**信息安全工程师每日一练试题（2017/2/15）**

试题**1**： 在信息系统设计中应高度重视系统的 (  ) 设计，防止对信息的篡改、越权获取和蓄意破坏以及防止自然灾害。
A、容错 B、结构化 C、可靠性 D、安全性

试题**2**： 网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行。其中，数据库容灾属于（ ）
A、物理线路安全和网络安全  B、物理线路安全和应用安全

C、系统安全和网络安全  D、系统安全和应用安全

试题**3**： 目前绝大多数 PKI使用的证书格式是()。
A、X506 , B、X509 C、PBE D、P7B

试题**4**： 防火墙要处理应用层的内容，首先需要进行数据包重组()
A、是B、否

试题**5**： PKI体系所遵循的国际标准是()
A、ISO 17799 B、ISO X.509 C、ISO 15408

试题**6**： 在 RSA 算法中,取 p=3,q=11,e=3,则 d 等于（）。
A.33        B.20          C.14          D.7

试题**7**： 信息安全策略,声称"密码的显示必须以掩码的形式"的目的是防范下面哪种攻击风险？（）
A.   尾随B.垃圾搜索C. 肩窥D. 冒充

试题**8**： 以下哪一种人给公司带来最大的安全风险？（）
A.临时工B.咨询人员C.以前员工D.当前员工

试题**9**： 在对某面向互联网提供服务的某应用服务器的安全检测中发现，服务器上开放了以下几个应用，除了一个应用外其他应用都存在明文传输信息的安全问题，作为一名检测人员，你需要告诉用户对应用进行安全整改以外解决明文传输数据的问题，以下哪个应用已经解决了明文传输数据问题：（）
A．SSH B．HTTP C．FTP D．SMTP

试题**10**： 电子商务系统除了面临一般的信息系统所涉及的安全威胁之外，更容易成为黑客分子的攻击目标，其安全性需求普遍高于一般的信息系统，电子商务系统中的信息安全需求不包括（）
A、交易的真实性B、交易的保密性和完整性C、交易的可撤销性D、交易的不可抵赖性

**信息安全工程师每日一练试题（2017/2/16）**

试题1： 公钥密码是（1），常用的公钥加密算法有（2），它可以是实现加密和数字签名。
（1）A、对称密钥技术，有1个密钥。B、不对称密钥技术，有2个密钥。
C、对称密钥技术，有2个密钥。D、不对称密钥技术，有1个密钥。
（2）A、DES B、IDES C、三元DES D、RSA

试题2： 信息安全的三个时代的认识，实践告诉我们()
A、不能只见物，不见人B、不能只见树，不见森林C、不能只见静，不见动D、A,B和C

试题3： 数字签名是附加于消息之后的一种数据，它是对消息的密码变换，保证了（）和完整性。
A．保密性                B．消息的来源              C．可用性        D．不可否认性

试题4： 对信息安全风险评估要素理解正确的是：（）
A．资产识别的粒度随着评估范围、评估目的的不同而不同，既可以是硬件设备，也可以是业务系统，也可以是组织机构
B．应针对构成信息系统的每个资产做风险评价
C．脆弱性识别是将信息系统安全现状与国家或行业的安全要求做符合性比对而找出的差
距项
D．信息系统面临的安全威胁仅包括人为故意威胁、人为非故意威胁

试题5： 以下哪个选项不是信息安全需求的来源?（）
A．法律法规与合同条约的要求B．组织的原则、目标和规定
C．风险评估的结果D．安全架构和安全厂商发布的病毒、漏洞预警

试题6： 以下哪一个是数据保护的最重要的目标？（）
A.确定需要访问信息的人员B.确保信息的完整性C.拒绝或授权对系统的访问D.监控逻辑访问

试题7： 下面哪一项不是通过IDS模型的组成部分：（）
A、传感器B、过滤器C、分析器D、管理器

试题8： 2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上指出，维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，正所谓“聪者听于无声，明者见于未形”。( )是最基本最基础的工作。
A. 感知网络安全态势B. 实施风险评估C. 加强安全策略D. 实行总体防御

试题9： 安全隔离网闸与防火墙相比，需要采取更强的安全隔离技术，请指出下列哪一项技术不会在安全隔离网闸中使用（）
A、专用的安全通信协议B、专用的硬件通信通道C、应用层的数据交换D、支持数据包路由

试题10： 利用公开密钥算法进行数据加密时，采用的方法是（）
A、发送方用公开密钥加密，接收方用公开密钥解密B、发送方用私有密钥加密，接收方用私有密钥解密
C、发送方用公开密钥加密，接收方用私有密钥解密D、发送方用私有密钥加密，接收方用公开密钥解密

