**信息安全工程师每日一练试题（2017/4/1）**

试题**1**： ()不会影响原系统负荷。  
A、防火墙B、基于主机的入侵检测系统C、审计系统D、基于网络的入侵检测系统   
  
试题**2**： 由引擎上传中心的信息是()  
A、原始数据B、事件C、规则  
  
试题**3**： RPC 系列标准是由(  )发布的：  
A．国际标准化组织(ISO)B．国际电工委员会(IEC) C．国际贸易中心(ITC)D．互联网工程任务组IETF  
  
试题**4**： 电子商务交易必须具备抗抵赖性，目的在于防止（）。    
A、一个实体假装另一个实体B、参与此交易的一方否认曾经发生过此次交易  
C、他人对数据进行非授权的修改、破坏D、信息从被监视的通信过程中泄露出去

试题**5**： 以下关于隧道技术说法不正确的是（）  
A、隧道技术可以用来解决TCP/IP协议的某种安全威胁问题

B、隧道技术的本质是用一种协议来传输另外一种协议  
C、IPSec协议中不会使用隧道技术 D、虚拟专用网中可以采用隧道技术

试题**6**： 有关系统工程的特点，以下错误的是（）  
A.系统工程研究问题一般采用先决定整体框架，后进入详细设计的程序  
B.系统工程的基本特点，是需要把研究对象解构为多个组成部分分别独立研究  
C.系统工程研究强调多学科协作，根据研究问题涉及到的学科和专业范围，组成一个知识结构合理的专家体系  
D.系统工程研究是以系统思想为指导，采取的理论和方法是综合集成各学科、各领域的理论和方法

试题**7**： 风险管理过程的产出是做以下什么东西的依据（）  
A、业务计划B、审计章程。C、安全政策。D、软件设计。  
  
试题**8**： 一个每天处理百万交易的金融机构,会有一个中央通信处理器,用于连接自动柜员机,下面哪些是为通信处理的最好的应变计划.（）  
A、与另一个组织签订互助协议.B、在同一地点设立候补处理器

C、候补处理器在另一个网络节点 D、安装全双工的通讯联系   
  
试题**9**： 下列哪个选项，你期望知道组织的战略计划？（）

测试一个新的帐户包B、评估信息技术C、在接下的一年中实行一个新项目计划系统D、成为产品的供应商  
  
试题**10**： 怎样签发信息来保证接收到的电子邮件信息的可靠性和机密性：（）  
A．用发件人的私钥签名并且用收件人的公钥对信息进行加密  
B．用发件人的公钥签名并且用收件人的私钥对信息进行加密  
C．用收件人的私钥签名并且用发件人的公钥对信息进行加密  
D．用收件人的公钥签名并且用发件人的私钥对信息进行加密

**信息安全工程师每日一练试题（2017/4/2）**

试题**1**： 用于在网络应用层和传输层之间提供加密方案的协议是 （ ） 。  
A、PGP B、SSL C、IPSec D、DES   
  
试题**2**： 加密技术的三个重要方法是()  
A、数据加工、变换、验证B、封装、变换、身份认证C、封装、变换、验证  
  
试题**3**： 评估BCP时，下列哪一项应当最被关注：（）  
A.灾难等级基于受损功能的范围，而不是持续时间B.低级别灾难和软件事件之间的区别不清晰  
C.总体BCP被文档化，但详细恢复步骤没有规定D.宣布灾难的职责没有被识别  
  
试题**4**： 信息保障技术框架（IATF）是美国国家安全局（NSA）制定的，为保护美国政府和工业界的信息与信息技术设施提供技术指南，关于IATF的说法错误的是？（）  
A.IATF的代表理论为“深度防御”。  
B.IATF强调人、技术、操作这三个核心要素，从多种不同的角度对信息系统进行防护。  
C.IATF关注本地计算环境、区域边界、网络和基础设施三个信息安全保障领域。  
D.IATF论述了系统工程、系统采购、风险管理、认证和鉴定以及生命周期支持等过程。  
  
