**信息安全工程师每日一练试题（2017/1/19）**

试题**1**： 安全审计是保障计算机系统安全的重要手段之一，其作用不包括（ ）。  
A. 检测对系统的入侵B. 发现计算机的滥用情况  
C. 发现系统入侵行为和潜在的漏洞D. 保证可信网络内部信息不外泄  
  
试题**2**： 以下对于蠕虫病毒的错误说法是（）  
A.通常蠕虫的传播无需用户的操作B.蠕虫病毒的主要危害体现在对数据保密的破坏  
C.蠕虫的工作原理与病毒相似，除了没有感染文件  
D.是一段能不以其他程序为媒介，从一个电脑系统复制到另一个电脑系统  
  
试题**3**： 职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（）  
A、数据安全管理员  B、数据安全分析员C、系统审核员 D、系统程序员  
  
试题**4**： 防火墙通常分为内外网和DMZ三个区域，按照受保护程度，从高到低正确的排列次序为（）。  
A．内网、外网和DMZ B．外网、内网和DMZ  
C．DMZ、内网和外网 D．内网、DMZ和外网

试题**5**： 关于监理过程中成本控制，下列说法中正确的是?（）  
A．成本只要不超过预计的收益即可B．成本应控制得越低越好  
C．成本控制由承建单位实现，监理单位只能记录实际开销  
D．成本控制的主要目的是在批准的预算条件下确保项目保质按期完成

试题**6**： 关于业务连续性计划（bcp）以下说法最恰当的是：（）  
A. 组织为避免所有业务功能因重大事件而中断，减少业务风险而建立的控制过程；  
B. 组织为避免关键业务功能因重大事件而中断，减少业务风险而建立的一个控制过程；  
C. 组织为避免所有业务功能因各种事件而中断，减少业务风险而建立的一个控制过程；  
D. 组织为避免信息系统功能因各种事件而中断，减少信息系统而建立的一个控制过程。  
  
试题**7**： 对信息安全事件的分级参考下列三个要素：信息系统的重要程度、系统损失和社会影响。依据信息系统的重要程度对系统进行划分，不属于正确划分级别的是：（）  
A.特别重要信息系统B.重要信息系统C.一般信息系统D. 关键信息系统

试题**8**： 对安全策略的描述不正确的是？（）  
A.信息安全策略应得到组织的最高管理者批准。  
B.策略应有一个所有者，负责按复查程序维护和复查该策略。  
C.安全策略应包括管理层对信息安全管理工作的承诺。  
D.安全策略一旦建立和发布，则不可变更。  
  
试题**9**： 以下哪一个不是风险控制的主要方式（）  
A.规避方式B.转移方式C.降低方式D.隔离方式

试题**10**： 信息化建设和信息安全建设的关系应该是：（）  
A．信息化建设的结果就是信息安全建设的 B．信息化建设和信息安全建设应同步规划、同步实施  
C．信息化建设和信息安全建设是交替进行的，无法区分谁先谁后  
D．以上说法都正确

**信息安全工程师每日一练试题（2017/1/20）**

试题**1**： “冲击波”病毒属于 （1） 类型的病毒，它利用 Windows 操作系统的 （2） 漏 洞进行快速传播。  
（1）A、蠕虫 B、文件 C、引导区 D、邮件  
（2）A、CGI 脚本 B、RPC C、DNS D、IMAP  
  
试题**2**： 按照RSA算法，若选两奇数p=5，q=3，公钥e=7，则私钥d为　（ ）　。  
A、6  B、7  C、8  D、9  
  
试题**3**： 以下关于对称密钥加密说法正确的是（）。  
A、加密方和解密可以使用不同的算法 B、加密密钥和解密密钥可以是不同的  
C、加密密钥和解密密钥必须是相同的 D、密钥的管理非常简单  
  
试题**4**： 计算机系统由硬件和软件构成()A、对B、错  
  
试题**5**： 以下关于拒绝服务攻击的叙述中，不正确的是（）。  
A．拒绝服务攻击的目的是使计算机或者网络无法提供正常的服务

B．拒绝服务攻击是不断向计算机发起请求来实现的  
C．拒绝服务攻击会造成用户密码的泄漏  
D．DDoS是一种拒绝服务攻击形式

试题**6**： 下面关于定量风险评估方法的说法正确的是（）  
A.易于操作，可以对风险进行排序并能够对那些需要立即改善的环节进行标识  
B.能够通过成本效益分析控制成本  
C."耗时短、成本低、可控性高"  
D.主观性强，分析结果的质量取决于风险评估小组成员的经验和素质