**信息安全工程师每日一练试题（2017/2/17）**

试题**1**： 默认情况下，SQL Server的监听端口是()。
A、 1434 B、 1433C、 3305 D、3306

试题**2**： AES算法支持几种密钥长度？()
A、1 B、2 C、3 D、5

试题**3**： 关于我国信息安全保障工作发展的几个阶段，下列哪个说法不正确：（）
A．2001-2002 年是启动阶段，标志性事件是成立了网络与信息安全协调小组，该机构是我国信息安全保障工作的最高领导机构
B．2003-2005 年是逐步展开和积极推进阶段，标志性事件是发布了指导性文件《关于加强信息安全保障工作的意见》(中办发27 号文件)并颁布了国家信息安全战略
C．2005-至今是深化落实阶段，标志性事件是奥运会和世博会信息安全保障取得圆满成功&
D．2005-至今是深化落实阶段，信息安全保障体系建设取得实质性进展，各项信息安全保障工作迈出了坚实步伐

试题**4**： 以下关于互联网协议安全(Internet Protocol Security，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(Authentication Head，AH)和IP 封装安全载荷协议(EncapsulatingSecurity Payload，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(Internet Protocol，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**5**： 风险评估的基本过程是怎样的？（）
A. 识别并评估重要的信息资产，识别各种可能的威胁和严重的弱点，最终确定风险
B.    通过以往发生的信息安全事件，找到风险所在
C.风险评估就是对照安全检查单，查看相关的管理和技术措施是否到位
D.  风险评估并没有规律可循，完全取决于评估者的经验所在

试题**6**： 对磁介质的最有效好销毁方法是 ？（）
A.格式化B.物理破坏C.消磁D.删除

试题**7**： 下列关于Kerberos的描述，哪一项是正确的？（）
A.埃及神话中的有三个头的狗。B.安全模型。C.远程身份验证拨入用户服务器。

D.一个值得信赖的第三方认证协议。

试题**8**： 下面对于信息安全特征和范畴的说法错误的是：（）
A、信息安全是一个系统性的问题，不仅要考虑信息系统本身的技术问题，还要考虑人员、管理、政策等众多因素
B、信息安全是一个动态的问题，它随着信息技术的发展普及，以及产业基础、用户认识、投入产出而发展
C、信息安全是无边界的安全，互联网使得网络边界越来越模糊，因此确定一个组织的信息安全责任是没有意义的
D、信息安全是非传统的安全，各种信息网络的互联互通和资源共享，决定了信息安全具有不同于传统安全的特点

试题**9**： 下面关于我们使用的网络是否安全的正确表述是（）
A、 安装了防火墙，网络是安全的B、 设置了复杂的密码，网络是安全的
C、 安装了防火墙和杀毒软件，网络是安全的D、 没有绝对安全的网络，使用者要时刻提高警惕，谨慎操作

试题**10**： 信息安全管理体系（information SecurltyManagement System.简称ISMS）的实施和运行ISMS 阶段，是ISMS过程模型的实施阶段，下面给出了一些备57①制定风险处理计划②实施风险处理计划③开发有效性测量程序④实施培训和意识教育计划⑤管理ISMS的运行⑥管理ISMS的资源⑦执行检测事态和响应事件的程序⑧实施内部审核⑨实施风险再评估选的活动，选项（）描述了在此阶段组织应进行的活动。
A.①②③④⑤⑥ B.①②③④⑤⑥⑦ C.①②③④⑤⑥⑦⑧ D.①②③④⑤⑥⑦⑧⑨

**信息安全工程师每日一练试题（2017/2/18）**

试题**1**： 第一个计算机病毒出现在()
A、40年代B、70 年代C、90年代

试题**2**： 权限控制的粒度通常可以分为网络、设备、系统和\_\_\_\_\_\_()
A、功能、数据表、记录、字段和具体数值B、功能、数据库、记录、字段和具体内容
C、应用模块、数据表、记录、关键字和具体数值