试题**5**： 下列关于计算机木马的说法错误的是（）。  
A、 Word文档也会感染木马B、 尽量访问知名网站能减少感染木马的概率  
C、 杀毒软件对防止木马病毒泛滥具有重要作用D、 只要不访问互联网，就能避免受到木马侵害  
  
试题**6**： 下面关于信息安全保障的说法正确的是:（）  
A.信息安全保障的概念是与信息安全的概念同时产生的  
B.信息系统安全保障要素包括信息的完整性、可用性和保密性  
C.信息安全保障和信息安全技术并列构成实现信息安全的两大主要手段  
D.信息安全保障是以业务目标的实现为最终目的，从风险和策略出发，实施各种保障要素，在系统的生命周期内确保信息的安全属性  
  
试题**7**： 与PDR模型相比，P2DR模型多了哪一个环节?（）  
A．防护B．检测C．反应D．策略

试题**8**： Which of the following provides the framework for designing and developing logical access controls?   
A、Information systems security policy B、Access control lists   
C、Password management D、System configuration files   
  
试题**9**： 当用作电子信用卡付款时，以下哪一项是安全电子交易协议的特性？  
A、买方被保证无论是商家还是任何第三方都不能滥用他们的信用卡数据  
B、所有的个人SET证书都被安全存储在买方的电脑中  
C、买方有义务为任何涉及到的交易提供个人SET证书  
D、由于不要求买方输入信用卡号和有效期，付款过程变得简单  
  
试题**10**： 在一个在线银行应用中，下面哪一个是最好的应对身份窃取的措施？（）  
A.对个人口令的加密B.限制用户只能使用特定的终端C.双因素认证D.定期审查访问日志

**信息安全工程师每日一练试题（2017/4/3）**

试题**1**： RSA是一种公开密钥算法，所谓公开密钥是指（ ）  
A.加密密钥是公开 B.解密密钥是公开 C.加密密钥和解密密钥都是公开 D.加密密钥和解密密钥都是相同  
  
试题**2**： 带VPN的防火墙一旦设置了VPN 功能，则所有通过防火墙的数据包都将通过VPN通道进行通讯()  
A、是B、否  
  
试题**3**： 组织在建立和实施信息安全管理体系的过程中，文档化形成的文件的主要作用是()  
A、有章可循，有据可查B、用于存档C、便于总结、汇报D、便于检查工作  
  
试题**4**： ISMS审核时，对审核发现中，以下哪个是属于严重不符合项？（）  
A.   关键的控制程序没有得到贯彻，缺乏标准规定的要求可构成严重不符合项  
B.风险评估方法没有按照ISO27005（信息安全风险管理）标准进行  
C. 孤立的偶发性的且对信息安全管理体系无直接影响的问题；  
D. 审核员识别的可能改进项  
  
试题**5**： OSI开放系统互联安全体系构架中的安全服务分为鉴别服务、访问控制、机密性服务、完整服务、抗抵赖服务，其中机密性服务描述正确的是：  （）  
A、包括原发方抗抵赖和接受方抗抵赖  
B、包括连接机密性、无连接机密性、选择字段机密性和业务流保密  
C、包括对等实体鉴别和数据源鉴别  
D、包括具有恢复功能的连接完整性、没有恢复功能的连接完整性、选择字段连接完整性、无连接完整性和选择字段无连接完整性  
  
试题**6**： 下列哪些措施不是有效的缓冲区溢出的防护措施？（）  
A．使用标准的C语言字符串库进行操作B．严格验证输入字符串长度  
C．过滤不合规则的字符D．使用第三方安全的字符串库操作  
  
试题**7**： TCP/IP中那个协议是用来报告错误并对消息进行控制（）  
A、ICMP B、IGMP C、ARP D、SNMP  
  
试题**8**： A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:   
A、analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.   
B、WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.   
C、the line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.   
D、users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.   
  