试题**7**： 以下关于风险评估的描述不正确的是？（）  
A.作为风险评估的要素之一，威胁发生的可能需要被评估  
B.作为风险评估的要素之一，威胁发生后产生的影响需要被评估  
C.风险评估是风险管理的第一步D.风险评估是风险管理的最终结果  
  
试题**8**： 中国信息安全测评中心对CISP注册信息安全专业人员有保持认证要求，在证书有效期内，应完成至少6次完整的信息安全服务经历，以下哪项不是信息安全服务：（）  
A、为政府单位信息系统进行安全方案设计B、在信息安全公司从事保安工作  
C、在公开场合宣讲安全知识D、在学校讲解信息安全课程  
  
试题**9**： 下面哪种安全代码最难以用遍历的方法来破解？（）  
A. 密文B. 用户口令C. 锁定口令D. 口令代码  
  
试题**10**： 依据国家信息安全等级保护相关标准，军用不对外公开的信息系统至少应该属于（）  
A、二级及二级以上B、三级及三级以上C、四级及四级以上D、五级

**信息安全工程师每日一练试题（2017/1/21）**

试题**1**： 某公司财务管理数据只能提供给授权用户，通过采取安全管理措施确保不能被未授权的个人、实体或过程利用或知悉，以确保数据的（ ）  
A、保密性B、完整性C、可用性D、稳定性

试题**2**： WEB 服务器、 MAIL 服务器、FTP服务器通常在网络区域划分时放在\_\_\_个安全区域中()  
A、1 B、2 C、3  
  
试题**3**： 在戴明环(PDCA)模型中，处置(ACT)环节的信息安全管理活动是：（）  
A．建立环境B．实施风险处理计划C．持续的监视与评审风险D.持续改进信息安全管理过程  
  
试题**4**： 以下有关信息安全方面的业务连续性管理的描述，不正确的是（）  
A. 信息安全方面的业务连续性管理就是要保障企业关键业务在遭受重大灾难/破坏时，能够及时恢复，保障企业业务持续运营  
B.    企业在业务连续性建设项目一个重要任务就是识别企业关键的、核心业务  
C.业务连续性计划文档要随着业务的外部环境的变化，及时修订连续性计划文档  
D.  信息安全方面的业务连续性管理只与IT部门相关，与其他业务部门人员无须参入  
  
试题**5**： 以下哪些不是网络类资产：（）  
A.网络设备B.基础服务平台C.网络安全设备D.主干线路

试题**6**： 由于病毒攻击、非法入侵等原因，校园网部分楼宇出现网络瘫痪，或者FTP及部分网站服务器不能响应用户请求，属于以下哪种级别事件（）  
A.特别重大事件B.重大事件C.较大事件D.一般事件  
  
试题**7**： 对于信息安全风险的描述不正确的是（）  
A.企业信息安全风险管理就是要做到零风险  
B.在信息安全领域，风险就是指信息资产遭受损坏并给企业带来负面影响及其潜在可能性  
C.风险管理就是以可接受的代价，识别、控制、减少或消除可能影响信息系统的安全风险的过程。  
D.风险评估就是对信息和信息处理设施面临的威胁、受到的影响、存在的弱点以及威胁发生的可能性的评估。  
  
试题**8**： 当前网络中的鉴别技术正在快速发展，以前我们主要通过账号密码的方式验证用户身份，现在我们会用到U盾识别、指纹识别、面部识别、虹膜识别等多种鉴别方式。请问下列哪种说法是正确的。（）  
A、 面部识别依靠每个人的脸型作为鉴别依据，面部识别无法伪造  
B、 指纹识别相对传统的密码识别更加安全  
C、 使用多种鉴别方式比单一的鉴别方式相对安全  
D、 U盾由于具有实体唯一性，被银行广泛使用，使用U盾没有安全风险

试题**9**： 要安全浏览网页，不应该( )。  
A、 在公用计算机上使用“自动登录”和“记住密码”功能B、 禁止开启ActiveX控件和Java脚本  
C、 定期清理浏览器CookiesD、 定期清理浏览器缓存和上网历史记录

试题**10**： 两个密钥三重DES加密：C=CK1[DK2[EK1[P]]],K1≠K2，其中有效的密钥为（）  
A、56 B、128 C、168 D、112

**信息安全工程师每日一练试题（2017/1/22）**

试题**1**： 在信息安全管理工作中“符合性”的含义不包括哪一项？（）  
A、对法律法规的符合                        B、对安全策略和标准的符合  
C、对用户预期服务效果的符合                D、通过审计措施来验证符合情况  
  