试题**3**： 风险评估实施过程中资产识别的范围主要包括什么类别（）
A.网络硬件资产B.数据资产C.软件资产D.以上都包括

试题**4**： 种植、自启动、隐藏是木马程序的三大关键技术。由于杀病毒软件的存在，隐秘种植木马并不容易，其中一种较好的方法是　（1）　。在Windows系统中，为实现木马的自动启动，通常的方法是将其放于　（2）　中。为避免用户发现木马的存在，较好的隐藏方法　（3）　。
（1）A．当用户不在现场时派人安装B．当用户下载合法软件时顺便下载并安装
C．当用户在线观看电影时下载并安装D．当用户打开邮件附件时安装
（2）A．autoexec.bat文件 B．boot.ini文件C．config.sys文件 D．注册表
（3）A．不显示自己的名称等信息B．把自己更名成操作系统中一个合法程序的名字
C．伪装成一个系统服务D．需要运行时启动，运行完后退出
试题**5**： 关于控制措施选择描述不正确的是（）
A.总成本中应考虑控制措施维护成本B.只要控制措施有效，不管成本都应该首先选择
C.首先要考虑控制措施的成本效益D.应该考虑控制措施实施的成熟度

试题**6**： 个人问责不包括下列哪一项？（）
A.访问规则。B.策略与程序。C.审计跟踪。D.唯一身份标识符。

试题**7**： 下列哪一个说法是正确的？（）
A.风险越大，越不需要保护B.风险越小，越需要保护C.风险越大，越需要保护D.越是中等风险，越需要保护

试题**8**： 关于软件安全开发生命周期(SDL)，下面说法错误的是：（）
A．在软件开发的各个周期都要考虑安全因素
B．软件安全开发生命周期要综合采用技术、管理和工程等手段
C．测试阶段是发现并改正软件安全漏洞的最佳环节，过早或过晚检测修改漏洞都将增大软件开发成本
D．在设计阶段就尽可能发现并改正安全隐患，将极大减少整个软件开发成本

试题**9**： 安全备份的策略不包括（）
A、所有网络基础设施设备的配置和软件B、所有提供网络服务的服务器配置
C、网络服务D、定期验证备份文件的正确性和完整性

试题**10**： 以下关于SMTP和POP3协议的说法哪个是错误的：（）
A.SMTP和POP3协议是一种基于ASCII编码的请求/响应模式的协议
B.SMTP 和POP3协议明文传输数据，因此存在数据泄漏的可能
C.SMTP 和POP3协议缺乏严格的用户认证，因此导致了垃圾邮件问题
D.SMTP和POP3协议由于协议简单，易用性更高，更容易实现远程管理邮件

**信息安全工程师每日一练试题（2017/2/19）**

试题**1**： 以下关于校验码的叙述中，正确的是 （ ） 。
A、海明码利用多组数位的奇偶性来检错和纠错  B、海明码的码距必须大于等于1
C、循环冗余校验码具有很强的检错和纠错能力  D、循环冗余校验码的码距必定为1

试题**2**： 在数据库系统中，为了保证数据库的（），通常由DBA使用DBMS提供的授权功能为不同用户授权。
A．可靠性B．安全性C．一致性D．完整性

试题**3**： 信息系统安全可以分为5个层面的安全要求，包括：物理、网络、主机、应用、数据及备份恢复，“当检测到攻击行为时，记录攻击源IP，攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警“属于（）层面的要求
A、物理B、网络C、主机D、应用

试题**4**： 实施信息系统访问控制首先需要进行如下哪一项工作？（）
A.信息系统资产分类B.信息系统资产标识C.创建访问控制列表D.梳理信息系统相关信息资产

试题**5**： 发现个人电脑感染病毒，断开网络的目的是()
A、 影响上网速度B、 担心数据被泄露电脑被损坏C 控制病毒向外传播D、 防止计算机被病毒进一步感染

试题**6**： “中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（）
A.“普密”、“商密”两个级别B.“低级”和“高级”两个级别
C.“绝密”、“机密”、“秘密”三个级别D.“一密”、“二密”、“三密”、“四密”四个级别

试题**7**： 某单位计划在今年开发一套办公自动化(OA)系统，将集团公司各地的机构通过互联网进行协同办公，在OA系统的设计方案评审会上，提出了不少安全开发的建议，作为安全专家，请指出大家提的建议中不太合适的一条?（）
A．对软件开发商提出安全相关要求，确保软件开发商对安全足够的重视，投入资源解决软件安全问题
B．要求软件开发人员进行安全开发培训，使开发人员掌握基本软件安全开发知识
C.要求软件开发商使用Java而不是ASP作为开发语言，避免产生SQL注入漏洞
D．要求软件开发商对软件进行模块化设计，各模块明确输入和输出数据格式，并在使用前对输入数据进行校验