  
试题**9**： A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:   
A、recovery. B、retention. C、rebuilding. D、reuse.   
  
试题**10**： 一个备份站点包括电线、空调和地板，但不包括计算机和通讯设备，那么它属于（）  
A、冷站B、温站C、直线站点D、镜像站点

**信息安全工程师每日一练试题（AD）**

试题**1**： 网络安全包含了网络信息的可用性、保密性、完整性和真实性。防范Dos攻击是提高（1）的措施，数字签名是保证（2）的措施。  
（1）A.可用性 B.保密性 C.完整性 D.真实性  
（2）A.可用性 B.保密性 C.完整性 D.真实性  
  
试题**2**： 选择产品主要是看品牌与价格，尤其是价格越贵越好()  
A、是B、否  
  
试题**3**： 下面威胁中不属于抵赖行为的是:（）  
A、发信者事后否认曾经发送过某条消息B、收信者事后否认曾经接收过某条消息  
C、发信者事后否认曾经发送过某条消息的内容D、收信者接收消息后更改某部分内容

试题**4**： 应急方法学定义了安全事件处理的流程，这个流程的顺序是:（）  
A、准备-遏制-检测-根除-恢复-跟进B、准备-检测-遏制-恢复-根除-跟进  
C、准备-检测-遏制-根除-恢复-跟进D、准备-遏制-根除-检测-恢复-跟进

试题**5**： An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?   
A、The corporate network is using an intrusion prevention system (IPS)   
B、This part of the network is isolated from the corporate network   
C、A single sign-on has been implemented in the corporate network   
D、Antivirus software is in place to protect the corporate network   
  
试题**6**： When assessing the design of network monitoring controls, an IS auditor should FIRST review network:   
A、topology diagrams. B、bandwidth usage. C、traffic analysis reports. D、bottleneck locations.   
  
试题**7**： Which of the following will help detect changes made by an intruder to the system log of a server?   
A、Mirroring the system log on another server   
B、Simultaneously duplicating the system log on a write-once disk   
C、Write-protecting the directory containing the system log   
D、Storing the backup of the system log offsite   
  
试题**8**：  IT治理的最终目的是: （）  
A、鼓励最优地运用计算机. B、降低IT成本. C、在组织中分散IT资源. D、集中控制IT.   
  
试题**9**： 交易审计痕迹的主要目的是?: （）  
A、减少使用存储媒介. B、为处理交易确定问责制和责任制.   
C、帮助系统审计师进行细微审查. D、为能力规划提供有益的信息.   
  
试题**10**： 下列哪项会使得无线局域网抵制非授权的访问变弱：（）  
A、MAC地址过滤B、WPA协议C、LEAP轻量级可扩展认证协议D、SSID广播

**信息安全工程师每日一练试题（2017/4/5）**

试题**1**： 最早的计算机网络与传统的通信网络最大的区别是什么？()  
A、计算机网络带宽和速度大大提高。B、计算机网络采用了分组交换技术。  
C、计算机网络采用了电路交换技术D、计算机网络的可靠性大大提高。  
  
试题**2**： 网络安全设计足网络规划与设计中的重点环节，以下关于网络安全设计原则的说法，错误的是 ( )。

A．网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提

B．强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失

C.考虑安全问题解决方案时无需考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合

D.充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，县设计网络安全系统的必要前提条件  
  
试题**3**： 关于源代码审核，下列说法正确的是：（）  
A．人工审核源代码审校的效率低，但采用多人并行分析可以完全弥补这个缺点  
B．源代码审核通过提供非预期的输入并监视异常结果来发现软件故障，从而定位可能导致安全弱点的薄弱之处  
C．使用工具进行源代码审核，速度快，准确率高，已经取代了传统的人工审核  
D.源代码审核是对源代码检查分析，检测并报告源代码中可能导致安全弱点的薄弱之处  
  
