**信息安全工程师每日一练（2016/7/26）**

第**1**题： 要成功实施信息系统安全管理并进行维护，应首先对系统（ ）进行评估鉴定。
A.风险 B.资产 C.威胁 D.脆弱性

第**2**题： 下面病毒中，属于蠕虫病毒的是  ( )。
A、Wom.Sasser病毒  B、Trojan.QQPSW病毒  C、Backdoor.IRCBot病毒  D、Macro.Melissa病毒

第**3**题： 下列叙述中错误的是(  )。
  A：数字签名可以保证信息在传输过程中的完整性B：数字签名可以保证数据在传输过程中的安全性
  C：数字签名可以对发送者的身份进行认证 D：数字签名可以防止交易中的抵赖法则

第**4**题： 下面对于标识和鉴别的解释最准确的是：()
A.标识用于区别不同的用户，而鉴别用于验证用户身份的真实性
B.标识用于区别不同的用户，而鉴别用于赋予用户权限
C.标识用于保证用户信息的完整性，而鉴别用于验证用户身份的真实性
D.标识用于保证用户信息的完整性，而鉴别用于赋予用户权限

第**5**题： 国际电信联盟将每年的5月17日确立为世界电信日，今年已经是第38届。今年世界电信日的主题为()
A、“让全球网络更安全”B、“信息通信技术：实现可持续发展的途径”C、“行动起来创建公平的信息社会”

第**6**题： 关于80年代Mirros蠕虫危害的描述，哪句话是错误的？（）
A、该蠕虫利用Unix系统上的漏洞传播 B、窃取用户的机密信息，破坏计算机数据文件
C、占用了大量的计算机处理器的时间，导致拒绝服务 D、大量的流量堵塞了网络，导致网络瘫痪

第**7**题： 为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（）
A、人际关系技能 B、项目管理技能 C、技术技能  D、沟通技能

第**8**题： 对MBOSS系统所有资产每年至少进行（）次安全漏洞自评估。
A、1               B、2               C、3               D、4

第**9**题： 数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？()
A、30%-40% B、40%-50% C、45%-60% D、50%-70%

第**10**题： 在IPSec中，（）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的IPSec协议、密码算法、密钥等信息。
A、ESP    B、SPI    C、SA    D、SP

**信息安全工程师每日一练（2016/7/27）**

第**1**题： 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

第**2**题： 修改已签订的合同文件，对原合同的什么属性造成了危害()。
A、完整性B、不可否认性C、可用性D、机密性

第**3**题： PDR模型中 Dt是从入侵者开始发动入侵开始，系统能够检测到()所花费的时间。
A、系统异常B、系统保护建立C、入侵行为D、灾难恢复启动

第**4**题： 不属于计算机病毒防治的策略的是（）
A.确认您手头常备一张真正“干净”的引导盘B.及时、可靠升级反病毒产品
C.新购置的计算机软件也要进行病毒检测 D.整理磁盘

第**5**题： 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

第**6**题： 信息安全风险缺口是指（）。
A、IT的发展与安全投入，安全意识和安全手段的不平衡 B、信息化中，信息不足产生的漏洞
C、计算机网络运行，维护的漏洞 D、计算中心的火灾隐患

第**7**题： 下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（）
A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定
B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级
C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案
D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

第**8**题： 只具有（）和FIN标志集的数据包是公认的恶意行为迹象。
A、SYN     B、date     C、head     D、标志位

第**9**题： 一般证书采用哪个标准？（）
A、ISO/IEC 15408       B、ISO/IEC 17799 C、BS  7799   D、X. 509V3

第**10**题： 网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？()
A、残余风险评估阶段 B、检查阶段C、入侵检测系统监控阶段 D、网络异常流量临控阶段

**信息安全工程师每日一练（2016/7/28）**

第**1**题： 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

第**2**题： 所谓网络安全漏洞是指\_\_\_(  )\_\_\_。
A.用户的误操作引起的系统故障
B.网络节点的系统软件或应用软件在逻辑设计上的缺陷
C.网络硬件性能下降产生的缺陷
D.网络协议运行中出现的错误
第**3**题： 在配置包过滤防火墙的规则时，以下说法不正确的是()。
A、使用源 IP地址过滤存在很大安全风险B、使用源端口过滤存在很大安全风险
C、按服务过滤数据包提供更高的安全性D、使用目的 IP地址过滤存在很大安全风险

