**信息安全工程师每日一练试题（2017/1/27）**

试题1： 比较先进的电子政务网站提供基于（ ）的用户认证机制用于保障网上办公的信息安全和不可抵赖性。  
A．数字证书B．用户名和密码C．电子邮件地址D．SSL  
  
试题2： 驻留在多个网络设备上的程序在短时间内同时产生大量的请求信息冲击某个Web服务器，导致该服务器不堪重负，无法正常响应其它合法用户的请求，这属于 （ ） 。  
A、网上冲浪  B、中间人攻击  C、DDoS攻击  D、MAC攻击  
  
试题3： 某web网站向CA申请了数字证书。用户登录该网站时，通过验证  （1）  ，可确认该数字证书的有效性，从而  （2）  。  
（1）A、CA的签名  B、网站的签名  C、会话密钥  D、DES密码  
（2）A、向网站确认自己的身份  B、获取访问网站的权限  C、和网站进行双向认证  D、验证该网站的真伪  
  
试题4： 信息系统安全风险评估是通过数字化的资产评估准则完成的，它通常会覆盖人员安全、人员信息、公共秩序等方面的各个要素，以下不会被覆盖的要素是（）  
A、立法及规章未确定的义务B、金融损失或对业务活动的干扰  
C、信誉的损失D、商业及经济的利益

试题5： 对于信息系统访问控制说法错误的是？（）  
A．应该根据业务需求和安全要求制定清晰的访问控制策略，并根据需要进行评审和改进。  
B．网络访问控制是访问控制的重中之重，网络访问控制做好了操作系统和应用层次的访问控制就会解决  
C．做好访问控制工作不仅要对用户的访问活动进行严格管理，还要明确用户在访问控制中的有关责任  
D．移动计算和远程工作技术的广泛应用给访问控制带来新的问题，因此在访问控制工作要重点考虑对移动计算设备和远程工作用户的控制措施  
  
  
试题6： （）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。  
A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰  
  
试题7： 以下哪一项不是SQL语言的功能（）  
A、数据定义B、数据检查C、数据操纵D、数据加密  
  
试题8： 账号锁定策略中对超过一定次数的错误登录账号进行锁定是为了对抗以下哪种攻击?（）  
A．分布式拒绝服务攻击(DDoS) B．病毒传染 C．口令暴力破解 D．缓冲区溢出攻击  
  
试题9： 以下关于可信计算说法错误的是：（）  
A．可信的主要目的是要建立起主动防御的信息安全保障体系  
B．可信计算机安全评价标准(TCSEC)中第一次提出了可信计算机和可信计算基的概念  
C．可信的整体框架包含终端可信、终端应用可信、操作系统可信、网络互联可信、互联网交易等应用系统可信  
D．可信计算平台出现后会取代传统的安全防护体系和方法  
  
试题10： 以下关于VPN的叙述中，正确的是（）  
A、VPN指的是用户通过公用网络建立的临时的、安全的连接  
B、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路  
C、VPN不能做到信息认证和身份认证  
D、VPN只能提供身份认证，不能提供数据加密的功能

**信息安全工程师每日一练试题（2017/1/28）**

试题**1**： 应用系统运行的安全管理中心，数据域安全是其中非常重要的内容，数据域安全包括（ ）  
A、行级数据域安全，字段级数据域安全B、系统性数据域安全，功能性数据域安全  
C、数据资源安全，应用性数据安全D、组织级数据域安全，访问性数据域安全

试题**2**： （ ） 不属于将入侵检测系统部署在DMZ中的优点。  
A、可以查看受保护区域主机被攻击的状态 B、可以检测防火墙系统的策略配置是否合理   
C、可以检测DMZ被黑客攻击的重点 D、可以审计来自Intemet上对受保护网络的攻击类型   
  