试题**4**： 下面哪类访问控制模型是基于安全标签实现的？（）    
A、自主访问控制B、强制访问控制C、基于规则的访问控制D、基于身份的访问控制

试题**5**： 在Clark-Wilson模型中哪一项不是保证完整性任务的？（）  
A、防止职权的滥用B、防止非授权修改C、维护内部和外部的一致性D、防止授权但不适当地修改  
  
试题**6**： 对"PDCA"循环的描述不正确的是:（）  
A、“PDCA”的含义是P-计划，D-实施，C-检查，A-改进  
B、“PDCA”循环又叫"戴明"环  
C、“PDCA"循环是只能用于信息安全管理体系有效进行的工作程序  
D、“PDCA”循环是可用于任何一项活动有效进行的工作程序  
  
试题**7**： 下面哪一项不是VPN 协议标准：（）  
A、L2TP B、IPSec C、TACACS+ D、PPTP

试题**8**： Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?   
A、Overwriting the tapes B、Initializing the tape labels C、Degaussing the tapes D、Erasing the tapes   
  
试题**9**： 数字签名包含一个消息摘要是为了：（）  
A.显示如果信息在传输后被改动B.定义加密算法C.确认源的标识（/身份）D.使得消息以数字格式传输  
  
试题**10**： 发送人的公钥将通过什么进行身份验证：（）  
A、证书机构B、数字签名C、数字证书D、注册机构

**信息安全工程师每日一练试题（2017/4/6）**

试题**1**： 为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机（）？  
A、SMTP身份认证 B、逆向名字解析 C、黑名单过滤 D、内容过滤  
  
试题**2**： 以下哪项不是应急响应准备阶段应该做的？（）  
A.确定重要资产和风险，实施针对风险的防护措施B.编制和管理应急响应计划  
C.建立和训练应急响应组织和准备相关的资源D.评估时间的影响范围，增强审计功能、备份完整系统

试题**3**： 某单位在实施风险评估时，按照规范形成了若干文档，其中，（）中的文档应属于风险评估中“风险要素识别”阶段输出的文档（）

A.《风险评估方法》，主要包括本次风险评估的目的、范围、目标，评估步骤，经费预算和进度安排等内容

B.《风险评估方法和工具列表》，主要包括拟用的风险评估方法和测试评估工具等内容

C.《风险评估准则要求》，主要包括现有风险评估参考标准、采用的风险分析方法，资产分类标准等内容

D.《已有安全措施列表》，主要经验检查确认后的已有技术和管理方面安全措施等内容

试题**4**： BIBA模型基于两种规则来保障数据的完整性的保密性，分别是：（）  
A.上读，主体不可读安全级别高于它的数据；下写，主体不可写安全级别低于它的数据  
B.下读，主体不可读安全级别高于它的数据；上写，主体不可写安全级别低于它的数据  
C.上读，主体不可读安全级别低于它的数据；下写，主体不可写安全级别高于它的数据  
D.下读，主体不可读安全级别低于它的数据；上写，主体不可写安全级别高于它的数据

试题**5**： 域名服务系统(DNS)的功能是：（）  
A、 完成域名和IP地址之间的转换B、 完成域名和网卡地址之间的转换

C、 完成主机名和IP地址之间的转换D、 完成域名和电子邮件地址之间的转换  
  
试题**6**： To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:   
A、avoidance. B、transference. C、mitigation. D、acceptance.   
  