第**4**题： “阳光绿色网络工程”的“阳光”寓意着光明和普惠万事万物，并要涤荡网络上的污浊；“绿色”代表要面向未来构建充满生机的和谐网络环境；“网络”代表活动的主要内容以网络信息服务为主；“工程”代表活动的系统性和长期性。系列活动的副主题为：倡导网络文明，\_\_\_\_\_。
A、构建和谐环境
B、打击网络犯罪
C、清除网络垃圾

第**5**题： 第一次出现"HACKER"这个词是在()
A、BELL实验室B、麻省理工AI实验室C、AT&T实验室

第**6**题： 文件型病毒传染的对象主要是（     ）类文件。
A．.EXE和.WPS    B．COM和.EXE      C．.WPS         D．.DBF

第**7**题： DES是一种block（块）密文的加密算法，是把数据加密成多大的块？（）
A、32位          B、64位            C、128位            D、256位

第**8**题： 下列哪项为信息泄露与错误处理不当Information Leakage and Improper
Error Handlina攻击具体实例？()
A、不明邮件中隐藏的html链接 B、发帖子，发消息C、上传附件 D、错误信息揭示路径

第**9**题： 以下哪项是数据库加密方法中的库外加密的缺点？（）
A、即使访问一条数据也要对整个数据库解密     B、密钥管理比较复杂
C、加密之后不能完整的查询数据     D、密钥过于简单，容易被破解

第**10**题： 以下哪个描述是不正确的？（       ）

A. 未经审批，不允许私自在建设银行网络系统内开设游戏网站、论坛、聊天室等与工作无关的网络服务

B. 发送办公邮件必须使用建行统一的邮箱（如xxx@ccb.com）

C. 采用3G上网卡或自行安装ADSL宽带等方式作为我行接入和访问互联网的备选方案.

D. 移动办公终端上不得处理敏感文件

**信息安全工程师每日一练（2016/7/29）**

第**1**题： 某企业应用系统为保证运行安全，只允许操作人员在规定的工作时间段内登录该系统进行业务操作，这种安全策略属于（ ）层次。
A．数据域安全 B．功能性安全C．资源访问安全 D．系统级安全

第**2**题： 以下关于信息安全管理的描述中，错误的是( )。
A.安全管理贯穿于计算机网络系统规划、设计、实施、运维等各个阶段，既包括行政手段，又包括技术措施
B.一级安全管理制度的控制点有两个，二级、三级、四级安全管理制度的控制点有3个
C.信息安全的3条基本管理原则是:单独工作原则、限制使用期限原则和责任分散原则
D.在安全管理中，最活跃的因素是人，对人的管理基于完备安全管理政策和制度这一前提

第**3**题： 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

第**4**题： 关于网络安全措施，以下说法错误的是（  ）。
A.加强口令管理  B.从著名网站上下载资料  C.安装防火墙  D.不限制浏览内容

第**5**题： 一般而言，网络安全审计从审计级别上可分为（  ）、应用级设计和用户级审计三种级别
A、组织级审计B、物理审计C、系统级审计D、单元级审计

第**6**题： 目前 Word加密时，使用的对称加密算法是()。
A、DES B、RC4 C、AES D、RSA

第**7**题： 测试数据库一个月程序主要应对的风险是（）。
A、非授权用户执行“ROLLBACK”命令 B、非授权用户执行“COMMIT”命令
C、非授权用户执行“ROLLRORWARD”命令 D、非授权用户修改数据库中的行

第**8**题： 单项散列函数的安全性来自于他的（）。
A、单向性    B、算法复杂性    C、算法的保密性    D、离散性

第**9**题： 对明文字母重新排列，并不隐藏他们的加密方法属于（）。
A、置换密码    B、分组密码    C、易位密码    D、序列密码

第**10**题： 网络病毒预防范阶段的主要措施是什么？()
A、强制补丁、网络异常流量的发现 B、强制补丁、入侵检测系统监控
C、网络异常流量的发现、入侵检测系统的监控阶段   D、缺少D选项