试题**2**： 理论上网络边界可以无限延伸()A、是B、否

试题**3**： 美国的关键信息基础设施(critical Information Infrastructure，CII)包括商用核 设施、政府设施、交通系统、饮用水和废水处理系统、公共健康和医疗、能源、银行和金融、国防工业基地等等，美国政府强调重点保障这些基础设施信息安全，其主要原因不包括：（）  
A．这些行业都关系到国计民生，对经济运行和国家安全影响深远  
B．这些行业都是信息化应用广泛的领域  
C.这些行业信息系统普遍存在安全隐患，而且信息安全专业人才缺乏的现象比其他行业更突出  
D．这些行业发生信息安全事件，会造成广泛而严重的损失  
  
试题**4**： 以下哪些是需要在信息安全策略中进行描述的：（）  
A．组织信息系统安全架构B．信息安全工作的基本原则

C．组织信息安全技术参数D．组织信息安全实施手段

试题**5**： 拒绝式服务攻击会影响信息系统的哪个特性？（）  
A.完整性B.可用性C.机密性D.可控性  
  
试题**6**： 以下哪一个不是OSI安全体系结构中的安全机制（）  
A.数字签名B.路由控制C.数据交换D.抗抵赖  
  
试题**7**： 以下对于蠕虫病毒的说法错误的是：（）  
A、通常蠕虫的传播无需用户的操作B、蠕虫病毒的主要危害体现在对数据保密性的破坏  
C、蠕虫的工作原理与病毒相似，除了没有感染文件阶段  
D、是一段能不以其他程序为媒介，从一个电脑系统复制到另一个电脑系统的程序  
  
试题**8**： )iPhone手机“越狱”是指( )  
A、 带着手机逃出去B、 通过不正常手段获得苹果手机操作系统的最高权限  
C、 对操作系统升级D、 修补苹果手机的漏洞

试题**9**： 世界上首例通过网络攻击瘫痪物理核设施的事件是?（）  
A、 巴基斯坦核电站震荡波事件B、 以色列核电站冲击波事件  
C、 伊朗核电站震荡波事件D、 伊朗核电站震网(stuxnet)事件

试题**10**： 浏览某些网站时，网站为了辨别用户身份进行session跟踪，而储存在本地终端上的数据是( )  
A、 收藏夹B、 书签C、 COOKIED、 https

**信息安全工程师每日一练试题（2017/1/23）**

试题**1**： 下列选项中，（ ）是最安全的信息系统。  
A. ERP-CRM B. MRPII C. MIS-S D. S-MIS  
  
试题**2**： 静态包过滤是在()层实现的。  
A、MAC B、数据链路 C、网络 D、传输   
  
试题**3**： “产品导向型”的信息安全解决方案是()  
A、解决信息安全问题的最佳方案  
B、过分依赖产品和技术，忽视管理和服务，多数是一次性工程，对于信息安  
全治标不治本  
C、只要选用国产信息安全产品就会更加安全  
D、只要采用了全线的信息安全产品就会实现信息安全  
  
试题**4**： 计算机病毒防治产品分为三级，其中三级品为最高级()A、对B、错  
试题**5**： 企业信息资产的管理和控制的描述不正确的是（）  
A. 企业应该建立和维护一个完整的信息资产清单，并明确信息资产的管控责任；  
B.    企业应该根据信息资产的重要性和安全级别的不同要求，采取对应的管控措施；  
C.企业的信息资产不应该分类分级，所有的信息系统要统一对待  
D.  企业可以根据业务运作流程和信息系统拓扑结构来识别所有的信息资产  
  
试题**6**： 有什么方法可以测试办公部门的无线安全？（）  
A.War dialing战争语言B.社会工程学C.战争驾驶D.密码破解  
  
试题**7**： 企业信息资产的管理和控制的描述不正确的是（）  
A.企业应该建立和维护一个完整的信息资产清单，并明确信息资产的管控责任；  
B.企业应该根据信息资产的重要性和安全级别的不同要求，采取对应的管控措施；  
C.企业的信息资产不应该分类分级，所有的信息系统要统一对待  
D.企业可以根据业务运作流程和信息系统拓扑结构来识别所有的信息资产  
  
试题**8**： 灾难恢复SHARE78的第三层是指（）  
A.卡车运送B.电子链接C.活动状态的备份中心D.0数据丢失  
  
试题**9**： 口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（）  
A、长期没有修改的口令B、过短的口令C、两个人公用的口令D、设备供应商提供的默认口令  
  
试题**10**： 在SSE-CMM中对工程过程能力的评价分为三个层次，由宏观到微观依次是:（）  
A．能力级别-公共特征(CF)-通用实践(GP)B．能力级别-通用实践-(GP)-公共特征(CF)  
C．通用实践-(GP)-能力级别-公共特征(CF)D．公共特征(CF)-能力级别-通用实践-(CP)