试题**7**： Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?   
A、A remote access server B、A proxy server C、A personal firewall D、A password-generating token   
  
试题**8**： 在完成了业务影响分析（BIA）后，下一步的业务持续性计划应该是什么（）  
A 测试和维护业务持续性计划B 制定一个针对性计划C 制定恢复策略D 实施业务持续性计划  
  
试题**9**： 在设计商业连续性计划时，商业影响分析可以用来识别关键业务流程和相应的支持程序，它主要会影响到下面哪一项内容的制定？（）  
A、维护商业连续性计划的职责B、选择站点恢复供应商的条件C、恢复策略D、关键人士的职责  
  
试题**10**： 当传输一个支付的指令时，以下哪一项可用来帮助校验该指令不是被复制的？（）  
A.使用密码学的哈希算法B.加密消息摘要C.解密消息摘要D.(使用)序列号及时间戳

**信息安全工程师每日一练试题（2017/4/7）**

试题**1**： 入侵检测系统使用入侵检测技术对网络和系统进行监视，并根据监视结果采取不同的处理，最大限度降低可能的入侵危害。以下关于入侵检测系统的叙述，不正确的是（ ） 。  
A、入侵检测系统可以弥补安全防御系统的漏洞和缺陷   
B、入侵检测系统很难检测到未知的攻击行为   
C、基于主机的入侵检测系统可以精确地判断入侵事件   
D、基于网络的入侵检测系统主要用于实时监控网络关键路径的信息   
  
试题**2**： 默认情况下，Windows 2000有 3个日志文件：应用程序日志文件、安全日志文件以及()。  
A、目录服务日志文件B、DNS服务器日志文件C、系统日志文件D、文件复制服务日志文件   
  
试题**3**： 当保护组织的信息系统时，在网络防火墙被破坏以后，通常的下一道防线是下列哪一项？（）  
A. 个人防火墙B.防病毒软件C.入侵检测系统D.虚拟局域网设置  
  
试题**4**： 以下关于备份站点的说法哪项是正确的（）  
A.应与原业务系统具有同样的物理访问控制措施  
B.应容易被找到以便于在灾难发生时以备紧急情况的需要  
C.应部署在离原业务系统所在地较近的地方  
D.不需要具有和原业务系统相同的环境监控等级  
  
试题**5**： 以下哪项不属于造成信息安全问题的自然环境因素？（）  
A.纵火。B.地震。C.极端天气。D.洪水。

试题**6**： 项目经理欲提高信息系统安全性，他首先要做的工作是（）  
A.考虑安全开发需要什么样的资源与预算  
B.考虑安全开发在开发生命周期各阶段应开展哪些工作  
C.对开发团队进行信息安全培训  
D.购买一定的安全工具，如代码扫描工具等  
  
试题**7**： 下面对于cookie的说法错误的是：（）  
A、cookie是一小段存储在浏览器端文本信息，web应用程序可以读取cookie包含的信息  
B、cookie可以存储一些敏感的用户信息，从而造成一定的安全风险  
C、通过cookie提交精妙构造的移动代码，绕过身份验证的攻击叫做cookie欺骗  
D、防范cookie欺骗的一个有效方法是不使用cookie验证方法，而是用session验证方法  
  
试题**8**： 分片攻击问题发生在：（）  
A、数据包被发送时B、数据包在传输过程中C、数据包被接收时D、数据包中的数据进行重组时

试题**9**： 在信息安全风险管理体系中分哪五个层面？（）  
A、决策层、管理层、执行层、支持层、用户层B、决策层、管理层、建设层、维护层、用户层  
C、管理层、建设层、运行层、支持层、用户层D、决策层、管理层、执行层、监控层、用户层

试题**10**： 依据国家标准《信息安全技术信息系统灾难恢复范围》（GB/T20988），灾难恢复管理过程的主要步骤是灾难恢复需求分析、灾难恢复策略制定、灾难恢复策略实现、灾难恢复预案制定和管理；其中灾难恢复策略实现不包括以下哪一项？（）  
A．分析业务功能B．选择和建设灾难备份中心  
C．实现灾备系统技术方案D．实现灾备系统技术支持和维护能力

