一．单选题。(1’x5=5’)

1.攻击者在局域网段发送虚假的 IP-MAC 对应信息，篡改网管 MAC 地址，使自己成为假网关的攻击是(C)。

A.MAC 欺骗　B.DNS 欺骗　C.ARP 欺骗　D.IP 欺骗

2.关于 Hash 函数下列描述不正确的是(B)。

A.把变长的信息映射到定长的信息　B.hash 函数具备可逆性

C.hash 函数速度较快　D.hash 函数可用于数字签名

3.代理防火墙工作在(D)。

A.传输层　B.网络层　C.数据链路层　D.应用层

4.下面哪一个不属于入侵系统的常见步骤(D).

A.系统漏洞扫描　B.安装系统后门　C.获取系统权限　D.传播病毒

5.公钥密码算法属于(C).

A.单向函数　B.带环-置换网络　C.陷门单向函数　D.模式变换

二．填空题。(1’x15=15’)

1.信息安全主要包括五个属性或安全需求，分别是可用性、保密性、可靠性、完整性、不可抵赖性。

2.P^{2}DR 模型包括：策略、保护、检测和响应等四个部分。

3.密码算法有不同的安全等级，包括无条件安全性、计算安全性和可证明安全性。

4.乘积密码通过交替代换和置换破坏对密码系统进行的各种系统分析，这种思想深刻影响着现代密码体制的设计，如数据加密标准 DES 和高级数据加密标准 AES。

5.可以用来做消息认证的函数主要有三类，分别是消息加密函数，MAC 和 HASH 函数。

6.PKI 包括认证机构 CA、注册机构 RA、证书库、档案库和 PKI 的用户等，其中 CA 是 PKI 的核心组成部分。

7.重放攻击是身份认证协议的主要威胁之一，为了抵御重放攻击通常采用的方法是在认证协议中加入一次性随机数和时间戳，或采用口令序列。

8.状态监测防火墙在 TCP 连接建立前使用包过滤规则进行数据包匹配过滤，在 TCP 连接建立好后用状态表进行数据包匹配过滤。

三．多选题。(2’x10=20’)

1.在信息安全体系结构中目前主要的安全服务有哪些？(ABCEF)

A.认证服务　B.不可否认服务　C.机密性服务

D.审计服务　E.完整性服务　F.访问控制服务

2.对公开密钥密码体制下列说法正确的是(ABD).

A.每个用户产生一堆密钥，公开密钥和私有密钥　B.加密算法和揭秘算法都公开

C.私有密钥由公开密钥决定，可以从公开密钥计算出私有密钥　D.基于数学难题

3.公钥以证书形式进行分配和管理，公钥证书用来绑定通信实体身份和对应公钥的凭证，公钥证书的内容包括(ABC)。

A.持有证书的通信实体标识符　B.公钥值

C.可信第三方签名　D.签名私钥

4.以下的常用算法中，属于对称加密算法的有(AC)，属于非对称加密算法的有(D)，属于 hash 函数的有(BE)。

A.DES　B.SHA　C.AES　D.RSA　E.MD5

5.下列实体或信息，能用于身份认证的有哪些？(ABCD)

A.口令　B.密钥　C.智能卡　D.指纹

6.访问控制的实现方法有哪些？(ABCDEF)

A.访问能力表　B.访问控制安全标签　C.加解密

D.访问控制表　E.访问控制矩阵　F.授权关系表

7.缓冲区溢出攻击是针对程序空间的哪些部分进行溢出？(BD)

A.代码段　B.栈　C.数据段　D.堆

8.公钥密码体制主要是针对对称密码体制的缺点而提出，它主要解决了下列哪些问题?(CD)

A.增强加密强度　B.提高加密速度　C.密钥管理和交换　D.数字签名

9.分组过滤防火墙可以根据哪些信息对数据包进行过滤？(ABCD)

A.IP 地址　B.数据包(协议)类型　C.端口　D.TCP 标志位

10.入侵检测系统通过在系统关键点收集并分析信息判断系统是否存在入侵行为，入侵检测信息收集的来源包括下列哪些?(ABCD)

A.程序执行中的异常行为　　B.网络流量

C.系统或网络的日志文件　　D.系统目录和文件的异常变化

四．简答题。(5’x5=25’)

1.简述什么是分布式拒绝服务攻击，如何进行预防？

借助客户/服务器技术，入侵并控制若干存在安全漏洞的计算机（作为傀儡或肉鸡）联合起来作为攻击平台——僵尸网络，通过主控程序与代理程序通讯，发送攻击指令，操纵傀儡主机同时对一个或多个目标发动 DoS 攻击。主控程序能在几秒钟内激活成百上千个代理程序的运行。成倍地提高拒绝服务攻击的威力。