试题**3**： 在Kerberor认证系统中，用户首先向  (1)  申请初始票据，然后从  (2)  获得会话密钥。  
（1）A、域名服务器DNS B、认证服务器AS C、票据授予服务器TGS D、认证中心CA  
（2）A、域名服务器DNS B、认证服务器AS C、票据授予服务器TGS D、认证中心CA  
试题**4**： 计算机网络系统中，入侵检测一般分为3个步骤，依次为（）。  
  ①数据分析  ②响应  ③信息收集  
A . ③①②  B. ②③① C. ③②① D. ②①③  
  
试题**5**： 《计算机信息系统国际联网保密管理规定》是由那个部门颁布的()  
A、保密局B、公安部C、密码办  
  
试题**6**： （）不属于将入侵检测系统部署在DMZ中的优点。  
A．可以查到受保护区域主机被攻击的状态      B．可以检测防火墙系统的策略配置是否合理  
C．可以检测DMZ被黑客攻击的重点            D．可以审计来自Internet上对受到保护网络的攻击类型  
  
试题**7**： 数据库管理员在检查数据库时发现数据库的性能不理想，他准备通过对部分数据表实施去除规范性（denormanization）操作来提高数据库性能，这样做将增加下列哪项风险？（）    
A、访问的不一致B、死锁C、对数据的非授权访问、数据完整性的损害  
  
试题**8**： 当访问web网站的某个资源时，请求无法被服务器理解将会出现的HTTP状态码是( )  
A、 200 B、 401 C、 302 D、 303  
  
试题**9**： 通过向被攻击者发送大量的ICMP回应请求，消耗被攻击者的资源来进行响应，直至被攻击者再也无法处理有效的网络信息流时，这种攻击称之为：（）  
A．Land攻击B．Smurf 攻击C．Ping ofDeath 攻击D．ICMPFlood  
  
试题**10**： 下列报告中，不属于信息安全风险评估识别阶段的是（）  
A、资产价值分析报告B、风险评估报告C、威胁分析报告D、已有安全威胁分析报告

**信息安全工程师每日一练试题（2017/1/29）**

试题**1**： Alice向Bob发送数字签名的消息M，则不正确的说法是  （ ）  。  
A、Alice可以保证Bob收到消息M B、Alice不能否认发送消息M   
C、Bob不能编造或改变消息M D、Bob可以验证消息M确实来源于Alice  
  
试题**2**： SQL Server 2005提供了4层安全防线，其中“SQL Server通过登录账号设置来创建附加安全层。用户只有登录成功，才能与SQL Server建立一次连接。”属于(    )。  
A．SQL Server的运行安全防线　　　　　 　B．操作系统的安全防线 　  
C．SQL Server数据库的安全防线 　　  D．SQL Server数据库对象的安全防线  
  
试题**3**： 信息安全政策声明：”每个人必须在进入每一个控制门时，都必须读取自己的证件”,防范的是哪一种攻击方式?（）  
A.尾随PiggybackingB.肩窥Shoulder surfingC.Dumpster divingD.冒充 Impersonation  
  
试题**4**： 内部审核的最主要目的是（）  
A.检查信息安全控制措施的执行情况B.检查系统安全漏洞

C.检查信息安全管理体系的有效性D.检查人员安全意识  
  
试题**5**： 为什么一个公司内部的风险评估团队应该由来自不同部门的人员组成？（）  
A、确保风险评估过程是公平的  
B、因为风险正是由于这些来自不同部门的人员所引起的，因此他们应该承担风险评估的职责  
C、因为不同部门的人员对本部门所面临的风险最清楚，由此进行的风险评估也最接近于实际情况  
D、风险评估团队不应该由来自不同部门的人员组成，而应该由一个来自公司外部的小型团队组成  
  
试题**6**： 下面哪一项不是黑客攻击在信息收集阶段使用的工具或命令：（）  
A．Nmap B．Nslookup C．LC D．Xscan

试题**7**： 如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（）  
A.自动软件管理B. 书面化制度C. 书面化方案D.书面化标准  
  