**信息安全工程师每日一练（2016/7/30）**

第**1**题： 在进行金融业务系统的网络设计时，应该优先考虑（ ）原则。
A. 先进性 B. 开放性 C. 经济性 D. 高可用性

第**2**题： 以下关于网络物理隔离技术的描述中，错误的是( )。
A.内网与外网(或内网与专网)永不连接
B.内网与外网(或内网与专网)的数据交换采用渡船策略
C.每一次数据交换，都需要经历数据写入和数据读出两个过程
D.内网和外网(或内网与专网)在同一时刻最多只有一个物理隔离设备建立TCP/IP数据连接

第**3**题： 信息安全策略的设计与实施步骤是( )。
A.定义活动目录角色、确定组策略管理安全性、身份验证、访问控制和管理委派
B.确定标准性、规范性、可控性、整体性、最小影响、保密性原则，确定公钥基本结构
C.确定安全需求、制订可实现的安全目标、制订安全规划、制订系统的日常维护计划
D.确定安全需求、确定安全需求的范围、制订安全规划、制订系统的日常维护计划

第**4**题： 以下关于WLAN安全机制的叙述中，（  ）是正确的
A、WPA是为建立无线网络安全环境提供的第一个安全机制
B、WEP和IPSec协议一样，其目标都是通过加密无线电波来提供安全保护
C、WEP2的初始化向量（IV）空间64位
D、WPA提供了比WEP更为安全的无线局域网接入方案

第**5**题： Windows 2000 中的 SAM文件默认保存在什么目录下？（）
A、 WINNT B、 WINNT/SYSTEM C、 WINNT/SYSTEM32 D、WINNT/SYSTEM32/config

第**6**题： 以下哪两个安全模型分别是多级完整性模型和多边保密模型？（）
A.Biba 模型和Bell一Lapadula 模型 B.Bell 一Lapaduia 模型和Biba 模型
C.Chinese Wall 模型和Bell 一Lapadula 模型 D.Biba 模型和Chinese Wall 模型

第**7**题： 用于实现交换机端口镜像的交换机功能是：（）
A、PERMIT LIST   B、PVLAN     C、VTP     D、SPAN

第**8**题： 在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（）
A、IETF 因特网工程工作小组   B、ISO 国际标准组织
C、IANA 因特网地址指派机构     D、OSI 开放系统互联

第**9**题： 机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（）m。
A、0.1B、0.6C、1.2D、0.3

第**10**题： 远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（）
A、知道什么    B、拥有什么   C、是谁    D、双因素认证

**信息安全工程师每日一练（2016/7/31）**

第**1**题： DES是一种 （ ） 算法。
A、共享密钥  B、公开密钥  C、报文摘要  D、访问控制

第**2**题： 静态包过滤技术是第（ ）代包过滤技术。
A、一B、二C、三D、四

第**3**题： 在信息安全的服务中，访问控制的作用是什么？()
A、如何确定自己的身份，如利用一个带有密码的用户帐号登录
B、赋予用户对文件和目录的权限
C、保护系统或主机上的数据不被非认证的用户访问
D、提供类似网络中“劫持”这种手段的攻击的保护措施

第**4**题： 下列关于政务内网和外网的关系，哪项描述是不准确的？ （）
A、两者适用级别不同B、两者对安全要求的级别不同
C、两者主要服务的对象不同D、两者是完全独立的

第**5**题： 信息产业的重要特征是（ ）。
A、高风险型产业B、知识能力密集型产业C、高回报型产业D、搞创新型产业

第**6**题： 在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（）
A、当信息安全事件的负面影响扩展到本组织意外时
B、只要发生了安全事件就应当公告
C、只有公众的什么财产安全受到巨大危害时才公告
D、当信息安全事件平息之后

第**7**题： U盘病毒依赖于哪个文件打到自我运行的目的？（）
A、autoron.inf B、autoexec.bat C、config.sys D、system.ini

第**8**题： 在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（）
A、产生日志的数量     B、攻击减少的速度    C、较低的价格     D、假阳性的减少量

第**9**题： 以下哪种符号在SQL注入攻击中经常用到？()
A、$\_         B、1             C、@           D、;

第**10**题： 下列关于口令持有人保证口令保密性的正确做法是：（      ）

A．将口令记录在笔记本中  B．将口令贴在计算机机箱或终端屏幕上

C．将计算机系统用户口令借给他人使用  D．一旦发现或怀疑计算机系统用户口令泄露，立即更换

**信息安全工程师每日一练（****2016/8/1）**

第**1**题： 在信息系统的用户管理中，(   )身份认证方式是一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾.
A.用户名/密码B.动态密码C.IC卡D.USB Key