**信息安全工程师每日一练试题（2017/1/24）**

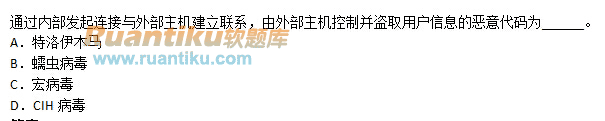
试题**1**： 以下关于Smurf 攻击的描述，那句话是错误的？()  
A、它是一种拒绝服务形式的攻击B、它依靠大量有安全漏洞的网络作为放大器  
C、它使用ICMP的包进行攻击D、攻击者最终的目标是在目标计算机上获得一个帐号  
  
试题**2**： 由于病毒攻击、非法入侵等原因，校园网整体瘫痪，或者校园网络中心全部DNS、主WEB服务器不能正常工作；由于病毒攻击、非法入侵、人为破坏或不可抗力等原因，造成校园网出口中断，属于以下哪种级别事件（）  
A.特别重大事件B.重大事件C.较大事件D.一般事件  
  
试题**3**： 下面哪一项是恢复非关键系统的最合理方案? （）  
A.温站B.移动站C.热站D.冷站

试题**4**： 下面哪条不属于SSE-CMM中能力级别3“充分定义”级的基本内容：（）    
A、改进组织能力B、定义标准过程C、协调安全实施、执行已定义的过程  
  
试题**5**： 一个VLAN可以看做是一个：（）  
A、冲突域B、广播域C、管理域D、阻塞域

试题**6**： 习近平总书记在第二届世界互联网大会上指出“各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体”，为此提出了五点主张，以下哪一项不属于五点主张范围()  
加快全球网络基础设施建设，促进互联互通 打造网上文化交流共享平台，促进交流互鉴  
构建互联网治理体系，促进公平正义 尊重网络知识产权，共筑网络文化

试题**7**： 小刘在某电器城购买了一台冰箱，并留下了个人姓名、电话和电子邮件地址等信息，第二天他收到了一封来自电器城提示他中奖的邮件，查看该邮件后他按照提示缴纳中奖税款后并没有得到中奖奖金，再打电话询问电器城才得知电器城并没有举办中奖活动。根据上面的描述，由此可以推断的是()?  
A、 小刘在电器城登记个人信息时，使用了加密手段B、 小刘遭受了钓鱼邮件攻击，钱被骗走了  
C、 小刘的计算机中了木马，被远程控制D、 小刘购买的冰箱是智能冰箱，可以连网  
  
试题**8**： Windows操作系统的注册表运行命令是：  
A.Regsvr32 B.Regedit C.Regedit.msc D.Regedit.mmc

试题**9**： 以下关于互联网协议安全(InternetProtocolSecurity，IPsec)协议说法错误的是：（）  
A．在传送模式中，保护的是IP 负载  
B．验证头协议(AuthenticationHead，AH)和IP封装安全载荷协议(EncapsulatingSecurityPayload，ESP)都能以传输模式和隧道模式工作  
C．在隧道模式中，保护的是整个互联网协议(InternetProtocol，IP)包，包括IP 头  
D．IPsec仅能保证传输数据的可认证性和保密性

试题**10**： 

**信息安全工程师每日一练试题（2017/1/25）**

试题**1**： （）针对TCP连接进行攻击。A．拒绝服务B．暴力攻击C．网络侦察D．特洛伊木马  
  
试题**2**： 信息网络安全的第二个时代()A、专网时代B、九十年代中叶前C、世纪之交D、2003年  
  
试题**3**： 具有政治目的的黑客只对政府的网络与信息资源造成危害()A、是B、不是  
  
试题**4**： 在数据链路层中MAC子层主要实现的功能是（）  
A.介质访问控制B.物理地址识别C.通信协议产生D.数据编码  
  
试题**5**： 以下哪一项不是流氓软件的特征？（）    
A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装B、通常添加驱动保护使用户难以卸载  
C、通常会启动无用的程序浪费计算机的资源D、通常会显示下流的言论  
  
试题**6**： 在ISO27001-2005中，制定风险处置计划应该在PDCA的哪个阶段进行？（）  
A、Plan B、Do C、Check D、Act  
  
试题**7**： 下面哪一项是对IDS的正确描述？（）  
A、基于特征（Signature-based）的系统可以检测新的攻击类型  
B、基于特征（Signature-based）的系统化基于行为（behavior-based）的系统产生更多的误报  
C、基于行为（behavior-based）的系统维护状态数据库来与数据包和攻击相匹配  
D、基于行为（behavior-based）的系统比基于特征（Signature-based）的系统有更高的误报  
  
