1、 信息系统安全威胁有哪四种？用实例阐明这几种威胁含义与特点。

截取：

含义：未授权方获得了访问资源权利，

特点：损失容易发现，人不容易抓住

例子：非法拷贝程序

中断：

系统资源丢失，不可得或不可用

恶意硬件破坏，程序，数据文献被删除

篡改：

未授权方不但访问资源，还修改资源

变化数据库某些值

伪造：未授权方也许在计算系统中假冒对象

入侵者也许在数据库中加入记录

2、 信息系统安全目的体当前哪三个方面？与上述四种安全威胁有何关系？

机密性，完整性，可用性

截取、篡改、伪造针对机密性，

中断、篡改针对完整性，

中断针对可用性。

3、计算机入侵最易渗入原则（最薄弱环节原则）指是什么？对安全管理工作有何指引意义？

一种入侵者总是企图运用任何也许入侵手段。这种入侵没有必要通过显而易见手段，也没有必要针对安装有最可靠防御系统。

1） 这条原则暗示安全专家们要考虑到所有也许入侵所有方式，

2） 入侵分析必要重复进行

3） 片面加强一种方面有也许引来入侵者对另一种方面兴趣

4、本课程所涉及几种古典加密算法加密过程。(涉及替代算法和置换算法)

替代算法：

凯撒密码（有无密钥），将某一字母直接替代为另一字母。

一次一密乱码本：与消息接受者共用一本密钥，每个密钥每次发信/接受即作废。明文+密钥=密文（弗吉尼亚表）。

破解办法：词频分析。

置换算法：

基本行列置换：横着写，竖着读。

带密钥行列置换：取密钥长度为段长，按照密钥字母字典序对每段排序。

破解办法：字母组分析破译法。

5、DES加密算法基本思路；DES加密与解密算法关系以及证明。

输入（64），初始置换，低块（32）作为新高块（32），低块加密（32），低块扩展（48），密钥移位，选取置换（64->56->48），扩展低块（48）与密钥（48）按位异或，替代[S盒，每组6位替代为4

位](48->32），排列，与高块（32）相加（32），作为新低块（32），循环16次，逆初始置换。（每次循环密钥移动不同位数）

S盒：行列选取（6->4）

加密与解密使用同一种算法，解密密钥是加密密钥逆序。证明见PPT P66。

6、何为对称(秘钥)加密算法和非对称(公钥)加密算法？试阐明各自特点以及重要应用场合。

对称密钥又称秘密密钥，需要发送、接受双方保证密钥保密性。非对称密钥又称公钥加密，公钥可公开。

加密解密速度：对称密钥快，非对称密钥慢。

密钥数量：

对称密钥：新顾客加入顾客组需要与其她顾客互换密钥，复杂，难度大。

非对称密钥：只需加一组公-私钥。

加密内容：

对称密钥：数据块，文献。

非对称密钥：身份鉴别，对称密钥互换。

7、密码哈希(Hash)函数特点与作用

特点：单向性，迅速性，抗碰撞性，雪崩性，定长输出。

作用：用于生成消息摘要，数字指纹，确认信息完整性，数字签名，数字证书。

8、基于Hash函数实现消息认证几种典型方案

1)

在文献末尾附加文献消息摘要，用对称密钥加密消息与摘要，接受者收到后先用对称密钥解密，再将文献用同样hash函数运算，所得摘要与附加摘要进行比对。

2）仅用对称密钥加密消息摘要。

3）仅用接受者公钥加密消息摘要。

9、密钥互换目与实现

公钥加密速度较慢无法满足即时通讯，而对称密钥加密需要密钥保密。对称加密密钥较短，用非对称加密算法进行加密、通信，建立一种受保护信道。

实现：A使用B公钥加密随机生成密钥Ka，B使用A公钥加密随机生成密钥Kb，A、B分别用自己密钥解密得到Kb、Ka，Ka与Kb相加作为对称密钥。进行安全传播。

10、数字签名作用，数字签名与验证过程。

作用：验证信息发送者（身份认证）。确认数据完整性，不可否认性。保证传播过程中不被非法篡改，破坏，并能对消息发送者进行身份认证，防止其对发送消息进行抵赖，也能防止袭击者冒充别人发送虚假信息。

