考试科目：网络安全理论与技术
考试形式：闭卷
考试时间：2016 年秋

一. （5 分） 单选题

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 (_____)。
   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 (_____)。
   A. 把边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 (_____)。
   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 (_____)。
   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 (_____)。
   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. （15 分） 填空题。

1. 信息安全主要包括五个属性或安全需求，分别是可用性、_____、可靠性、_____、不可抵赖性。
2. P^2DR 模型包括：策略、_____、检测和_____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、_____和_____。
4. 乘积密码通过交替_____和_____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、_____和_____。
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_____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_____和_____，或采用口令序列。
8. 状态检测防火墙在 TCP 连接建立前使用_____进行数据包匹配过滤，在 TCP 连接建立好后用_____进行数据包匹配过滤。

三. （20 分） 多选题。

1. 在信息安全体系结构中目前主要的安全服务由哪些?
   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. 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:
   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

3. 以下的常用算法中,属于对称加密算法的有 (_____),属于非对称加密算法的有 (_____),属于 hash 函数的有 (_____)。
   A. DES B. SHA C. AES D. RSA E. MD5
4. 对公开密钥密码体制下列说法正确的是 (_____)
   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
5. 下列实体或信息，能用于身份认证的有哪些？(_____)
   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？(_____)
   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？(_____)
   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?(_____)
   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？(_____)
   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?(_____)
    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. （25 分） 简答题。

1. 简述什么是分布式拒绝服务攻击，如何进行预防？

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?

3. 简书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?

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?

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。

五. （35 分） 设计题。

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?

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?

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）

六. 附加题

1. 信息隐藏和数据加密的主要区别

2. 数字签名的概念，在信息安全中的主要作用

3. 对称密码体制和公钥密码体制的优缺点

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？