预防：网络出口禁 IP 欺骗；无驱动力；建立纵深体系。

2.结合 C 语言在函数调用及返回时的堆栈操作过程，说明缓冲区溢出攻击的原理，以及缓冲区溢出攻击的防范机理？

栈溢出攻击的原理：

编译后 C 程序运行时，内存空间：代码段、数据段和堆栈段，堆和堆栈都可以被利用来进行溢出。

缓冲区溢出修改栈中返回地址，使其指向 Shellcode；函数返回，EIP 取篡改后的返回地址，并执行 Shellcode

缓冲区溢出攻击原理：通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈（超出部分写入（覆盖）其他缓冲区），使程序转而执行其它指令（恶意代码 shellcode），以达到攻击的目的。

防范原理：

1、防止缓冲区溢出：a)采用安全 C 语言库函数最新版本 strcpy()——》strncpy(), printf()——》sprintf()等; b)程序员检查数组与指针等越界代码;

2、允许溢出但不允许改变控制流（禁止未经授权控制流的改变）

3、允许改变控制流但禁止敏感代码执行（禁止攻击代码执行，如禁止诸如 exec()等系统调用函数的非法使用）

3.简述加盐口令身份认证机制，分析加盐的作用，说明该认证机制能否抵抗重放攻击，如不能如何抵御该攻击？

密码通过加盐后，可以增加密码的复杂度，即便最简单的密码，在加盐后，也能变成复杂的字符串，这大大提高了密码破解的难度。但是如果将盐硬编码在程序中或随机一次生成的，每个密码进行 hash 使用相同的盐会降低系统的防御力，因为相同密码的 hash 两次后的结果也是一样的。所以比较正确的做法是每次创建用户或修改密码都使用一个新的随机盐。

重放攻击(Replay Attacks)是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器。重放攻击在任何网络通过程中都可能发生，是计算机世界黑客常用的攻击方式之一。

(1)加随机数。该方法优点是认证双方不需要时间同步，双方记住使用过的随机数，如发现报文中有以前使用过的随机数，就认为是重放攻击。缺点是需要额外保存使用过的随机数，若记录的时间段较长，则保存和查询的开销较大。

(2)加时间戳。该方法优点是不用额外保存其他信息。缺点是认证双方需要准确的时间同步，同步越好，受攻击的可能性就越小。但当系统很庞大，跨越的区域较广时，要做到精确的时间同步并不是很容易。

(3)加流水号。就是双方在报文中添加一个逐步递增的整数，只要接收到一个不连续的流水号报文(太大或太小)，就认定有重放威胁。该方法优点是不需要时间同步，保存的信息量比随机数方式小。缺点是一旦攻击者对报文解密成功，就可以获得流水号，从而每次将流水号递增欺骗认证端。

(4)还可以使用挑战一应答机制和一次性口令机制

4.为了阻止木马被发现，木马的设计者通常会采用多种手段(或多个方面)隐藏，试分类说明常用的木马隐藏手段及如何防范木马？

木马为了规避杀毒软件，防止被发现，增加生命周期，通常在进入系统后会以各种方法隐藏其行踪，木马的隐藏能力直接决定了木马的攻击效果。主要分为三种方式：文件隐藏、进程隐藏、通信隐藏。

文件隐藏是指木马程序通过伪装目标磁盘文件，让用户在表面上难以辨别出木马程序，通常的**文件隐藏**方法如下：

（1）嵌入宿主文件。采用此方法的木马主要是嵌入到系统文件中，当启动系统时，木马随即启动，有的也是捆绑到某个应用程序中，当此程序被用户使用时，木马也跟随启动。

（2）修改文件属性，很多木马会把文件释放到 windows 或者 windows\system32 等系统目录下，而且会修改此文件的生成日期，以此来迷惑用户。

（3）文件替换。也叫 DLL 技术，是木马程序发展的一种比较新的技术产物。这种技术的精髓所在是将系统原来的 DLL 替换为木马 DLL，将原来的 DLL 修改并保存为其他名称，并且过滤进程对此系统 DLL 函数的调用，对于正常的调用，木马 DLL 直接转发给原来的系统 DLL，当接到特殊的调用时，木马 DLL 就行行相关的操作。

最简单的**进程隐藏**方式：（1）进程名字迷惑（2）把木马写入到驱动和内核的级别：通过拦截系统调用的服务，替代或嵌入系统功能（驱动程序或动态链接库）如，将木马嵌入 windows.exe，系统运行 windows.exe，实际上同时运行了木马和 windows.exe。（3）木马进程不容易发现，发现后没法或不允许删除.

