**信息安全工程师每日一练（2016/8/3）**

第**1**题： 信息安全风险评估（ ）。
A、只需要实施一次就可以B、应该根据变化了的情况定期或不定期地适时进行
C、不需要形成文件化评估结果报告D、仅对网络做定期的扫描就行

第**2**题： （ ） 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

第**3**题： 《电信条例》规定，在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显包含违法内容时，应当立即，保存有关记录并\_\_\_\_\_，并向国家有关机关报告。
A、停止传输B、中断网络C、跟踪调查

第**4**题： 安全基线达标管理办法规定：BSS系统口令设置应遵循的内控要求是（）
A、数字+字母     B、数字+字母+符号C、数字+字母+字母大小写   D、数字+符号

第**5**题： 档案权限755，对档案拥有者而言，是什么含义？（）
A、可读，可执行，可写入 B、可读 C、可读，可执行 D、可写入

第**6**题： 在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（）
A、报文服务拒绝     B、假冒   C、数据流分析    D、报文服务更改

第**7**题： 下列哪种工具不是WEB服务器漏洞扫描工具（）？
A、Nikto B、Web  Dumper C、paros  Proxy D、Nessus

第**8**题： 在Oracle中，建表约束包括引用完整性约束、check完整性约束，还有以下三项是正确的，请排除一个错误选项。（）
A、非空完整性约束 B、唯一完整性约束 C、主码完整性约束 D、数据角色性约束

第**9**题： （）原则允许某些用户进行特定访问。
A、保密性   B、鉴别    C、完整性     D、访问控制

第**10**题： 以下各种加密算法中属于双钥制加密算法的是（）。
A、DES加密算法    B、Caesar替代法    C、Vigenere算法    D、Diffie-Hellman加密

**信息安全工程师每日一练（2016/8/4）**

第**1**题： 银河大学是一所拥有6万多名师生的综合性大学。规划师对于该大学数据中心网络防火墙的访问控制问题，最可能采取的方案是( )。
A.基于角色的访问控制(RBAC)方案B.自主型访问控制(DAC)方案
C.基于任务的访问控制(TBAC)方案D.强制型访问控制(MAC)方案

第**2**题： CA安全认证中心可以（ ）。
A、用于在电子商务交易中实现身份认证 B、完成数据加密，保护内部关键信息
C、支持在线销售和在线谈判，认证用户的订单 D、提供用户接入线路，保证线路的安全性

第**3**题： 实现VPN的关键技术主要有隧道技术、加解密技术、  （ ）  和身份认证技术。
A、入侵检测技术 B、病毒防治技术 C、安全审计技术 D、密钥管理技术
第**4**题： 以下不是安全审计系统作用的是()。
A、记录和跟踪各种系统状态的变化B、对审计日志进行智能分析
C、实现对各种安全事故的定位D、对攻击者的犯罪行为进行处罚
第**5**题：  安全策略管理：指管理、保护及自动分发()的安全策略。
A、设备B、全局性C、用户D、组织

第**6**题： 关于组策略的描述哪些是错误的?()
A、首先应用的是本地组策略
B、除非冲突，组策略的应用应该是累积的
C、如果存在冲突，最先应用的组策略将获胜
D、策略在策略容器上的顺序决定应用的顺序

第**7**题： 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（）。
A、已买的软件   B、定做的软件   C、硬件     D、数据

第**8**题： 在安全审计的风险评估阶段，通常是按什么顺序来进行的？（）
A、侦查阶段、渗透阶段、控制阶段     B、渗透阶段、侦查阶段、控制阶段
C、控制阶段、侦查阶段、渗透阶段   D、侦查阶段、控制阶段、渗透阶段

第**9**题： 为什么要对数据库进行“非规范化”处理（）？
A、确保数据完整性 B、增加处理效率 C、防止数据重复 D、节省存储空间

第**10**题： 加密技术不能实现（）。
A、数据信息的完整性    B、基于密码技术的身份认证    C、机密文件加密    D、基于IP头信息的包过滤

**信息安全工程师每日一练（2016/8/5）**

第**1**题： （ ）不是超安全的信息安全保障系统（S2-MIS）的特点或要求。
A．硬件和系统软件通用
B．PKI/CA安全保障系统必须带密码
C．业务应用系统 在实施过程中有重大变化
D．主要的硬件和系统软件需要PKI/CA认证