签名过程：发送者使用发送者私钥对消息摘要进行加密，将明文与加密摘要发送给接受者。

验证过程：接受者使用发送者公钥对消息摘要进行解密，并用相似哈希函数进行比对。

完整过程：A使用A私钥对消息摘要签名，使用随机生成对称密钥K对明文加密，使用B公钥对K加密，密文+密钥+签名发送给B。B使用B私钥对K解密，使用K对密文解密得到明文，使用同样哈希函数对其运算得到一组摘要，使用A公

钥对发送来加密摘要解密，并于自己运算得到摘要比对。

11、证书作用以及有关实现机制

作用：通过第三方，对不结识双方可信度进行担保。

实现：每个需要验证员工将自己信息与公钥用自己私钥加密发送给上司，上司附上自己信息与公钥，用自己私钥加密，若不存在上司，则该员工为根节点。验证过程：某员工使用根节点公钥解密得到第二层上司公钥，使用第二层上司公钥解密到第三层，……，直到找到需要确认身份对方或找到最底依然没有找到对方（验证失败）。

12、何为缓冲区溢出漏洞？它也许会产生哪些危害？

访问非法内存区域。

危害：若溢出到顾客数据空间，则影响程序运营成果；若溢出到顾客代码空间，则程序运营出错；若一出道系统数据或系统代码空间时，也许引起系统操作成果错误，系统操作逻辑错误，甚至引起系统崩溃。

13、举例阐明何为“检查时刻到使用时刻(TOCTTOU)”漏洞？简述其解决方案。

运用检查到使用时间差实现篡改。例如：假钞掉包。

解决方案：数字签名，访问控制仲裁器。

14、计算机病毒特点以及运营机制。（涉及老式计算机病毒、宏病毒以及蠕虫病毒）

老式计算机病毒：附着于宿主程序，通过运营宿主程序传染，传染目的为本地文献。

宏病毒：Office宏中恶意代码，运营宏时发作，传染目的为Office软件有关文档。

蠕虫病毒：独立程序，积极袭击，传染目的为网络计算机。

老式病毒机制：宿主程序运营->检查病毒与否驻留内存（若未驻留则将病毒驻留于内存，修改中断向量、中断服务程序）->[等待触发中断]->相应中断触发->[传染、袭击开始]->文献与否有传染标志（若没有传染标志，则进行传染）->进行相应袭击（通过各种中断体现）。

PS：此类计算机病毒会通过变化进驻途径（如感染设备驱动程序，改首尾链接为中间插入，修改文献首簇号以一方面进驻系统）修改中断屏蔽寄存器禁止单步调试，减少代码可读性，避免修改中断向量，维持宿主外部特性，不使用明显传染标志，加密等办法提高隐蔽性。

蠕虫病毒机制：扫描系统漏洞->获得主机管理员权限->通过本机与其相连网络计算机交互将自身复制到新主机并启动。重要通过电子邮件、恶意网页、共享网络资源、聊天工具等形式传播。

宏病毒机制：

加载过程：宏病毒普通保存在自动宏，原则宏中。当顾客打开了感染病毒文档后，宏病毒就会被激活，获得对文档控制权，转移到计算机上，并驻留在Normal等模板上。

传染过程：感染宏病毒后，所有用到这些模板定义宏Office文献都会染上宏病毒，并会随着这些文档传播到其她计算机上。

破坏过程：对Office文档进行破坏，或调用系统命令，对系统进行破坏。

15、木马程序特点、功能以及运营机制。（从程序构造、植入方式、控制

等几方面阐述）

特点：[Client/Server概念]木马程序不会自我繁殖，或刻意传染其她文献，通过伪装自身吸引顾客下载执行[隐蔽性，自动运营性，欺骗性，自动回答性，自动打开端口]，有些木马除了普通文献操作，尚有搜索cache中口令，设立口令，扫描IP，记录键盘，注册表操作等。

功能：为木马发送者提供操控被害者计算机门户，实行各种破坏，窃取，远程操控[资源浏览，远程控制（I/O），窃取信息，发送信息]。

运营机制：黑客将木马服务端加以伪装，在网络上发布，通过Email、网页等Server程序植入[间接入侵法，直接入侵法，伪装法，网页法，Email法]。袭击阶段：联机，设立[设立合同，端口，连接密码，插件]并使用木马客户端扫描已被感染计算机（检查Email获得被黑者IP地址），运营客户端，输入相应IP地址联机，开始操作。

