# 1.中间人攻击的思想是什么？

假设有A、B两个人在进行通信，而第三个人C可以同时解惑A和B的信息，C告诉A说它是B，C告诉B说它是A，A和B质检好像是在直接诶通信，其实它们都是在和C通信，C作为中间人得到了A和B的通信内容。

# 2.试列出对称与非对称密钥加密的优缺点

（1）非对称加密算法解决了伸缩性和密钥协议与密钥狡猾问题，对称加密算法无法解决此问题；

（2）分队成加密算法加密速度慢，对称加密算法则快；

（3）非对称加密算法比对称密钥加密更大的密文块。

# 3.简述SSL的功能

**安全套接字层，SSL** 是一种安全协议，它为网络的通信提供私密性，工作在应用层和传输层之间。SSL使应用程序在通信时不用担心被窃听和篡改。SSL实际上是共同工作的两个协议，SSL记录协议和SSL握手协议。SSL记录协议是两个协议中较低级别的协议，它为较高级别的协议。例如SSL握手协议对数据的边长的记录进行机密和解密，SSL握手协议处理应用程序的交换和验证。

# 4.网络黑客留后门的原则是什么？

（1）留后门的功能是保持对目标主机的长期控制；  
（2）判断它的好坏取决于被管理员发现的概率  
（3）所以留后门原则是方便对目标主机的长久控制，且隐蔽性较好，不容易被发现

# 5.在DOS命令行下，添加一个用户Hacke，密码为123456的命令

net user Hacke add  
net user Hacke 123456

# 6.公钥交换存在什么问题？

发送方与接收方通过以下方式交换公钥并验证真实性：

（1）**数字证书认证**：发送方将公钥与数字证书绑定，证书由可信第三方（CA）签名，接收方通过CA公钥验证证书有效性。

（2）**数字签名验证**：发送方用私钥对公钥进行签名，接收方用发送方的公钥解密签名并验证其真实性。

（3）**密钥交换协议**：通过Diffie-Hellman等协议安全传输公钥，确保传输过程不被中间人截获。

（4）**公钥指纹核对**：双方预先共享公钥的哈希值（指纹），通过加密通道传递指纹以确认公钥未被篡改。

（5）**物理介质分发**：通过安全的物理介质（如U盘、硬件安全模块）传递公钥，限制非接收方访问。

非接收方无法识别公钥，因公钥在传输过程中被加密或仅在接收方的密钥管理系统中解密，且公钥与发送方身份绑定的验证过程需专用密钥完成。

# 7.计算机病毒活动时，经常有哪些现象出现？

① 屏幕显示异常，屏幕显示出不是由正常程序产生的画面或字符串，屏幕显示混乱；  
② 程序装入时间增长，文件运行速度下降；  
③ 用户没有访问的设备出现工作信号；  
④ 磁盘出现莫名其妙的文件和坏块，卷标发生变化；  
⑤ 系统自行引导；  
⑥ 丢失数据或程序，文件字节数发生变化；  
⑦ 内存空间、磁盘空间减小；  
⑧ 异常死机；  
⑨ 磁盘访问时间比平时增长；  
⑩ 系统引导时间增长。

# 8.怎样防范木马

**日常防范**  
 A.经常升级系统和更新病毒库  
 B.及时修补漏洞和关闭可疑的端口  
 C.尽量少用共享文件夹  
 D.运行实时监控程序  
 E.不要随意打开来历不明的邮件  
 F.不要随意下载来历不明的软件  
**被感染后的紧急措施**  
 A.所有的账号和密码都要马上更改  
 B.删掉所有你硬盘上原来没有的东西  
C.检查一次硬盘上是否有病毒存在

# 9.蠕虫的工作流程主要有哪几个阶段

（1）漏洞扫描

（2）攻击

（3）传染

（4）现场处理

# 10.简述计算机网络安全定义及核心。

**信息安全**是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。其核心是通过计算机网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的信息的保密性、完整性、真实性、可靠性、可用性和不可抵赖性等。

