能力的问题、错误、或者隐藏的功能缺陷，软件漏洞是是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而使攻击者能够在未授权的情况下访问或破坏系统。
2. 软件漏洞是软件缺陷导致的发生。
3. 软件漏洞可以转变为软件后门，利用软件漏洞在目标系统中插入并执行精心设计的代码，执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。
4. **什么是逆向工程？举例分析逆向工程的积极意义，以及可能带来的安全隐患。**

**答：**

1. 将可执行程序反汇编，通过分析反汇编代码来理解代码功能，然后用高级语言重新描述这段代码，逆向分析原始软件的思路，这个过程就称作逆向工程。
2. 逆向工程的积极意义，对病毒文件，恶意软件等进行分析，试探并找到软件的运行流程，甚至反向分析出软件的源代码
3. 可能带来的隐患，非法破解软件或者第三方分析系统漏洞造成破坏。
4. **什么是沙箱与虚拟机？其在安全领域有哪些具体应用？**

答：虚拟机是一个可以指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。

沙河是一种安全机制，为运行中的程序提供的隔离环境。

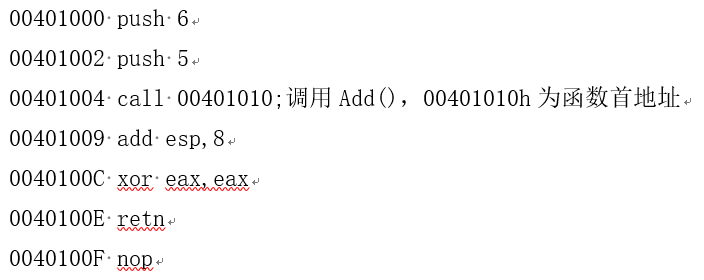
它们在安全领域内都可以隔离安全风险。

4、请选择一个安全公司的历年安全报告进行仔细阅读，请从近10年以来互联网软件安全发展趋势进行分析，给出一个简要对比分析，要求至少说明软件安全发展特点和趋势。（选做）

逆向习题

1. **简述软件逆向的作用。**
2. 病毒防治
3. 软件破解
4. 开发测试
5. 软件问题分析
6. 系统栈在程序执行中的作用有哪些？
7. 临时存放变量
8. 保存断点和恢复断点
9. 以一个EXE（C程序）反编译代码为例，说明参数的传递和函数执行过程。（注：需按反编译结果给出虚拟地址）

|  |
| --- |
| 1. C语言代码 2. int Add(int x,int y); 3. int main() 4. { 5. int a=5,b=6; 6. Add(a,b); 7. return 0; 8. } 9. int Add(int x,int y) 10. { 11. return (x+y); 12. } |

反汇编结果

参数传递是通过栈来完成的，栈保存变量，需要时从栈中取出

1. **子过程自身的局部变量可以表示为[ebp+Y]形式，此处Y为正值还是负值，为什么？**

Y为负值，因为子程序自身的局部变量需要在栈中分配新的空间，需要入栈，把栈顶指针减去一个值，相当于加负值。

1. **考虑到内存对齐，计算并显示回答如下数据结构实际所占内存单元大小，并在图中标示出来数据的实际存储情况**。

Struct AAA{

short a;

int b;

|  |
| --- |
| 00010001 |
| 00010001 |
| 填充 |
| 填充 |
| 00100010 |
| 00100010 |
| 00100010 |
| 00100010 |
| 00110011 |
| 00110011 |
| 00110011 |
| 00110011 |

int c; 从此处开始填（低端地址）●

} bbb；

bbb.a = 0x1111;

bbb.b = 0x22222222;

bbb.c = 0x33333333;

答： 该结构体实际所占内存数是\_\_12字节\_\_\_