16、何为跳板入侵？分析其原理以及实现办法。

黑客通过控制第三方计算机，使用port转向袭击目的计算机，以达到隐藏身份目。通过修改服务端口实现。

17、何为间谍程序？分析其特点以及危害。避免间谍程序侵入对策。

在顾客不知情状况下安装，截获某些机密信息发送给黑客程序。

特点和危害：安装后很难察觉，计算机很容易感染间谍程序，大某些为广告程序（将顾客购买习惯发送，以进行有针对性推销活动），大多数间谍程序会干扰浏览器正常运营，泄露隐私。

避免被侵入对策：间谍程序植入方式有软件捆绑，恶意网站，邮件发送。相对对策：不浏览不健康、无安全证书站点，不在非正规网站下载软件，不收阅陌生人电子邮件。另一方面可以安装防火墙进行监控，不定期运用反间谍软

件搜索，查杀。

18、何为陷门？何为salami袭击(腊肠袭击)？

陷门：通往一种模块内部入口，在文档中没有记录。陷门普通在开发期间加入，目是供开发者更以便调试程序，或者为将来模块修改和功能增强提供入口，或者程序失效时一种维护通道。若没有维护好，容易被黑客运用获得系统控制权。

腊肠袭击：运用数据精度限制，获得精度无法记录获利，而许多账户累积起来获利非常可观。例子见书。

19、何为隐蔽通道？试阐明它普通有哪些实现办法？

隐蔽，看似合理地将信息传送给黑客。

实现办法：存储通道，运用存储器中与否有某个特定目的传递信息；文献上锁通道，通过鉴定一种文献与否被上锁传递一位信息；时间通道，通过事件发生速度来传递信息。

20、试简述操作系统对普通对象惯用访问控制办法，分析这些办法特点并比较之。

操作系统中，对普通对象访问控制采用访问目录、访问控制列表和访问控制矩阵三种控制办法。

采用访问目录控制办法，每个顾客都需要一张访问目录表，该列表指定了该顾客可以访问对象以及访问权限，该办法易于实现。但重要有三个问题，一方面，如果所有顾客都可访问共享对象太多，将导致列表太大；另一种问题是如果要撤除某一种共享对象访问权限，要更新列表也许诸多，开销很大。第三

个问题从文献划名关了。

基于访问控制列表控制办法：每个对象附有一种列表，列表中包括可以访问该对象所有主体，以及主体具有访问权限。这一控制办法可以在列表包括默认顾客以及相应访问权限，这样，特殊顾客可以在列表前面阐明其访问权限，而其他顾客则是默认访问权限。这一办法可以大大地减少控制列表，使维护更加以便。

访问控制矩阵是一张表格，每一行代表一种主体，每一列代表一种对象，表中每个元素都表达一种主体对某一种对象访问权限。总之来，访问控制矩阵是一种稀疏矩阵，由于许多主

体对大多数对象没有访问权。访问控制矩阵可以用一种形式为<主体，对象，权限>三元组表达。但是查找大量三元组效率太低，故很少使用。

21、试简述unix系统中Suid访问允许特点以及应用。

在unix系统中，可以通过对一种可执行文献设立suid位，使其他顾客在运行该程序时获得文献主访问权限，可以对该文献主其他文献拥有完全访问权限，而一旦退出该程序，顾客恢复其本来权限。

可以运用Suid访问允许特点做许多关于系统安全面工作。unix系统口令修改程序就是一种较好例子，任何顾客都可以且只能通过运营该程序来修改自己口令，而顾客自己则不能直接修改口令文献，保证了系统安全。

22、试简述口令袭击普通办法，并讨论一种安全口令选取要注意什么？如何构造一种安全鉴别系统？

口令袭击有在线口令袭击和离线口令两种。

在线口令袭击是通过截取口令，如果口令是加密，还要采用暴力袭击、字典袭击或猜测顾客也许口令等办法对口令进行解密。

离线口令袭击则通过度析系统中口令文献来获得有关口令。如果口令文献是加密，则可以采用暴力袭击、字典袭击或猜测顾客也许口令等办法对有关口令进行解密；如果口令文献是明文，则系统普通是通过设立访问权限办法控制对口令文献访问，袭击者可以通过运用操作系统缺陷来获取对口令文献访问权限、分析口令也许存储内存区或运用系统备份来获取有关口令。

