计算题

文件系统，FAT32，引导扇区的比较多，比如算一个分区的大小，分了几个区，

PE文件格式，考的比较多，压缩后的PE字段

程序分析题

给出一段代码，分析代码的漏洞，给源代码，分析漏洞，原因

有可能会考漏洞利用的知识，eg：LOP，实验当中有的内容

双向链表，怎么破坏，在上链卸链有什么问题

概念题

普通的网络攻击和APT攻击有什么联系，在课本上有

有一部分的简答题10~15，缓冲分数

计算题20~30

程序分析题30~40

实验内容很重要，考试大部分内容都跟这部分有关

知识点内容

大部分和操作系统内容相似

文件系统：FAT32，FAT表，文件分配表

第二个作业的目的是为了了解文件系统怎么工作的，FAT32是根据FAT表，NTFS是根据文件属性

PE文件格式：OS装在可执行程序，代码和数据区分，各种各样的数据->PE文件中进行定义，PE文件中有格式，OS才能根据loader进行装载文件，程序到进程的创建

基础性的知识：链接、编译的输入和输出，链接是生成PE文件的关键步骤，生成可执行程序

windows下病毒的传播机理：病毒传播->从OS的角度来看，是写文件，写入文件的内容是代码和数据。

重定位内容，病毒为什么需要重定位？三个场景：地址固定的情况下，不需要重定位，每次装载的地址是一样的；感染特定的程序，只需要偏移源程序的代码偏移；感染所有的程序，那么就需要进行重定位

列举若干种重定位的方式：如何重定位？重新拿到该地址就是重定位

eg：一种重定位的方式，拿到的地址就是重定位

```
call
pop
```

导入表、导出表：这部分内容有可能会考，考试题目maybe：给某一个函数的API函数地址，给出导出表的结构，maybe是一个内存镜像，如何根据导出表的结构解析内存镜像，找到另一个API函数的地址？

病毒分析相关：进程监控、文件监控，病毒->远程控制的程序

前面的知识点是病毒，后面一部分内容讲的是漏洞，病毒是附加的恶意软件，漏洞属于软件自身的bug，属于软件自身的问题。

漏洞的类型：缓冲区溢出、可格式化字符串的漏洞、堆内存：OS管理的未分配的堆，数据结构，涉及到链表的操作，可能会导致指针遭到破坏

系统安全防御：讲了三个内容

做实验、作业要搞懂，涵盖了考试的大部分的内容

mooc的最后的内容，涉及到windows漏洞的分析（闭源），课本上讲的大部分是Linux（开源），看一下，了解一下