木马的**通信隐藏**方法有以下 2 种：

（1）端口隐藏。一般来讲，木马植入主机后，会选择 1024 等高端口上驻留，也有部分木马采用端口复用技术，选择常用端口。

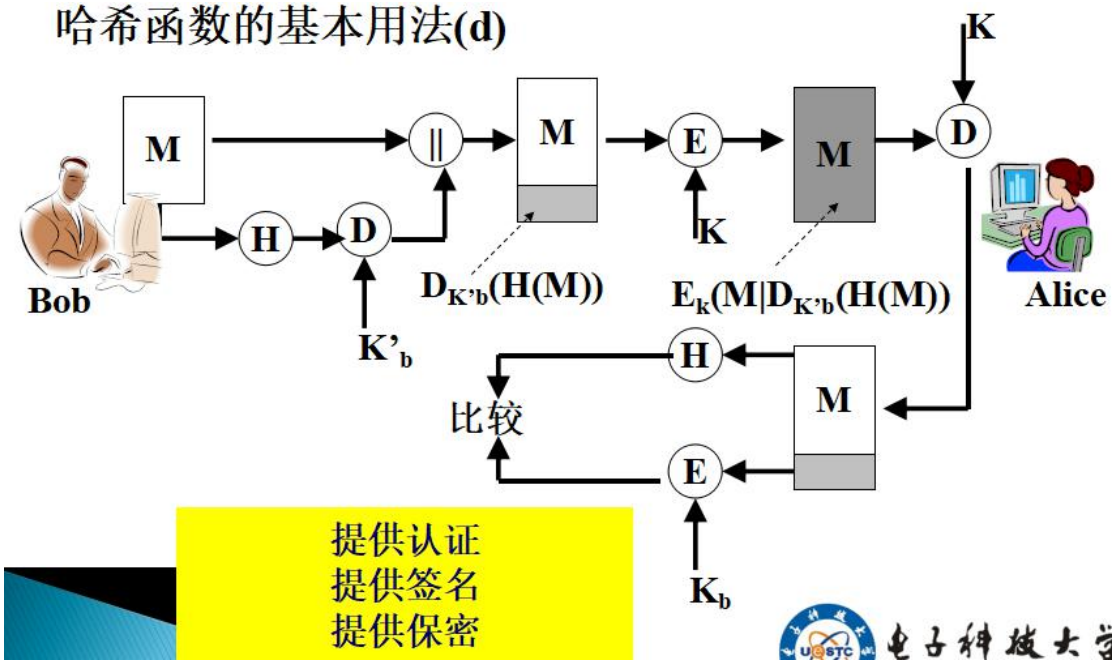
（2）反向连接技术，反弹端口型木马采用的采用的是反向链接的编程方法，即：服务器端（被控制端）采用主动端口，客户端（控制端）采用的是被动端口.

防范木马:

(1)技术手段：运行实时监控程序：防火墙、防病毒软件；端口扫描；查看连接。

(2)安全意识：不要随意打开来历不明的邮件；不要随意下载来历不明的软件；及时修补漏洞和关闭可疑的端口；尽量少用共享文件夹；经常升级系统和更新病毒库。

5. 假设明文用 M 表示，H( )为 hash 函数。Ekx（）表示为用户 x 的私钥签名函数，表示密钥为 K 的对称加密函数。Alice 为发送方，Bob 为接收方。试结合对称密码体制和公钥密码体制的优缺点，运用对称密码体制，公钥密码体制和 hash 算法，设计一个涵盖保密、认证、数字签名和数字信封的通信模型。



三、设计题。(共 35')

1、用户数据的安全性和隐私保护是制约云计算发展和应用的主要障碍之一，试结合本课程分析信息安全技术说明如何解决云计算环境中的数据安全和隐私保护问题？

隐私保护问题：在云计算平台的存储系统中存在着许多种不同类型的数据，包括文档、视频、图片、电子邮件等等。每种数据对于用户来讲，数据的安全性和重要性都是有所差别的，这是因为这些数据中所涉及的信息的重要程度是不同的。对于上述数据根据重要程度进行等级划分，划分的依据是数据的重要程度和数据的敏感程度。对于不同需求的客户要采取不同的数据加密算法来对数据进行保护。