可以通过如下办法来构造一种安全鉴别系统：

（1）帐户封锁。多次登陆错误，就封锁有关帐户。

（2）鉴别程序响应延时。发生一次登陆错误后，延时显示登陆界面。

（3）采用一次性口令。

（4）采用质询响应系统。

（5）采用<CTRL><ALT><Del>组合健保证安全鉴别。

（6）采用生物特性鉴别方式。

23、何为salt口令？其作用是什么？采用salt口令时顾客鉴别过程。

salt口令作用是防止在密文口令系统中通过查找相似口令密文来猜测口令，详细做法是在本来口令中加上扩展信息(即salt)，这样虽然口令相似，由于每个口令salt不同，最后口令密文也不同，避免了从相似口令密文推测口令也许性。salt可以是顾客ID+口令创立时间，创立顾客同步，在口令表中要登记相应salt，这样在顾客登录时，依照顾客输入顾客名，可以找到口令表中相应表目，再依照顾客输入口令附加上相应salt，按照相应单向加密算法，求得相应口令密文，跟口令表中口令密文做比对，以此来拟定顾客身份合法性。

24、试简述数据库两阶段更新方案。

如果在修改数据途中计算系统浮现故障，则数据库完整性有也许被破坏，为理解决此问题，数据库系统普通采用两阶段更新方案。

第一阶段称为意向阶段，在这个阶段计算成果，并将其保存于某些暂时变量中，这个阶段不会对数据库做任何修改，因此如果在期间系统浮现故障，所有操作可以等系统恢复时重做。

第一阶段最后事件是设立提交标记，意味着系统进入第二阶段，即永久更新阶段，在这个阶段数据库将前一种阶段保存于暂时变量计算成果复制到相应数据库字段中，如果在这个阶段系统浮现故障，则等系统恢复后只需重复第二阶段操作即可。提交标记为 0 或 1 是区别系统在哪个更新阶段浮现故障根据，数据库系统可以依照不同状况做不同解决。

25、举例阐明数据库记录推理袭击原理以及惯用对策。

数据库记录推理袭击是一种通过非敏感数据(如某些敏感数据记录成果)推断或推导敏感数据办法。例如可以综合运用某些敏感数据“和”和“计数”记录成果，揭露某个计数为 1 分类个体敏感数据。推理问题是数据库安全中一种很微妙弱点，惯用对策有查询控制和数据项控制，其中数据项控制涉及有限响应禁止、组合成果、随后样本和随机数据扰乱几种办法。

26、TCP/IP合同中各层作用是什么？各层提供服务有哪些？

27、DNS域名解析作用以及实现过程

28、钓鱼网站(Phishing，网络钓鱼)袭击原理以及防止办法

钓鱼网站袭击原理是伪装，通过将黑客控制网站伪装成另一网站，并发布在互联网上，吸引顾客点击链接并输入私密信息，然后进行网络欺诈，严重危

害互联网顾客利益，这种诱捕式袭击类似钓鱼活动，故叫钓鱼网站袭击。惯用方式有混淆域名和覆盖受害者主页。

防止办法：

（1）精确记忆惯用网址，输入时进入小心校对，以免疏忽大意进入此类网站。 （2）不要容易打开陌生人给网址，或不熟悉网址，谨防被骗。

（3）安装个人防火墙进行保护，并及时升级病毒库和补丁更新。也可以有安装专门拦截钓鱼网站安全软件，一旦发现此类网站便将其过滤掉。

29、典型MITM袭击手段哪些？试分析它们各自实现机制。(涉及ARP袭击、DNS欺骗、代理中间人袭击等)