# 11.列举出网络的加密传输方式。

（1）链路到链路的加密传输方式；（2）节点到节点的加密传输方式；(3）端到端的加密传输方式。

# 12.VPN有那几个实现层次？各个层次代表协议或技术是什么？

（1）**数据链路层**，代表协议有PPTP（或L2TP）（2）**网络层**，代表协议有IPSec（或GRE或IP overIP）；（3）**会话层（或传输层）**，SSL（或SOCKS）；（4）**应用层**，采用代理技术

# 13.数据库加密方法有哪几种？

（1）密本方式；

（2）密码块链方式；

（3）子密钥数据库加密技术；

（4）秘密同态技术。

# 14.计算机病毒检查方法有哪些？

（1）比较法；（2）搜索法；（3）特征字识别法（4）分析法。

# 15.当通信双方发生了下列情况时，数字签名技术必须能够解决引发的争端：

1.否认，发送方不承认自己发送过某一报文。

2.伪造，接收方自己伪造一份报文，并声称它来自发送方。

3.冒充，网络上的某个用户冒充另一个用户接收或发送报文。

4.篡改，接收方对收到的信息进行篡改。

# 16.现代通信中易受到的攻击有哪些？解决方法是什么？

1.泄露

2.通信量分析

3.伪装、伪造

4.内容篡改

5.序号、计时篡改

6.否认抵赖

至于解决方法，

1.（1）（2）采用加密

2.（3）（4）（5）采用报文鉴别

3.（6）采用数字签名

# 17.列举因特网电子商务系统必须保证网络安全的四大要素。

1.传输数据的保密性；

2.交易各方身份的真实性；

3.交易的不可抵赖性；

# 18.给出序列密码和分组密码的实现原理，并给出各自的优缺点

**对称密钥密码系统**：如果加密密钥和解密密钥相同或相近，由其中一个很容易地得出另一个，这样的系统称为对称密钥密码系统。在这种系统中，加密和解密密钥都需要保密。**非对称密钥密码系统**：如果加密密钥与解密密钥不通，且由其中一个不容易得到另一个，则这种密码系统是非对称密钥密码系统。这两个不同的密钥，往往其中一个是公开的，另一个是保密的

# 19.什么是MD5？

**MD消息摘要算法**是由Rivest提出，是当前最为普遍的Hash算法，MD5是第5个版本，该算法以一个任意长度的消息作为输入，生成128位的消息摘要作为输出，输入消息是按512位的分组处理的。

# 20.数字签名有什么作用？

数字签名技术必须能够解决引发的争端：

1.否认，发送方不承认自己发送过某一报文。

2.伪造，接收方自己伪造一份报文，并声称它来自发送方。

3.冒充，网络上的某个用户冒充另一个用户接收或发送报文。

4.篡改，接收方对收到的信息进行篡改。

# 21.Windows NT的网络安全性依赖于给用户或组授予的哪3种能力？

**（1）权力**  
在系统上完成特定动作的授权，一般由系统指定给内置组，但也可以由管理员将其扩大到组和用户上。适用于整个系统范围内的对象和任务的操作。当用户登录到一个具有某种权力的帐号时，该用户就可以执行与该权力相关的任务。

（2）**共享**  
用户可以通过网络使用的文件夹，只适用于文件夹（目录），如果文件夹不是共享的，那么网络上就不会有用户看到它，也不能访问。

（3）**权限**  
权限适用于对特定对象如目录和文件（只适用于NTFS卷）的操作，指定允许哪些用户可以使用这些对象以及如何使用。权限分为目录权限和文件权限，每一个权限级别都确定了一个执行特定的任务组合的能力，这些任务是：Read(R)、Execute(X)、Write(W)、Delete(D)、Set Permission(P)和Take Ownership(O)。