如果要对云平台设置一个数据安全的策略，那么就需要将数据的隐私级别和用户的隐私级别联系起来。作为云服务提供商可以根据数据对于用户隐私程度的不同来设定相应的隐私等级。可以将数据的隐私划分为三个等级：隐私级别 1：在这个数据隐私等级中不包括用户较为敏感的数据，该等级的数据可以采用较为简单的加密算法，使得系统的资源不至于被浪费太多。级别 2：在这个等级的数据当中有部分数据对于用户来讲是非常敏感的，那么就要针对这些数据区域，

采用与此等级相符的加密算法。级别 3：在这个级别的数据当中存在着大量的用户隐私数据，那么应该对该等级的数据采取较为复杂的加密算法使得数据的安全得到保证。

2、从互联网下载是用户获取软件应用的常见方式，但是存在软件发布方不可信及软件被恶意捆绑木马或后门的风险，试说明运用什么信息安全技术，怎么解决这一问题？

答：一、查看软件发布方的证书，验证证书，确保其安全性；二、借助一些反捆绑工具进行检测；三、搜索是否可疑文件是否带了 http://,.exe 这样的 URL 信息，并对其定位检测；四、硬盘监测，注册表监测，一旦硬盘和注册表出现变化或有新文件建立都会被记录；五、可从软件官网下载，降低风险；六、打开电脑管家-杀毒，打开小红伞引擎，这样可以增强查杀效果；下载软件后先扫描；安装过程中尽量不要用傻瓜式安装，自定义其安装路径，手动选择是否安装捆绑软件；七、及时对自己的电脑安装防火墙系统打补丁和对杀毒软件升级。

3、通过伪造的 Web 站点实施网络钓鱼是一种典型的网络欺骗攻击方式，诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信品牌或商家的网站，引诱受害者来点击，从而骗取受害者的私人信息，如信用卡号、银行卡账户、身份证号等内容。试运用相关信息安全技术，设计一套解决方案。（提示：从真实性、完整性和机密性等角度来思考设计）

核对网址，网上支付需选择第三方支付平台，切忌向个人账户汇款或转账，如发现自己的信息泄露，应及时挂失。

1、信息隐藏与数据加密的主要区别

信息隐藏将在未来网络中保护信息不受破坏方面起到重要作用,信息隐藏是把机密信息隐藏在大量信息中不让对手发觉的一种方法。信息隐藏的方法主要有隐写术、数字水印、可视密码、潜信道、隐匿协议等。

信息加密技术是利用数学或物理手段，对电子信息在传输过程中和存储体内进行保护，以防止泄漏的技术。保密通信，计算机密钥，防复制软盘 等都属于信息加密技术。

2、数字签名的概念，在信息安全中的主要作用

它的主要方式是，报文的发送方从报文文本中生成一个 128 位的散列值（或报文摘要）。发送方用自己的私人密钥对这个散列值进行加密来形成发送方的数字签名。然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出 128 位的散列值（或报文摘要），接着再用发送方的公用密钥来对报文附加的数字签名进行解密。如果两个散列值相同、那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别。

采用数字签名，也能确认以下两点：第一，信息是由签名者发送的；第二，信息自签发后到收到为止未曾作过任何修改。这样数字签名就可用来防止电子信息因易被修改而有人作伪，或冒用别人名义发送信息。或发出（收到）信件后又加以否认等情况发生。

3、对称密码体制和公钥密码体制的优缺点

对称密钥体制中，它的加密密钥与解密密钥的密码体制是相同的，且收发双方必须共享密钥，对称密码的密钥是保密的，没有密钥，解密就不可行，知道算法和若干密文不足以确定密钥。

优点：计算开销小，算法简单，密钥较短，加密速度快，目前用于信息加密的主要算法。

缺点：规模复杂；通信前安全密钥交换；没法鉴别，无法签名。

公钥密码体制中，它使用不同的加密密钥和解密密钥，且加密密钥是向公众公开的，而解密密钥是需要保密的，发送方拥有加密或者解密密钥，而接收方拥有另一个密钥。两个密钥之一也是保密的，无解密密钥，解密不可行，知道算法和其中一个密钥以及若干密文不能确定另一个密钥。

优点：密钥数量很小；密钥发布不成问题；数字签名

缺点：密钥尺寸大，加密 / 解密时的速度慢。

4、信息安全有哪些常见的威胁？信息安全的实现有哪些主要技术措施？

信息安全常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。

信息安全的实现可以通过物理安全技术，系统安全技术，网络安全技术，应用安全技术，数据加密技术，认证授权技术，访问控制技术，审计跟踪技术，防病毒技术，灾难恢复和备份技术。