试题**8**： Linux系统对文件的权限是以模式位的形式来表示，对于文件名为test的一个文件，属于admin 组中user用户，以下哪个是该文件正确的模式表示?（）  
A.rwxrxr-3useradmin1024Sep 1311：58test B.drwxr-xr-x 3user admin1024 Sep 1311：58 test  
C.rwxr-xr-x 3admin user1024 Sep 1311：58 test D.drwxrxr-x 3adminuser1024Sep 1311：58test  
  
试题**9**： 甲收到一份来自乙的电子订单后，将订单中的货物送达到乙时，乙否认自己曾经发送过这份订单，为了解除这种纷争，采用的安全技术是（）  
A、数字签名技术B、数字证书C、消息认证码D、身份认证技术  
  
试题**10**： 入侵检测系统放置在防火墙内部所带来的好处是（）  
A、减少对防火墙的攻击B、降低入侵检测C、增加对低层次攻击的检测D、增加检测能力和检测范围

**信息安全工程师每日一练试题（2017/1/30）**

试题**1**： 黑客的主要攻击手段包括：()  
A、社会工程攻击、蛮力攻击和技术攻击B、人类工程攻击、武力攻击及技术攻击

C、社会工程攻击、系统攻击及技术攻击  
  
试题**2**： 我国《刑法》中规定的“破坏计算机信息系统罪”是指()  
A、破坏计算机信息系统功能。  
B、破坏计算机信息系统数据和应用程序罪以及制作、传播计算机破坏性程序罪。  
C、破坏计算机信息系统功能、破坏计算机信息系统数据和应用程序、以及制作、传播计算机破坏性程序。  
  
试题**3**： 当曾经用于存放机密资料的PC在公开市场出售时（）  
A.对磁盘进行消磁 B.对磁盘低级格式化 C.删除数据 D.对磁盘重整  
  
试题**4**： 干管灭火器系统使用（）  
A.水，但是只有在发现火警以后水才进入管道 B. 水，但是水管中有特殊的防水剂  
C.CO2代替水 D.哈龙代替水  
  
试题**5**： 椭圆曲线密码方案是指：（）  
A、基于椭圆曲线上的大整数分解问题构建的密码方案  
B、通过椭圆曲线方程求解的困难性构建的密码方案  
C、基于椭圆曲线上有限域离散对数问题构建的密码方案  
D、通过寻找是单向陷门函数的椭圆曲线函数构建的密码方案  
  
试题**6**： 世界首个量子卫星，中科院量子科学实验卫星(简称量子卫星)于()发射  
A、 2016年7月B、 2015年10月C、 2015年11月D、 2016年 5月  
  
试题**7**： Linux系统对文件的权限是以模式位的形式来表示，对于文件名为test的一个文件，属于admin 组中user用户，以下哪个是该文件正确的模式表示？（）  
A．rwxr-xr-x3useradmin1024Sep1311:58test  
B．drwxr-xr-x3user admin1024 Sep1311:58 test  
C．rwxr-xr-x3admin user1024 Sep1311:58 test  
D．drwxrxr-x3adminuser 1024Sep1311:58test  
  
试题**8**： 关于《计算机信息系统安全保护条例》，以下错误的是：（）  
A、计算机信息系统实行安全等级保护制度。B、计算机信息系统使用单位应当建立健全安全管理制度。  
C、计算机信息系统实行性能测试和安全测评制度。

D、公安部主管全国计算机信息系统安全保护工作（含安全监督职权）。  
  
试题**9**： 以下哪一项不应被看做防火墙的主要功能?（）  
A、协议过滤B、包交换C、访问控制规则的实现D、审计能力的扩展  
  
试题**10**： 国家科学技术秘密的密级分为绝密级、机密级、秘密级，以下哪项属于绝密级的描述?（）  
A．处于国际先进水平，并且有军事用途或者对经济建设具有重要影响的  
B．能够局部反应国家防御和治安实力的  
C．我国独有、不受自然条件因素制约、能体现民族特色的精华，并且社会效益或者经济效益显著的传统工艺  
D．国际领先，并且对国防建设或者经济建设具有特别重大影响的