试题**8**： 以下哪一种局域网传输媒介是最可靠的？（）  
A.同轴电缆B.光纤C.双绞线（屏蔽）D.双绞线（非屏蔽）

试题**9**： 下列对于信息安全保障深度防御模型的说法错误的是：（）  
A．信息安全外部环境：信息安全保障是组织机构安全、国家安全的一个重要组成部分，此对信息安全的讨论必须放在国家政策、法律法规和标准的外部环境制约下。  
B．信息安全管理和工程：信息安全保障需要在整个组织机构内建立和完善信息安全管理体系，将信息安全管理综合至信息系统的整个生命周期，在这个过程中，我们需要采用信息系统工程的方法来建设信息系统。  
C．信息安全人才体系：在组织机构中应建立完善的安全意识，培训体系也是信息安全保障的重要组成部分。  
D．信息安全技术方案：“从外而内、自下而上、形成边界到端的防护能力”。

试题**10**： 

**信息安全工程师每日一练试题（2017/1/26）**

试题**1**： 在网络管理中要防护各种安全威胁。在SNMPv3中，不必要或无法防护的安全威胁是  （ ）  。  
A、篡改管理信息：通过改变传输中的SNMP报文实施未经授权的管理操作    
B、通信分析：第三者分析管理实体之间的通信规律，从而获取管理信息    
C、假冒合法用户：未经授权的用户冒充授权用户，企图实施管理操作    
D、消息泄露：SNMP引擎之间交换的信息被第三者偷听  
   
试题**2**： 下面对于“电子邮件炸弹”的解释最准确的是：()  
A.邮件正文中包含的恶意网站链接B.邮件附件中具有强破坏性的病毒  
C.社会工程的一种方式，具有恐吓内容的邮件D.在短时间内发送大量邮件软件，可以造成目标邮箱爆满  
  
试题**3**： Unix系统中的账号文件是（）。  
A、/etc/passwd B、/etc/shadow C、/etc/group D、/etc/gshadow  
  
试题**4**： 构成风险的关键因素有哪些？（）  
A.人，财，物B.技术，管理和操作C.资产，威胁和弱点D.资产，可能性和严重性  
  
试题**5**： 下面哪项不是实施信息安全管理的关键成功因素（）  
A.理解组织文化B.得到高层承诺C.部署安全产品D.纳入奖惩机制  
  
试题**6**： 依据国家标准《信息安全技术信息系统灾难恢复规范》（GB/T20988），需要备用场地但不要求部署备用数据处理设备的是灾难恢复等级的第几级？（）  
A、2 B、3 C、4 D、5

试题**7**： 以下哪项是对系统工程过程中“概念与需求定义”阶段的信息安全工作的正确描述？（）  
A．应基于法律法规和用户需求，进行需求分析和风险评估，从信息系统建设的开始就综合信息系统安全保障的考虑  
B．应充分调研信息安全技术发展情况和信息安全产品市场，选择最先进的安全解决方案和技术产品  
C．应在将信息安全作为实施和开发人员的一项重要工作内容，提出安全开发的规范并切实落实  
D．应详细规定系统验收测试中有关系统安全性测试的内容  
  
试题**8**： LDAP的作用是什么？（）  
A、提供证书的保存、修改、删除和获取的能力B、证书的撤销列表，也成“证书黑名单”  
C、数字证书注册审批D、生成数字证书  
  
试题**9**： S/Key口令是一种一次性口令生产方案，它可以对抗（）  
A、恶意代码木马攻击B、拒绝服务攻击C、协议分析攻击D、重放攻击  
  
试题**10**： 在访问因特网时，为了防止Web页面中恶意代码对自己计算机的损害，可以采取的防范措施是（）  
A、将要访问的Web站点按其可信度分配到浏览器的不同安全区域B、在浏览器中安装数字证书  
C、利用IP安全协议访问Web站点D、利用SSL访问Web站点

**2017/1/19 1~5 D B D D D 6~10 B D D D B**

**2017/1/20 1~5 AB B C A C 6~10 B D B A B**

**2017/1/21 1~5 A A D D B 6~10 C A C A D**

**2017/1/22 1~5 C A C B B 6~10 D B B D C**

**2017/1/23 1~5 D C B B C 6~10 D C B D A**

**2017/1/24 1~5 D A D A B 6~10 D B B D A**

**2017/1/25 1~5 A A B A D 6~10 A D B D A**

**2017/1/26 1~5 B D A C C 6~10 B A A D A**