第**2**题： （ ） 不属于PKICA认证中心的功能
A、接收并验证最终用户数字证书的申请
B、向申请者颁发或拒绝颁发数字证书
C、产生和发布证书废止列表（CRL），验证证书状态
D、业务受理点LRA的全面管理

第**3**题： 以下关于第三方认证服务的叙述中，正确的是（）。
A．Kerberos认证服务中保存数字证书的服务器叫CA B．第三方认证服务的两种体制分别是Kerberos和PKI
C．PKI体制中保存数字证书的服务器叫KDC D．Kerberos的中文全称是“公钥基础设施”

第**4**题： 目前使用最广泛的公钥算法是()。
A、DES B、RSA C、Elgamal D、ECC

第**5**题： 黑客进行攻击的最后一个步骤是：()
A.侦查与信息收集    B.漏洞分析与目标选定   C.获取系统权限   D.打扫战场、清楚证据

第**6**题： 抵御电子邮箱入侵措施中，不正确的是（）
A、不用生日做密码B、不要使用少于5位的密码C、不要使用纯数字D、自己做服务器
第**7**题： 在Solaris 8下，对于/etc/shadow文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（）。
A、是/etc/passwd文件格式 B、是/etc/shadow文件格式 C、既不是/etc/passwd也不是/etc/shadow文件格式
D、这个root用户没有SHELL，不可登录 E、这个用户不可登录，并不是因为没有SHELL

第**8**题： 下列（）灭火器是扑救精密仪器火灾的最佳选择。
A、二氧化碳灭火剂   B、干粉灭火剂   C、泡沫灭火剂

第**9**题： 数字证书的应用阶段不包括（）。
A、证书检索   B、证书验证    C、密钥恢复    D、证书撤销

第**10**题： 在为计算机设置使用密码时，下面（）密码是最安全的。
A、12345678   B、66666666 C、20061001   D、72aB@#41

 **信息安全工程师每日一练（2016/8/6）**

第**1**题： 设置计算机的无线网卡，使该计算机与实验室的无线访问点LabAP之间的通信能够受密码保护，指定密钥为2350AD9FE0，则下图中应设置  （ ）  。

A、SSID为LabAP，网络验证为开放式，数据加密为WEP
B、SSID为2350AD9FE0，网络验证为开放式，数据加密为WEP
C、SSID为LabAP，网络验证为WEP，数据加密为开放式
D、SSID为2350AD9FE0，网络验证为WEP，数据加密为开放式

第**2**题： 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. ②③①C. ③②①D. ②①③
第**3**题： 操作系统指纹扫描技术的关键技术（ ）。
A、TCP/IP协议的指纹技术B、HTTP协议的指纹技术
C、FTP协议的指纹技术D、Telnet协议的指纹技术

第**4**题： 什么是标识用户、组和计算机帐户的唯一数字？()
A、 SID B、 LSA C、 SAM D、 SRM

第**5**题： 一个单位在处理一台储存过高密级信息的计算机是首先应该做什么？（）
A.将硬盘的每一个比特写成“O” B.将硬盘彻底毁坏C．选择秘密信息进行删除D．进行低级格式化
第**6**题： 接口被绑定在2层的zone，这个接口的接口模式是（）。
A、NAT mode B、Route mode C、-Transparent mode D、NAT或Route mode

第**7**题： 有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（）。
A、L2TP是由PPTV协议和Cisco公司的L2F组合而成
B、L2TP可用于基于Internet的远程拨号访问
C、为PPP协议的客户建立拨号连接的VPN连接
D、L2TP只能通过TCP/IP连接

第**8**题： Windows NT 和Windows 2003系统能设置为在几次无效登录后锁定帐号,这可以防止：（  ）。
A．木马      B．暴力攻击     C．IP欺骗       D．缓存溢出攻击

第**9**题： 若单项散列函数的输入串有很小的变化，则输出串（）。
A、可能有很大的变化    B、一定有很大的变化
C、可能有很小的变化    D、一定有很小的变化

第**10**题： Web应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（）
A、静态密码     B、短信挑战     C、指纹认证     D、图片认证