**信息安全工程师每日一练试题（2017/1/31）**

试题**1**： 某Web网站向CA申请了数字证书。用户登录该网站时，通过验证  （1）  ，可确认该数字证书的有效性，从而 （2） 。  
（1）A、CA的签名 B、网站的签名 C、会话密钥 D、DES密码  
（2）A、向网站确认自己的身份 B、获取访问网站的权限 C、和网站进行双向认证 D、验证该网站的真伪  
  
试题**2**： 下列算法中，用于密钥交换的是（）。  
A. DES     B. SHA-1      C. Diffie-Hellman   D. AES  
  
试题**3**： 在 MS-SQL 2000的安装或打补丁过程中，相关的信息包括口令会被收集并存放在主机上的一个名为()的文件中。  
A、 patch.iss B、 setup.issC、 install.issD、 uninstall.iss    
  
试题**4**： 下列算法中，属于对称加密算法的是（ ）。  
A、DES B、德国二战时期密码机 C、凯撒密码 D、RSA   
  
试题**5**： 从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（）。  
A、每个分割区G有g=|G|记录，其中g=0或g>=n，且g为偶数，  
B、记录必须成对地加入G或从G中删除  
C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从m各分割区G1，G2，… …Gm中每一个分割区而来的，则统计信息g（G1VG2V… …VGm）是允许发布  
D、记录必须不对地加入G或从G中删除  
  
试题**6**： 以下密码使用方法中正确的是（）。  
A、将密码记录在日记本上以避免忘记    B、任何情况下均不得使用临时性密码      
C、密码中的字母不得重复    D、不要使用全部由字母组成的密码  
  
试题**7**： CA数字证书中不包含的信息有（）。  
A、CA的数字签名 B、证书申请者的个人信息C、证书申请者的私钥  D、证书申请者的公钥信息  
  
试题**8**： 入侵检测系统一般由数据收集器、检测器、（1）构成。（2）不属于入侵检测系统的功能。  
（1）A．分配器和报警器B．知识库和控制器C．数据库和控制器D．知识库和分析器  
（2）A．异常行为模式的统计分析B．重要系统和数据文件完整性评估  
C．定期或不定期地使用安全性分析软件对整个内部系统进行安全扫描，及时发现系统的安全漏洞  
D．检查网络或系统中是否存在违反安全策略的行为  
  
试题**9**： 下面哪个功能属于操作系统中的资源管理功能()  
A、控制用户的作业排序和运行B、对CPU,内存，外设以及各类程序和数据进行管理  
C、实现主机和外设的并行处理以及异常情况的处理D、处理输入/输出事务  
  
试题**10**： 计算机信息系统的安全等级需求确定：()  
A、以二维模型（第一维为资产价值类别、第二维为威胁）的交叉点导出安全保护等级。  
B、以一维模型资产价值类别导出安全保护等级。  
C、以一维模型威胁导出安全保护等级。  
  
试题**11**： Kerberos认证协议时，首先向密钥分发中心发送初始票据（），请求一个会话票据，以便获取服务器提供的服务  
A.RSA              B.TGT          C.DES            D.LSA  
  
试题**12**： 在信息系统设计阶段，“安全产品选择”处于风险管理过程的哪个阶段?（）  
A．背景建立B．风险评估C．风险处理D．批准监督  
  
试题**13**： 对信息安全的理解，正确的是（）  
A.信息资产的保密性、完整性和可用性不受损害的能力，是通过信息安全保障措施实现的  
B. 通过信息安全保障措施，确保信息不被丢失  
C. 通过信息安全保证措施，确保固定资产及相关财务信息的完整性  
D. 通过技术保障措施，确保信息系统及财务数据的完整性、机密性及可用性  
  
试题**14**： 2016年04月19日，习近平总书记在网络安全和信息化工作座谈会上的讲话强调，要建立（）网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制。  
A. 政府和企业B. 企业和企业C. 企业和院校D. 公安和企业  
  