中间人袭击就是一种恶意中间人可以通过截取加密通信密钥，偷听甚至修改某些通信内容。如果顾客A和顾客B要通过公钥体制进行加密通信，则中间人袭击实行过程如下：

（1）截取顾客A发往密钥服务器规定顾客B公钥祈求，代之以其对顾客B公钥祈求，传送给服务器。

（2）当服务器用顾客B公钥进行响应时候，她又将它截取下来，并将她自己公钥发送给顾客A。

（3）顾客A用获取公钥（事实上是中间人公钥）对数据进行加密，中间人将截取并解密，读取甚至修改其中内容，而后重新用顾客B公钥进行加密后，发送给顾客B。而以上这些状况顾客A和顾客B都很难有所察觉。

30、常用回绝服务(DoS)袭击有哪些？试分析各自特点以及实现机制

DoS是 Denial of Service简称，即回绝服务，导致DoS袭击行为被称为DoS袭击，其目是使计算

机或网络无法提供正常服务。最常用DoS袭击有计算机网络带宽袭击和连通性袭击。带宽袭击指以极大通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法顾客祈求就无法通过。连通性袭击指用大量连接祈求冲击计算机，使得所有可用操作系统资源都被消耗殆尽，最后计算机无法再解决合法顾客祈求。

（1）连接洪泛是运用ICMP(Internet Control Message Protocol，网间控制报文合同)一种网络袭击，而同步洪泛则是运用使用面向会话TCP合同组缺陷来实行袭击，它们本质都是回绝服务袭击。

（2）以常用连接洪泛袭击为例，如响应索取、死亡之Ping和Smurf袭击等，阐明其原理以及回绝服务袭击本质。

（3）同步洪泛袭击则要着重阐明三次连接握手过程，要解释被袭击运用面向会话TCP合同组缺陷。

31、何为分布式回绝服务(DDoS)袭击？试分析其特点以及实行过程。

机制：通过海量无用祈求占用正常服务通道使系统无法提供正常服务。

实行过程：扫描大量主机以寻找入侵目的->入侵有安全漏洞主机使其成为僵尸主机->在每台僵尸主机安装袭击程序->运用已扫描入侵主机继续扫描->袭击者发出袭击指令->僵尸主机向目的发起袭击。

32、分析ARP袭击、DNS欺骗原理以及实现机制。它们是如何实现中间人袭击和回绝服务袭击？

33、何为通信流推理威胁？简述对付通信流推理威胁惯用办法。

所谓通信流推理袭击是指通过度析网络通信流量变化和通信源地址和目的地址，来推理某些敏感信息。普通采用维护节点间流量平衡来抵抗流量分析，

还可以洋葱式路由通信控制方式来隐匿源节点和目的节点地址，，，

34、何为Tor路由（洋葱式路由）？试其作用以及实现过程。

35、SSL(Secure Sockets Layer)建立安全通信通道过程。HTTPS合同和FTPS合同特点以及安全机制。

（1）客户祈求一种SSL会话。

（2）服务器用它公钥证书响应，以便客户可以确认服务器真实性

（3）客户返回用服务器公钥加密对称会话密钥，服务器用它私钥解开。

（4）双方用共享会话密钥进行加密通信。

36、签名代码机制以及实现过程。

签名代码是让一种值得信赖第三方对代码进行签名，言外之意，使代码更值得信赖，通过数字签名来证明软件来源及发布者真实身份，签名后裔码将不能被恶意修改，这也保证了代码完整性，顾客下载到软件包时，也可以验证代码可信度。

实现过程：

（1）可信任第三方对代码计算哈希值，并用其私钥进行数字签名。

（2）顾客下载代码后，用该第三方公钥对其进行解密并得到该代码本来哈希值。

（3）重新求代码哈希值并与本来哈希值对比，若相似，则阐明该代码真实性由第三方保证，并且该代码没有被恶意修改过。

37、何为链路加密和端对端加密？试分析它们各自特点以及利弊。

38、在网络构造设计中如何考虑信息系统安全需求？

39、何为VPN？试分析其作用以及实现机制。

40、一次性口令（口令令牌）、质询响应系统（挑战响应系统）实行方案（原理、顾客鉴别过程）以及特点比较。

在一次性口令系统中，每个口令就只使用一次，每次鉴别采用不同口令。可以采用口令列表或口令令牌方式来管理一次性口令。口令列表中存储着可用口令，每次鉴别使用一种口令，顾客和主机使用相似口令列表，口令列表方式中对于口令列表维护是个难题；口令令牌方式使用硬件设备来产生不可预测口令序列，采用是同步令牌，这种设备能定期地（如每分钟）产生一种随机数，顾客读取设备显示数据，将它作为一种一次性口令输入，接受端主机执行算法产生适合于当前时刻口令，如与顾客输入口令相符，则顾客可通过鉴别。采用口令令牌方式要解决设备间时间偏差问题，此外两个口令之间一种时间间隔内，本来这个口令是可以重用，截取者有也许会运用这一弱点。