试题**11**： 信息安全管理的根本方法是:（）  
A、风险处置B、应急响应C、风险管理D、风险评估  
  
试题**12**： 信息系统安全保护等级为3级的系统，应当()年进行一次等级测评?  
A．0．5 B．1 C．2 D．3  
  
试题**13**： （1）is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party. the goal of steganography is to hide the data from a third party. In this article, I will discuss what steganography is, what purposes it serves, and will provide an example using available software.  
There are a large number of steganographic （2）that most of us are familiar with (especially if you watch a lot of spy movies), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding informations, such as:  
Covert channels (c,g, Loki and some distributed denial-of-service tools use the Internet Control （3）Protocol, or ICMP, as the communication channel between the “bad guy”and a compromicyed system)  
Hidden text within Web pages  
Hiding files in “plain sight”(c,g. what better place to “hide”a file than with an important sounding name in the c:\winnt system32 directory)  
Null ciphers(c,g, using the first letter of each word to form a hidden message in an otherwise innocuous text)  
steganography today, however, is significantly more （4）than the example about suggest, allowing a user to hide large amounts of information within image and audio. These forms of steganography often are used in conjunction with cryptography so the information is double protected; first it is encrypted and then hidden so that an advertisement first. find the information ( an often difficult task in and of itself) and the decrypted it.  
The simplest approach to hiding data within an image file is called （5）signature insertion. In this method, we can take the binary representation of the hidden data and the bit of each byte within the covert image. If we are using 24-bit color the amount and will be minimum and indiscriminate to the human eye.  
（1）A、Cryptography B、Geography C、Stenography D、Steganography  
（2）A、methods B、software C、tools D、services  
（3）A、Member B、Management C、Message D、Mail  
（4）A、powerful B、sophistication C、advanced D、easy  
（5）A、least B、most C、much D、less  
  
试题**14**： 下列那一项能保证发送者的真实性和e-mail的机密性？  
A、用发送者的私钥加密消息散列(hash)，然后用接收者的公钥加密消息散列(hash)  
B、发送者对消息进行数字签名然后用发送者的私钥加密消息散列(hash)  
C、用发送者的私钥加密消息散列(hash)，然后用接收者的公钥加密消息。  
D、用发送者的私钥加密消息，然后用接收者的公钥加密消息散列(hash)  
  
试题**15**： While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?   
A、Observe the response mechanism.   
B、Clear the virus from the network.   
C、Inform appropriate personnel immediately.   
D、Ensure deletion of the virus.   
  
试题**16**： A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?   
A、Reviewing logs frequently B、Testing and validating the rules   
C、Training a local administrator at the new location D、Sharing firewall administrative duties   
  
试题**17**： Responsibility for the governance of IT should rest with the:   
A、IT strategy committee. B、chief information officer (CIO).   
C、audit committee. D、board of directors.   
  
试题**18**： 在安全官的帮助下，赋予数据访问权的是（）  
A、数据所有者B、程序编写员C、系统分析员D、库管理员  
  
试题**19**： 连续审计方法的主要优点是：（）  
A、在处理过程中无需信息系统审计师进行系统可靠性证据搜集  
B、需要信息系统审计师回顾并立刻跟进所有搜集的信息  
C、可以提高大事务量分时环境的系统安全  
D、与组织的计算机系统复杂性无关  
  
试题**20**： 当发生灾难时，以下哪一项能保证业务交易的有效性（）  
A、从当前区域外的地方持续每小时1次地传送交易磁带  
B、从当前区域外的地方持续每天1次地传送交易磁带  
C、抓取交易以整合存储设备  
D、从当前区域外的地方实时传送交易磁带

**2017/4/1 1~5 D B D B C 6~10 B C C D A**

**2017/4/2 1~5 B C D C D 6~10 D D A C C**

**2017/4/3 1~5 A B A D B 6~10 A A A B A**

**2017/4/4 1~5 AD B D C B 6~10 A B A B D**

**2017/4/5 1~5 B C D B A 6~10 C C C A C**

**2017/4/6 1~5 D D D D A 6~10 C C C C D**

**2017/4/7 1~5 A C C A A 6~10 B C D D A**

**11~15 C B AACBA C C 16~20 B D A C D**