# 22.说明SSL的概念和功能。

**SSL协议的功能**  
安全套接层协议SSL主要是使用公开密钥体制和X.509数字证书技术保护信息传输的机密性和完整性，但它不能保证信息的不可抵赖性，主要适用于点对点之间的信息传输。它是Netscape公司提出的基于Web应用的安全协议，它包括服务器认证、客户认证(可选)、SSL链路上的数据完整性和SSL链路上的数据保密性。SSL通过在浏览器软件和Web服务器之间建立一条安全通道，实现信息在Internet中传送的保密性。

**SSL在TCP/IP中的位置**  
在TCP/IP协议族中，SSL位于TCP层之上、应用层之下。这使它可以独立于应用层，从而使应用层协议可以直接建立在SSL之上。SSL协议包括以下一些子协议；SSL记录协议、SSL握手协议、SSL更改密码说明协议和SSL警告协议。

**SSL的子协议**  
SSL记录协议建立在可靠的传输协议(例如TCP)上，用来封装高层的协议。SSL握手协议准许服务器端与客户端在开始传输数据前，能够通过特定的加密算法相互鉴别。

# 23.解释访问控制的基本概念。

（1）访问控制是建立在身份认证基础上的，通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

（2）访问控制的目的：限制主体对访问客体的访问权限（安全访问策略），从而使计算机系统在合法范围内使用。

# 24.说明TLS和SSL的异同点。

传输层安全TLS是建立在SSL 3.0协议基础之上。在传输层上，TLS在源和目的实体间建立了一条安全通道，提供基于证书的认证、信息完整性和数据保密性。

# 25.现有的数字证书由谁颁发，遵循什么标准，有什么特点？

**数字证书**是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心(CA)作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。认证中心颁发的数字证书均遵循X.509 V3标准。X.509标准在编排公共密钥密码格式方面已被广为接受。X.509证书已应用于许多网络安全，其中包括IPSec(IP安全)、SSL、SET、S/MIME。

# 26.数字证书的原理是什么？

**数字证书**采用公开密钥体制（例如RSA）。每个用户设定一仅为本人所知的私有密钥，用它进行解密和签名；同时设定一公开密钥，为一组用户所共享，用于加密和验证签名。  
采用数字证书，能够确认以下两点：  
(1) 保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。  
(2) 保证信息自签发后到收到为止未曾做过任何修改，签发的信息是真实信息。

# 27.VPN有哪些分类？各应用于何种场合？

**内部VPN：** 如果要进行企业内部异地分支结构的互联，可以使用Intranet VPN的方式，即所谓的网关对网关VPN。在异地两个网络的网关之间建立了一个加密的VPN隧道，两端的内部网络可以通过该VPN隧道安全地进行通信。  
**远程VPN：** 公司总部和远程雇员或旅行之中的雇员之间建立的VPN，通过拨入当地的ISP进入Internet再连接企业的VPN网关，在用户和VPN网关之间建立一个安全的“隧道”，通过该隧道安全地访问远程的内部网（节省通信费用，又保证了安全性）。拨入方式包括拨号、ISDN、ADSL等，唯一的要求就是能够使用合法IP地址访问Internet。  
**联网VPN：** 如果一个企业希望将客户、供应商、合作伙伴连接到企业内部网，可以使用Extranet VPN。其实也是一种网关对网关的VPN，但它需要有不同协议和设备之间的配合和不同的安全配置。

# 28.IDEA是对称加密算法还是非对称加密算法？加密密钥是多少位？

IDEA是一种对称密钥算法，加密密钥是128位。初始级，可管理级，可定义级，可预知级，优化级。

# 29.常用的网络安全注入方式有哪些？

**SQL 注入：** 通过在 SQL 语句中注入恶意代码来执行不受信任的操作，以获取敏感数据或者篡改数据。

**命令注入：** 攻击者将能够执行不受信任的操作的命令注入到应用程序中。

**LDAP 注入：** 利用 LDAP 查询中的漏洞来获取敏感信息或者更改应用程序的行为。

**OS 注入：** 利用操作系统的漏洞，向服务器输入不受信任的数据，以利用操作系统上的缺陷来执行可疑操作。

**XML 注入：** 利用 XML 编辑器中的漏洞创建恶意 XML 代码的攻击

），两者不能兼容。