试题**8**： 根据《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》的规定，以下正确的是：（）
A．涉密信息系统的风险评估应按照《信息安全等级保护管理办法》等国家有关保密规定标准进行
B．非涉密信息系统的风险评估应按照《非涉及国家秘密的信息系统分级保护管理办法》等有关要求进行
C．可委托同一专业测评机构完成等级测评和风险评估工作，并形成等级测评报告和风险评估报告
D．此通知不要求将“信息安全风险评估”作为电子政务项目验收的重要内容
试题**9**： 有一种攻击是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪。这种攻击叫做（）
A、重放攻击B、拒绝服务攻击C、反射攻击D、服务攻击

试题**10**： Kerberos是一种常用的身份认证协议，它采用的加密算法是（）
A、Elgamal B、DES C、MD5 D、RSA

**信息安全工程师每日一练试题（2017/2/20）**

试题**1**： 入侵检测通过对计算机网络或计算机系统中的若干关键点收集信息并进行分析，发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件和硬件的组合就构成了入侵检测系统。（ ）是入侵检侧系统的核心。
A、评估主要系统和数据的完整性B、信息的收集C、系统审计D、数据分析

试题**2**： 甲利用对称密钥签名体制将签过名的文件发送给乙，甲不能抵赖、乙也不能伪造签名的原因是  （ ）  。
A．只有甲知道他的签名（除可信的仲裁者外），仲裁者转发甲的签名文件给乙时附加了唯一的声明信息
B．只有甲和乙知道共享密钥C．只有仲裁者同时知道所有的密钥D．只有乙知道甲的密钥

试题**3**： X.509数字证书中的签名字段是指（）。
A.用户对自己证书的签名B.用户对发送报文的签名 C.发证机构对用户证书的签名 D.发证机构对发送报文的签名

试题**4**： 组织允许外部通过互联网访问组织的局域网之前，首先要考虑实施以下哪项措施？（）
A.保护调制解调器池。B.考虑适当的身份验证方式。C.为用户提供账户使用信息。D.实施工作站锁定机制。

试题**5**： 数字签名应具有的性质不包括：（）
A、能够验证签名者B、能够认证被签名消息C、能够保护被签名的数据机密性

D、签名必须能够由第三方验证

试题**6**： 信息安全风险评估分为自评估和检查评估两种形式，下列描述不正确的是：（）
A、信息安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充
B、检查评估可在自评估实施的基础上，对关键环节或重点内容实施抽样评估
C、检查评估也可委托风险评估服务技术支持方实施，但评估结果仅对检查评估的发起单位负责
D、检查评估是指信息系统上级管理部门组织有关职能部门开展的风险评估

试题**7**： 关于比特币敲诈者的说法不正确的是（）
A、 流行于2015年初B、 受害者只要在规定时间内交纳一定数额的比特币，才可以解开被病毒加密的资料
C、 病毒作者波格挈夫来自俄罗斯D、 主要通过网页传播

试题**8**： 下列哪一项功能可以不由认证中心CA完成？（）
A.撤销和中止用户的证书B.产生并分发CA的公钥
C.在请求实体和它的公钥间建立链接D.发放并分发用户的证书

试题**9**： 通过反复尝试向系统提交用户名和密码以发现正确的用户密码的攻击方式称为：（）
A.账户信息收集B.密码分析C.密码嗅探D.密码暴力破解

试题**10**： 下述攻击手段中不属于DOS 攻击的是: （ ）
A.Smurf攻击B. Land 攻击C. Teardrop攻击D. CGI溢出攻击

**信息安全工程师每日一练试题（2017/2/21）**

试题**1**： （ ） 无法有效防御DDoS攻击。
A、根据IP地址对数据包进行过滤 B、为系统访问提供更高级别的身份认证 C、安装防病毒软件
D、使用工具软件检测不正常的高流量

试题**2**： 为了方便用户记忆使用、便于短信息服务提供商推广业务以及便于社会和政府监督短信息服务提供商的经营行为，作为“阳光绿色网络工程”中的一项工作，信息产业部将统一短信息服务提供商在不同移动运营企业的。()
A、服务内容B、服务代码C、宣传方式

试题**3**： 下面哪个不是执行备份操作的用户（    ）。
A．Administrators组的成员  B．Power Users组的成员C．Server Operators组的成员   D．Backup Operators组的成员

试题**4**： Kerberos算法是一个（）。
A、面向访问的保护系统 B、面向票据的保护系统    C、面向列表的保护系统    D、面向门与锁的保护系统

试题**5**： 在网络安全中，“拒绝服务攻击”是指（）。
A．用超出被攻击目标处理能力的海量数据包消耗可用系统、带宽资源等方法的攻击
B．全称是Distributed Denial Of Service的病毒传播技术
C．拒绝来自一个服务器所发送回应请求的指令的漏洞
D．入侵控制一个服务器后远程关机的破坏技术