试题**15**： 如果你家里的电话或者手机只响一声就挂了，最佳的处理方式是（）  
A、 立刻报警，一定是诈骗电话  
B、 “响一声”电话多数为吸费电话，如果是陌生号码，就不要理睬  
C、 立刻报警，一定是诈骗电话  
D、 不管是谁，拨回去把对方大骂一顿  
  
试题**16**： 某公司正在对一台关键业务服务器进行风险评估：该服务器价值138000元，针对某个特定威胁的暴露因子（EF）是45%，该威胁的年度发生率（ARO）为每10年发生1次。根据以上信息，该服务器的年度预期损失值（ALE）是多少？（）  
A．1800元B．62100 元C．140000 元D．6210元  
  
试题**17**： 信息安全工作具有投资收益的要求，以下关于信息安全与业务发展的关系说法最准确的是：（）  
A、信息安全的投入很容易测算其产生收益的  
B、信息安全为业务发展提供基础安全保障  
C、信息安全与网络信息系统有着密切联系  
D、信息安全的投入是不能测算其产生收益的

试题**18**： 对信息技术保障框架的内涵和特点（IATF）理解不正确的是（）  
A、基于PDCA思想构建攻防一体化安全体系  
B、对信息系统进行多层防护  
C、IATF描述了保护领域的安全需求和相应的可选择措施  
D、它体现了分层、深度、强健性的防御特点  
  
试题**19**： 数据在进行传输前，需要由协议栈自上而下对数据进行封装，TCP／IP协议中，数据封装的顺序是：（）  
A．传输层、网络接口层、互联网络层B．传输层、互联网络层、网络接口层  
C．互联网络层、传输层、网络接口层D．互联网络层、网络接口层、传输层  
  
试题**20**： 《信息安全技术信息安全风险评估规范GB／T 20984-2007》中关于信息系统生命周17期各阶段的风险评估描述不正确的是：（）  
A.规划阶段风险评估的目的是识别系统的业务战略，以支撑系统安全需求及安全战略等  
B.设计阶段的风险评估需要根据规划阶段所明确的系统运行环境、资产重要性，提出安全功能需求  
C.实施阶段风险评估的目的是根据系统安全需求和运行环境对系统开发、实施过程进行风险识别，并对系统建成后的安全功能进行验证  
D.运行维护阶段风险评估的目的是了解和控制运行过程中的安全风险，是一种全面的风险评估。评估内容包括对真实运行的信息系统、资产、脆弱性等各方面

**信息安全工程师每日一练试题（2017/2/1）**

试题**1**： 在（ ）中，①代表的技术通过对网络数据的封包和加密传输，在公网上传输私有数据、达到私有网络的安全级别；②代表的技术把所有传输的数据进行加密，可以代替telnet，可以为ftp提供一个安全的“通道”；③代表的协议让持有证书的Internet浏览器软件和WWW 服务器之间构造安全通道传输数据，该协议运行在TCP/IP 层之上，应用层之下。  
A. ①SSH②VPN③SSL B. ①VPN②SSH③SSL C. ①VPN②SSL③SSH D. ①SSL②VPN③SSH  
  
试题**2**： 下面病毒中，属于蠕虫病毒的是（ ）  
A. CIH病毒B. 特洛伊木马病毒C. 罗密欧和朱丽叶病毒D.Melissa病毒  
  
试题**3**： 安全策略管理系统中，()负责保护主机系统和服务器的安全，收集系统的各种安全信息和日志，执行定制的安全策略。部署在需要保护用户 PC和服务器上。  
A、安全终端B、策略执行点C、桌面防火墙D、防病毒软件   
  
试题**4**： CDS是按信息分类还原信息，之后进行分类检测()A、是B、否  
  
试题**5**： 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**6**： 在部署风险管理程序的时候，哪项应该最先考虑到：（）  
A.组织威胁，弱点和风险概括的理解  
B. 揭露风险的理解和妥协的潜在后果  
C. 基于潜在结果的风险管理优先级的决心  
D. 风险缓解战略足够在一个可以接受的水平上保持风险的结果  
  
