**1. 习近平主席在2016年4月19日讲话中指出“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”，试结合本课程所学知识，浅谈对这句话的理解。**

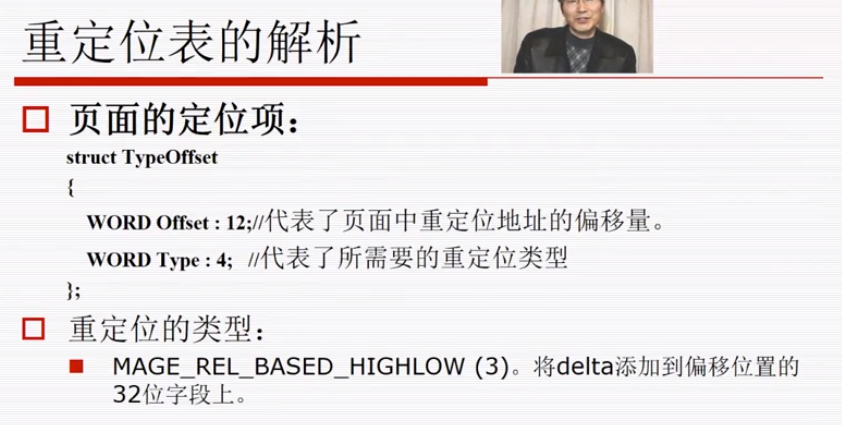
**2. 一般USB采用FAT32文件格式，其储存的一个JPG照片被无意删除，试给出手动恢复的原理和过程。**

文件被删除后，文件首字节被修改为E5，首簇的高位被清零，FAT表的簇链被全部清空，但同时文件内容没有变化，手动恢复具体过程为还原文件名首位，确定高位并还原，同时修复FAT表簇链。其中还原文件名首字节在知道文件名的情况下，长文件名可以通过目录项来进行查询，首簇高位可以参考相邻目录向的首簇高位，也可以从0向上试探，观察首簇只想内容是否为预期文件头部。修复簇链通过文件大小计算所占簇数，之后按照连续存储假设，进行簇链修补，最后一个簇用0FFFFFFF结尾，当文件不是连续存储时，只能恢复出一部分内容。

**3. 简述PE结构中重定位节的结构，以及重定位的作用。**

在重定位节中存放了一个重定位表，若装载器不是把程序装到程序编译时默认的基地址时，就需要重定位表进行调整。





**4. 简述GS、DEP、ASLR机制在对抗漏洞利用攻击时的作用机理。**

GS：GS选项为每个函数调用增加了一些额外的数据和操作，用以检测栈中的溢出，在所有函数调用发生时，向栈帧内压入一个额外的随机DWORD，这个随机数被称为“canary”，IDA中将这个随机数称为Security Cookie，当栈中发生溢出时，Cookie将首先被淹没，之后才是EBP和返回地址，函数返回前系统将进行一个额外的安全验证操作称为Securitycheck，如果发现Cookie和.data中副本的值不相同，就表明栈中发生了溢出。

DEP：DEP的基本原理是将数据所在的内存页标识为不可执行，当程序溢出成功转入shellcode时，程序会尝试在数据页面上执行命令，此时CPU就会抛出异常。

ASLR：ASLR包含映像随机化、堆栈随机化和PEB与TEB随机化，通过对堆、栈、共享库映射等线性区布局的随机化，增加攻击者预测目的地址的难度，防止攻击者直接定位攻击代码位置，达到阻止溢出攻击的目的。

**5. 关于计算机信息系统犯罪，根据我国刑法规定，主要涉及到哪几种罪？如何量刑？**

《刑法》第二百八十五条　【非法侵入计算机信息系统罪；非法获取计算机信息系统数据、非法控制计算机信息系统罪；提供侵入、非法控制计算机信息系统程序、工具罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

《刑法》第二百八十六条　【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

《刑法》第二百八十七条　【利用计算机实施犯罪的提示性规定】利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。例如，利用互联网传播淫秽色情的，按照《刑法》第九节【制作、贩卖、传播淫秽物品罪】相关条款论处。此外，2013年9月，最高人民法院、最高人民检察院公布并施行了《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》，对办理利用信息网络实施的侮辱、诽谤，寻衅滋事，敲诈勒索，非法经营，聚众扰乱公共场所，编造、故意传播虚假恐怖信息等刑事案件适用法律的若干问题进行了解释。

