1. 单选题。(1’x5=5’)
2. 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)。
3. MAC欺骗 B.DNS欺骗 C.ARP欺骗 D.IP欺骗
4. 关于Hash函数下列描述不正确的是(B)。
5. 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

1. 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

1. 填空题。(1’x15=15’)
2. 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。
3. P2DR模型包括：策略、保护、检测和响应等四个部分。
4. 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。
5. 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。
6. 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。
7. 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。
8. 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。
9. 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。
10. 多选题。(2’x10=20’)
11. 在信息安全体系结构中目前主要的安全服务有哪些？(ABCEF)
12. 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

1. 对公开密钥密码体制下列说法正确的是(ABD).
2. 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

1. 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)。
2. 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

1. 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)。
2. DES B.SHA C.AES D.RSA E.MD5
3. 下列实体或信息，能用于身份认证的有哪些？(ABCD)
4. 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

1. 缓冲区溢出攻击是针对程序空间的哪些部分进行溢出？(BD)
2. 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

1. 简答题。(5’x5=25’)
2. **简述什么是分布式拒绝服务攻击，如何进行预防？**

**答：**攻击者利用大量的傀儡主机向被攻击主机发送大量的合法的无用分组，造成被攻击主机CPU或者网络带宽资源耗尽，主要攻击对象是大型网站、搜索引擎、政府部门等站点。

预防：网络出口禁IP欺骗，无驱动力，各司其职协调防御，建立纵深体系。（1）尽可能对系统更新最新补丁，降低漏洞利用风险；（2）采取合适的安全域划分，配置防火墙，入侵检测和防范系统，减缓攻击；（3）采用分布式网络，负载均衡，提升系统容量等可靠性措施，增强总体服务能力。

采用高性能网络设备、尽量避免NAT的使用，充足的网络带宽保证，升级主机服务硬件，把网站做成静态页面。

1. **试结合C语言程序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？**

**答：**堆栈是一个先入后出的队列，他的生长方向与内存的生长方向正好相反，规定内存的生长方向为向上，栈则向下。

防范：（1）在系统管理上的防范：关闭不需要的特权程序，及时给程序漏洞打补丁（我天天打）；（2）在软件开发过程的防范：编写正确代码、缓冲区不可执行、改进C语言函数库、数组边界检查、使堆栈向高地址方向增长，程序指针完整性检查。

1. **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？**

**答：**盐是一种随机字符串，它与口令连接在一起，再用单向函数对其运算，然后将salt值和单向函数运算结果存入主机。

作用：增加系统复杂度，当盐与用户密码结合后，在通过摘要处理就能得到隐蔽性更强的摘要值，使密码更安全。

不能抵抗重放攻击。（1）一次性口令：在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同；（2）使用签名密钥签署某消息，签名包含一非重复值以抵抗重放攻击。

1. **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？**

答：常用隐藏手段：存放位置以及文件名、通信方式、进程隐藏三种。

防范：（1）技术手段：运行实时监控程序（防火墙、防病毒软件等）;端口扫描;查看链接。（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。

1. **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。**

**答：**

1. 设计题。(共35’)
2. **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？**

答：（1）加强云终端的安全控制，加强移动网络传输与接入的安全性。（2）加强对云服务业务的访问控制，针对业务系统制定一套安全统一的策略管理模式，以免业务流程被非法控制。（3）对互联网运营环境进行优化，对用户身份及IP地址严格管理，提高云服务下用户数据信息安全。（4）阅读隐私声明使用过滤器，使用过滤器对数据进行邮箱检测，确保数据在流失时可被及时发现。（5）云计算是将大量计算资源、存储资源和软件资源连接在一起，形成大规模虚拟共享资源地，在存储数据的时候，应该把数据交给公共数据中心统一加密处理。（应该也可根据信息安全几个方面比如可靠性、机密性等方面答）

1. **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：（1）禁止或监督非web源的协议在企业网络内使用。（2）确保在所有的桌面系统和服务器上安装最新的浏览器、操作系统、应用程序补丁，并确保[垃圾邮件](https://baike.baidu.com/item/%E5%9E%83%E5%9C%BE%E9%82%AE%E4%BB%B6)和浏览器的安全设置达到适当水平。（3）确保安装所有的[安全软件](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E8%BD%AF%E4%BB%B6)，并及时更新并且使用最新的威胁数据库。（4）不要授权普通用户使用[管理员](https://baike.baidu.com/item/%E7%AE%A1%E7%90%86%E5%91%98)权限，特别要注意不要让其下载和安装设备[驱动程序](https://baike.baidu.com/item/%E9%A9%B1%E5%8A%A8%E7%A8%8B%E5%BA%8F)，因为这正是许多恶意软件乘虚而入的方式。（5）制定处理恶意事件的策略，在多个部门组建可实现协调响应职责并能够定期执行安全培训的团队。（6）教育[员工](https://baike.baidu.com/item/%E5%91%98%E5%B7%A5)正确使用[电子邮件](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB%B6)和Web。

1. 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）