**信息安全工程师每日一练（2016/8/7）**

第**1**题： 在系统集成项目中，采取相应的措施保护计算机网络设备免受环境事故的影响，属于ISO/IEC27000系列标准中信息安全管理的( )范畴.
A.组织信息安全B.通信和操作安全C.物理和环境安全D.访问控制
第**2**题： 以下关于利用三重DES进行加密的说法，（）是正确的。
A．三重DES的密钥长度是56位
B．三重DES使用三个不同的密钥进行三次加密
C．三重DES的安全性高于DES
D．三重DES的加密速度比DES加密速度快
第**3**题： 哪一条不是防止 FTP跳转攻击的方法？()
A、服务器最好不要打开数据链接到小于 1024的 TCP端口号
B、禁止使用 PORT命令也是避免跳转攻击的一种方法
C、使用适当的文件保护措施
D、防火墙控制
第**4**题：  以下哪一项不是安全策略管理系统的组成部分？()
A、日志与审计服务B、策略管理中心C、策略执行点D、SPM网关
第**5**题： “在遇到应急事件后所采取的措施和行动”被称为（）。
A、灾难恢复B、数据恢复C、应急响应D、计算机取证
第**6**题： 除了哪种特性之外，其他安全特性在 Windows 2000种都可以通过系统本身的工具来进行设置和控制？()
A、物理安全性B、用户安全性C、文件安全性D、入侵安全性
第**7**题： 为了规范互联网电子邮件服务，依法治理垃圾电子邮件问题，保障互联网电子邮件用户的合法权益，信息产业部于2006年2月20日颁布了\_\_\_\_\_，自2006年3月30日开始施行。
《互联网信息服务管理办法》
《互联网电子邮件服务管理办法》
《互联网电子公告服务管理规定》
第**8**题： 向有限的空间输入超长的字符串是哪一种攻击手段？（）
A、缓冲区溢出B、网络监听C、拒绝服务D、IP欺骗
第**9**题： 以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（）
A、主从式结构是指一个主机带多个终端的多用户结构
B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上
C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源
D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈
第**10**题： 《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（）。
A、GA 163-1997 B、GA 267-2000 C、GA 243-2000 D、GB 17859-1999

**信息安全工程师每日一练（2016/8/8）**

第**1**题： 某商业银行决定开发网络安全审计系统，希望该系统是在应用系统内部嵌入一个与应用服务同步运行专用的审计服务应用进程，用于全程跟踪应用服务进程的运行。该商业银行的安全审计系统最适合采用（  ）。
A．基于网络旁路监控的审计B．基于应用系统独立程序的审计
C．基于网络安全入侵检测的预警系统D．基于应用系统代理的审计
第**2**题： 计算机感染特洛伊木马后的典型现象是 （ ） 。
A、程序异常退出 B、有未知程序试图建立网络连接
C、邮箱被垃圾邮件填满 D、Windows 系统黑屏
第**3**题： 杀毒软件报告发现病毒 Macro.Melissa，由该病毒名称可以推断病毒类型是 （1）  ，这类病毒主要感染目标是  （2）  。
（1）A、文件型  B、引导型  C、目录型  D、宏病毒
（2）A、EXE 或 COM 可执行文件  B、Word 或 Excel 文件
C、DLL 系统文件  D、磁盘引导区
第**4**题： 异常入侵检测以()作为比较的参考基准。
A、异常的行为特征轮廓B、正常的行为特征轮廓C、日志记录D、审计记录
第**5**题： 下面哪个功能属于操作系统中的日志记录功能（）
A、控制用户的作业排序和运行
B、以合理的方式处理错误事件，而不至于影响其他程序的正常运行
C、保护系统程序和作业，禁止不合要求的对程序和数据的访问
D、对计算机用户访问系统和资源的情况进行记录
第**6**题： 系统管理员属于（）。
A、决策层       B、管理层 C、执行层 D、既可以划为管理层，又可以划为执行层
第**7**题： 有一些应用，如微软Out look或MSN。它们的外观会在转化为基于Web界面的过程中丢失，此时要用到以下哪项技术：（）
A、Web代理     B、端口转发    C、文件共享    D、网络扩展
第**8**题： 一般来说，通过WEB运行http服务的子进程时，我们会选择（）的用户权限方式，这样可以保证系统的安全。
A、root B、httpd C、guest D、nobody
第**9**题： 通过收集和分析计算机系统或网络的关键节点信息，以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的技术被称为（）
A、系统检测B、系统分析C、系统审计D、入侵检测
第**10**题： 信息风险主要指那些？（      ）
A．信息存储安全         B．信息传输安全   C．信息访问安全     D．以上都正确

**2016/8/3 1~5 B D A C A 6~10 C B D D D**

**2016/8/4 1~5 A A D D B 6~10 C D A B D**

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

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

**2016/8/7 1~5 C C D D C 6~10 A B A D B**

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