《治安处罚法》第二十九条　有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

(一)违反国家规定，侵入计算机信息系统，造成危害的；

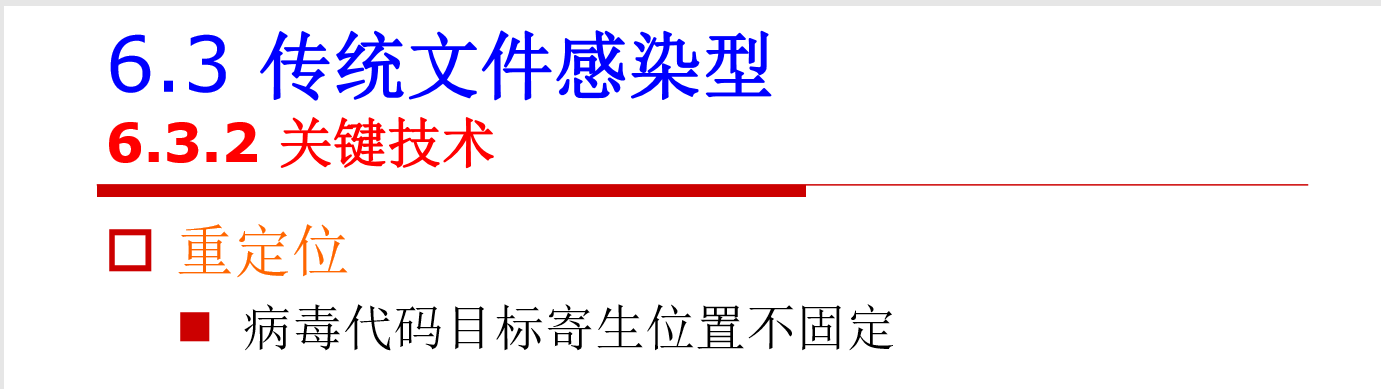
(二)违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

(三)违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

(四)故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的

**6. 为什么需要地址重定位？正常PE程序以及恶意代码在重定位上有何差异？**

若装载器不是把程序装到程序编译时默认的基地址时，就需要重定位进行地址调整。



**7. 熊猫烧香病毒在感染文件后为什么目标程序图标会变为熊猫烧香图案？对于熊猫烧香病毒的感染方式而言，怎样做才能不使被感染程序的图标发生变化？**

熊猫烧香病毒属于捆绑式感染，病毒会目标HOST程序作为数据存储在病毒体内，当程序被触发执行时，会首先执行病毒程序，之后将HOST释放并执行目标程序，当目标程序被感染后，目标程序会处于病毒程序之后，此时系统识别的是熊猫烧香病毒，所以图标也是熊猫烧香的图标。对于这种感染方式而言，可以将目标程序的资源节提出，找到其中和图标相关的内容，并复制到病毒程序之中，这样操作系统虽然识别了病毒程序，但此时病毒程序的图标和目标程序的图标相同，进而感染程序的图标不会发生变化。

**8. 什么是DWORD SHOOT，请简要描述机理。**

发生栈溢出时，非法数据可以淹没下一个堆块的块首，块首是可以被攻击者控制的，即堆栈中存放的前向指针和后向指针是可以被攻击者伪造的，当这个堆块从双向链表中remove时，node -> blink -> flink = node -> flink将把伪造的flink写入到伪造的blink所指的地址中去，通过这一手段可以修改关键地址，这就是DWORD SHOOT。

**9. 漏洞的通用阻断技术包括GS、DEP、ASLR、SafeSEH等，请各自通过一句话简要描述他们的作用和机理？**

SafeSEH：在程序调用异常处理函数前，对要调用的异常处理函数进行一系列的有效性校验，当发现异常处理函数不可靠时将终止异常处理函数的调用，SafeSEH实现需要操作系统与编译器的双重支持，二者缺一都会降低SafeSEH的保护能力。

10. 

