一、填空题：

1、操作系统面临的安全威胁包括**病毒、蠕虫、木马、逻辑炸弹、隐蔽通道、天窗**。

2、操作系统的安全目标是：对系统的用户**进行身份认证**，依据安全策略对用户操作进行**访问控制**，阻止用户对系统资源的**非法访问**，监督系统运行的**安全**，保证系统自身的**安全性和完整性**。

3、操作系统的存储保护中，数据存储单元可以分为**字、字块、页面或段**。

4、操作系统的硬件安全机制包括：**存储保护、运行保护和I/O保护**。

二、选择题：

1、以下可以进行网络攻击的威胁是：（**ABCDEF**）

A．病毒；B. 蠕虫；C. 木马；D. 逻辑炸弹；E. 隐蔽通道；F. 天窗

2、以下攻击具有传染性的是（**AB**）

A．病毒；B. 蠕虫；C. 木马；D. 逻辑炸弹；E. 隐蔽通道；F. 天窗

3、以下属于最小特权保护机制的是（**CD**）

A. 将系统用户的角色分为管理员角色和一般用户角色；

B．将系统用户的角色分为root角色和一般用户角色；

C．将系统用户的角色分为系统安全管理员、系统安全审计管理员、系统安全数据复制管理员和一般用户；

D．不给用户分配超过执行任务所需特权以外的权限

三、简答题：

1、病毒和蠕虫的区别？他们的传播途径分别是什么？

**病毒需要依附与包括操作系统在内的其他程序，没有独立运行的能力；传播方式是通过被已感染文件运行来感染目标文件，从而在计算机中传播。**

**蠕虫与病毒不同的地方在于可以不依赖宿主程序独立运行，将与自己相同的程序传播到其他目标机器中；传播方式是利用系统自身脆弱性，比如操作系统、网络协议的漏洞等完成传播。**

2、简要说明存储管理中，虚拟地址空间和物理地址空间是如何对应的?

**虚拟地址通过页表映射到物理内存，页表由操作系统维护并被处理器引用，每个进程都有自己的页表。**

**不完整**

四、问答题

1、隐蔽通道划分成哪两类？每类一个举例，说明工作原理。

**隐蔽通道分为隐蔽存储通道和隐蔽定时通道。**

**隐蔽存储通道：该通道在系统中通过两个进程利用不受安全策控制的存储单元传递信息。前一个进程通过改变存储单元的内容发送信息，后一个进程通过观察存储单元的变化来接受信息。举例：在第五章中强制访问技术中的BLP模型部分，就存在高密级主体和低密级主体，通过读写中间文件以及更改权限的方式来传递高密级信息的隐蔽通道。**

**隐蔽定时通道：该通道在系统中通过利用一个不受安全策略控制的广义存储单元传递信息，前一个进程通过改变广义存储单元的内容发送信息，后一个进程通过观察广义单元的变化接受信息，并用如时钟这样的坐标进行测量。举例：假设有H和L两个进程，H的安全级高于L，H企图将信息传递给L。它们约定一系列间隔均匀的时间点t1，t2，t3，…（间隔时间至少允许两次CPU调度）。L在每个时间点都请求使用CPU，而H在每个时间点，若要发送0，则不请求使用CPU；若要发送1，则请求使用CPU（假设H的优先级高于L）。于是，在每个时间点，L若能立即获得CPU的使用权，则确认收到0，若要等待，则确认收到1。**

2、操作系统的硬件安全机制中，存储单元越小，存储保护的精度越高。那是不是可以认为存储单元越小越好？存储单元过大除了存储保护的精度低外，还会对系统造成什么影响？

**若存储单元过小，会导致文件存储时分散到不同的存储区域，从而占用较多的页面，导致文件或进程的页表长，换页的频率过高，降低程序运行效率。**

**若存储单元过大，存储保护精度低，容易产生内存碎片，降低内存利用率。**