第**2**题： 许多黑客利用缓冲区溢出漏洞进行攻击，对于这一威胁，最可靠的解决方案是 （ ） 。
A、安装防火墙 B、安装用户认证系统 C、安装相关的系统补丁 D、安装防病毒软件

第**3**题： 物理安全技术包括机房安全和（）。
A、数据安全   B、系统安全 C、通信安全  D、设施安全

第**4**题： 下列存储介质中，容量最小的是()。
A、软盘B、CD-RWC、闪盘D、移动硬盘

第**5**题： 全球最大网络设备供应商是（）
A.华为B.H3CC.思科D.中兴

第**6**题： 在Oracle中，用ALTER将scott的口令改为hello，下列哪个是正确的？（）
A、ALTER  USER   scott  IDENTIFIED  BY  hello
B、ALTER   scott   USER    IDENTIFIED   BY  hello
C、ALTER   USER   scott  IDENTIFIED   AS  hello
D、ALTER   USER   hello   IDENTIFIED   BY  scott

第**7**题： 计算机电源系统的所有节点均应镀铅锡处理（）连接。
A、热压B、冷压C、焊锡D、直接

第**8**题： CA指的是（）。
A、证书授权    B、加密认证    C、虚拟专用网    D、安全套接层

第**9**题： 高级加密标准AES算法中，加密回合数不可能是（）。
A、10    B、12    C、14    D、16

第**10**题： 下列哪项不是安全编码中输入验证的控制项？()
A、数字型的输入必须是合法的数字 B、字符型的输入中对’进行特殊处理
C、验证所有的输入点，包括Get，Post，Cookie以及其他HTTP头
D、正确使用静态查询语句，如PreDaredStatement

**信息安全工程师每日一练（****2016/8/2）**

第**1**题： 灾难恢复目标的设置不包括（）
A、关键业务功能及恢复的优先顺序 B、RTO C、RPO D、灾难环境

第**2**题： 以下用于在网路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

第**3**题： 在Kerberos系统中，使用一次性密钥和 （ ） 来防止重放攻击。
A、时间戳 B、数字签名 C、序列号 D、数字证书

第**4**题： 网络的可用性是指( )。
A、网络通信能力的大小  B、用户用于网络维修的时间  C、网络的可靠性  D、用户可利用网络时间的百分比

第**5**题： 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

第**6**题：  新买回来的未格式化的软盘()。
A、可能会有计算机病毒B、与带病毒的软盘放在一起会有计算机病毒
C、一定没有计算机病毒D、经拿过带病毒的软盘的手碰过后会感染计算机病毒

第**7**题： 以下哪一项是DOS攻击的一个实例()
A.SQL注入    B.IP Spoof   C.Smurf攻击    D.字典破解

第**8**题： 什么是IDS？（）
A、入侵检测系统    B、入侵防御系统    C、网络审计系统    D、主机扫描系统

第**9**题： 关于CA和数字证书的关系，以下说法不正确的是（）。
A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由CA签发
B、数字证书一般依靠CA中心的对称密钥机制来实现
C、在电子交易中，数字证书可以用于表明参与方的身份
D、数字证书能以一种不能被假冒的方式证明证书持有人身份

第**10**题： Web应用漏洞按类别进行排名，由多到少正确的顺序为？（）
A、跨站脚本、注入、恶意代码、引用不当    B、注入、跨站脚本、恶意代码、引用不当
C、恶意代码、跨站脚本、注入、引用不当    D、引用不当、跨站脚本、注入、恶意代码

**2016/7/26 1~5 D A B A A 6~10 B D A C C**

**2016/7/27 1~5 B A C D C 6~10 A C A D A**

**2016/7/28 1~5 C B D A B 6~10 B B D A C**

**2016/7/29 1~5 D C A D C 6~10 B B A C A**

**2016/7/30 1~5 D D C D D 6~10 D D D B B**

**2016/7/31 1~5 A A B D B 6~10 A A B D D**

**2016/8/1 1~5 D C D A C 6~10 A B A D D**

**2016/8/2 1~5 D B A D B 6~10 C C A B A**