试题**6**： 以下关于直接附加存储(Direct Attached Storage，DAS)说法错误的是：（）
A．DAS 能够在服务器物理位置比较分散的情况下实现大容量存储．是一种常用的数据存储方法
B．DAS 实现了操作系统与数据的分离，存取性能较高并且实施简单
C．DAS 的缺点在于对服务器依赖性强，当服务器发生故障时，连接在服务器上的存储设备中的数据不能被存取
D．较网络附加存储(Network Attached Storage，NAS)，DAS 节省硬盘空间，数据非常集中，便于对数据进行管理和备份

试题**7**： 信息系统安全工程(ISSE)的一个重要目标就是在IT 项目的各个阶段充分考虑安全因素，在IT 项目的立项阶段，以下哪一项不是必须进行的工作：（）
A．明确业务对信息安全的要求B．识别来自法律法规的安全要求C．论证安全要求是否正确完整
D．通过测试证明系统的功能和性能可以满足安全要求

试题**8**： TCSEC（橘皮书）中划分的7个安全等级中，（）是安全程度最高的安全等级
A．A1 B．A2 C．C1 D．C2

试题**9**： 以下哪一项不是PKI/CA 要解决的问题：（）
A、可用性、身份鉴别B、可用性、授权与访问控制C、完整性、授权与访问控制D、完整性、身份鉴别

试题**10**： 软件安全设计和开发中应考虑用户稳私包，以下关于用户隐私保护的说法哪个是错误的?（）
A．告诉用户需要收集什么数据及搜集到的数据会如何披使用
B．当用户的数据由于某种原因要被使用时，给用户选择是否允许
C．用户提交的用户名和密码属于稳私数据，其它都不是
D．确保数据的使用符合国家、地方、行业的相关法律法规

**信息安全工程师每日一练试题（2017/2/22）**

试题**1**： （ ） 无法有效防御DDos攻击
A、根据IP地址对数据包进行过滤 B、为系统访问提供更高级别的身份认证
C、分安装防病毒软件 D、使用工具软件检测不正常的高流量

试题**2**：  入侵检测的第一步是：()
A、信息收集B、信息分析C、数据包过滤D、数据包检查

试题**3**： 语义攻击利用的是()
A、信息内容的含义B、病毒对软件攻击C、黑客对系统攻击D、黑客和病毒的攻击

试题**4**： 等级保护三级的安全功能要素增加了()
A、强制访问控制、身份鉴别和数据完整性B、客体重用、标记C、强制访问控制、标记

试题**5**： 作为信息安全治理的成果,战略方针提供了:（）
A.企业所需的安全要求B.遵从最佳实务的安全基准C. 日常化制度化的解决方案D. 风险暴露的理解

试题**6**： 在计算可接受的关键业务流程恢复时间时（）
A.只需考虑停机时间的成本B.需要分析恢复操作的成本
C.停机时间成本和恢复操作成本都需要考虑D.可以忽略间接的停机成本

试题**7**： 以下哪一项不在数字证书数据的组成中? ( )
A、 版本信息B、 有效使用期限C、 签名算法D、 版权信息

试题**8**： 以下哪个拒绝服务攻击方式不是流量型拒绝服务攻击？（）
A．Land B．UDPFlood C．Smurf D．Teardrop

试题**9**： 下面对SSE-CMM保证过程的说法错误的是：（）
A.保证是指安全需求得到满足的可信任程度
B.信任程度来自于对安全工程过程结果质量的判断
C.自验证与证实安全的主要手段包括观察、论证、分析和测试
D.PA“建立保证论据”为PA“验证与证实安全”提供了证据支持

试题**10**： 证书中一般不包括以下内容中的：（）
A、证书主体的名称B、证书主体的公钥C、签发者的签名D、签发者的公钥

**2017/2/15 1~5 D D B A B 6~10 D C D A C**

**2017/2/16 1~5 BD D B A D 6~10 A B A D C**

**2017/2/17 1~5 B C C D A 6~10 B D C D B**

**2017/2/18 1~5 B A D DDB B 6~10 B C C C A**

**2017/2/19 1~5 A B B D B 6~10 C C C B B**

**2017/2/20 1~5 D A C B C 6~10 B D C D D**

**2017/2/21 1~5 C B B B A 6~10 A D A B C**

**2017/2/22 1~5 C A A C A 6~10 C D D D D**