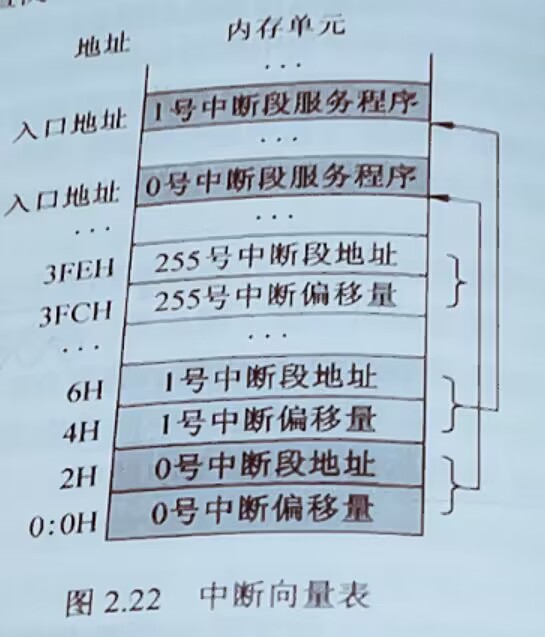
第二次作业

1. 简述实模式下中断的原理，画图展示中断向量表的结构。

中断就是CPU暂停当前程序的执行，转而执行处理紧急事务的程序，并在该事务处理完成后能自动恢复执行原先程序的过程。

中断向量表如下：



1. 简述引导型病毒中中断劫持、病毒代码激活的原理。

中断劫持：即利用中断(在一个程序被中断时会根据中断向量表中的地址跳转到中断服务程序)的原理，将中断向量表中的地址改为病毒的地址，就可以实现在中断时，将中断服务程序劫持为病毒程序。

病毒代码激活原理：利用一些常规的中断需求，在代码产生中断时，就可以劫持中断服务程序，跳转到病毒代码部分，激活病毒。

1. 简述病毒重定位的原因以及实现的原理。

原因：

1.正常程序在源程序编译时，变量在内存中的位置都被计算好了，在装入内存时，系统不会为它重定位。

2.而病毒在感染HOST程序时，是将已编译好的代码附在HOST上，此时病毒代码中的变量地址并没有随着在内存位置改变而发生改变，故需要对病毒进行重定位操作。

原理：

利用call指令中会先将返回地址压入堆栈，再将IP置为call语句所指向的地址的特点。call语句调用紧接着call语句的函数，即调用call指令后，会将call指令调用的函数地址压入堆栈中，此时的call指令不需要ret指令返回，直接使用pop指令得到call指令调用的函数地址。

1. 简述MZ文件型病毒中感染、激活等过程的基本原理。

感染：搜索载入内存的其他文件，查看其他文件是否有被感染的标志。如果没有，将病毒加在文件的末端，并修改CS、IP的值指向病毒起始地址，修改文件长度和SS、SP

激活：运行含有病毒的HOST程序，则病毒会随着程序一块被载入到内存， 且常驻内存。