试题**7**： 区别脆弱性评估和渗透测试是脆弱性评估（）  
A.检查基础设施并探测脆弱性，然而穿透性测试目的在于通过脆弱性检测其可能带来的损失  
B.和渗透测试为不同的名称但是同一活动  
C.是通过自动化工具执行，而渗透测试是一种完全的手动过程  
D.是通过商业工具执行，而渗透测试是执行公共进程  
  
试题**8**： 下列哪个选项是不能执行木马脚本的后缀()?  
A、 asp B、 php C、 cer D、 htm  
  
试题**9**： 以下关于PGP(Pretty GoodPrivacy)软件叙述错误的是：（）  
A．PGP可以实现对邮件的加密、签名和认证B．PGP可以实现数据压缩  
C．PGP可以对邮件进行分段和重组D．PGP采用SHA算法加密邮件  
  
试题**10**： 杂凑函数SHAI的输入分组长度为（）比特  
A、128 B、258 C、512 D、1024

**信息安全工程师每日一练试题（2017/2/2）**

试题**1**： Linux系统/etc目录从功能上看相当于Windows的哪个目录？（）  
A、program files B、Windows C、system volume information D、TEMP  
  
试题**2**： 加密技术中验证这一重要环节采用的关键技术是数字签名()A、是B、否  
  
试题**3**： 目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准()  
A、GB/T 18336-2001 信息技术安全性评估准则  
B、GB 17859-1999 计算机信息系统安全保护等级划分准则  
C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构  
D、GA/T 391-2002 计算机信息系统安全等级保护管理要求  
  
试题**4**： 关于双钥密码体制，下列说法中错误的是（）。  
A．双钥密码体制中加解密密钥不相同，从一个很难计算出另一个  
B．利用双钥密码体制实现数据保密时，用接收方的公钥加密数据  
C．双钥密码体制中加解密密钥虽不相同，但是可以从一个推导出另一个  
D．利用双钥密码体制可以实现数字签名  
  
试题**5**： 安全策略体系文件应当包括的内容不包括（）  
A.信息安全的定义、总体目标、范围及对组织的重要性B.对安全管理职责的定义和划分  
C. 口令、加密的使用是阻止性的技术控制措施；D. 违反安全策略的后果  
  
试题**6**： ATM机是我们日常存取现金都会接触的设备，以下关于ATM机的说法正确的是?（）  
A、 所有ATM机运行的都是专业操作系统，无法利用公开漏洞进行攻击，非常安全，  
B、 ATM机可能遭遇病毒侵袭  
C、 ATM机无法被黑客通过网络进行攻击  
D、 ATM机只有在进行系统升级时才无法运行，其他时间不会出现蓝屏等问题。  
  
试题**7**： 传统密码学的理论基础是（）  
A、 数学B、 物理学C、 计算机学科D、 力学  
  
试题**8**： 防火墙中网络地址转换（NAT）的主要作用是：（）  
A、提供代理服务B、隐藏内部网络地址C、进行入侵检测D、防止病毒入侵  
  
试题**9**： 公钥基础设施中不包括以下哪一项？（）  
A、CRL B、RA C、IKE D、CA  
  
试题**10**： 不属于物理安全威胁的是（）  
A、自然灾害B、物理攻击C、硬件故障D、系统安全管理人员培训不够

**2017/1/27 1~5 A C AD A B 6~10 A D C D A**

**2017/1/28 1~5 A D BC A A 6~10 D D B D B**

**2017/1/29 1~5 A A A A C 6~10 C A A A B**

**2017/1/30 1~5 A C A A C 6~10 A B C D D**

**2017/1/31 1~5 AD B B A B 6~10 D C BC B A**

**11~15 B C A A B 16~20 d b a b d**

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

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