质询响应中，质询和响应设备看起来更象一种简朴计算器，顾客先到设备上进行鉴别（普通使用PIN），远程系统就会发送一种称为“质询”随机数，顾客将它输入到设备中，然后将该设备响应数字传递给系统。这种方式消除了顾客重用一种时间敏感口令弱点，并且没有PIN，响应生成器虽然落到其她人手中也是安全。

41、以祈求访问文献服务器中一种文献F为例，试从顾客身份鉴别、访问祈求授权、访问祈求实现三方面来阐述Kerberos系统运营机制以及特点。

在Kerberos系统中，该过程分如下三步实现：（1）启动一种Kerberos会话

在顾客登陆时，顾客工作站将顾客身份发送给Kerberos服务器，在验证该

顾客是已授权合法顾客后，Kerberos服务器发送给顾客工作站一种会话密钥SG和票据授权服务器(G)一种票据TG，其中用于与票据授权服务器通信，使用顾客口令进行加密：E(SG+TG，pw)；同步给票据授权服务器一种会话密钥SG拷贝和顾客身份，用Kerberos服务器与票据授权服务器之间共享KS-TGS密钥加密。

如果顾客可以使用它口令pw成功解密E(SG+TG，pw)，则该顾客通过了鉴别，事实上也认证了Kerberos服务器真实性。顾客口令存储于Kerberos服务器中，没有在网络上传送，保证了系统基本安全。

（2） 获得访问文献票据

顾客U向票据授权服务器发送一种用SG加密访问文献F祈求，票据授权服务器对U访问允许进行验证后，它会返回一种票据和一种会话密钥SF，其中SF将用于与文献服务器通信，返回票据包括了U已鉴别身份、F阐明、容许访问权限、会话密钥SF以及该票据有效日期等，票据使用一种票据授权服务器与文献服务器之间共享TGS-F密钥加密，顾客以及其她人不能读取、修改或伪造它，其中时间戳也在一定限度上保证了该票据不能被重用。

已加密票据和会话密钥SF通过SG加密后返回给顾客U，顾客解密后即可获得SF，以上这一种过程事实上也认证了票据授权服务器真实性。

（3） 向文献服务器祈求访问文献F

顾客U向文献服务器发送已用TGS-F密钥加密服务票据，文献服务器用TGS-

F密钥解密后，分析容许访问权限、票据时间戳等后，依照规定提供服务，随后文献传送数据是用会话密钥SF加密。

文献服务器能用TGS-F解密相应服务票据，也就认证了其身份真实性。

42、试从邮件（电子支票）机密性、完整性、发送者身份鉴别和加密密钥互换四个方面阐述安全邮件系统（电子支票系统）实现方案。

安全邮件系统普通结合了公钥（非对称）加密体制、密钥（对称）加密体制和数字签名技术，来保证邮件系统安全性和效率。

邮件系统机密性通过对邮件加密来实现，考虑加密解密效率，普通采用密钥（对称）加密体制，发送者用系统随机产生对称密钥对邮件进行加密后，再用接受者公钥对该对称蜜钥进行加密，并将其附在加密后邮件中，这样接受者收到加密邮件后，可以先用其私钥解密发送者事先用接受者公钥加密对称加密密钥，获得该对称密钥，就可以解密邮件，获得邮件明文。

在发送者对邮件进行加密此前，可以先获得该邮件消息摘要，并用其私钥对该消息摘要进行数字签名，并将数字签名后邮件消息摘要附在加密邮件中，这样接受者可以用发送者公钥解密加密消息摘要，并计算邮件当前消息摘要，如果与本来保存一致，就证明邮件没有被篡改，同步也确认了发送者身份。