**信息安全工程师每日一练试题（2017/3/1）**

试题**1**： 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  
  
试题**2**： 黑客小张企图入侵某公司网络，窃取机密信息。为快速达到目的，他做的第一步通常是(1)；第二步通常是(2)。在成功入侵该公司网络某台主机并取得该主机的控制权后，通常还需(3);在窃取到机密信息后，最后还会(4)。为了预防黑客入侵的第一步，该公司网络应该采取的预防措施为(5);针对第二步的预防措施为(6)。为了能及时发现上述入侵，该公司网络需要配备(7)  。  
(1)A．收集目标网络的所在位置及流量信息B．到网上去下载常用的一些攻击软件  
C．捕获跳板主机，利用跳板主机准备入侵

D．通过端口扫描等软件收集目标网站的IP地址、开放端口和安装的软件版本等信息  
(2)A．了解目标网络的所在位置的周围情况及流量规律，选择流量小的时间发起攻击  
B．下载攻击软件，直接发起攻击C．向目标网络发起拒绝服务攻击

D．根据收集的开放端口和安装的软件版本等信息，到网络查找相关的系统漏洞，下载相应的攻击工具软件?  
(3)A．修改该主机的root或管理员口令，方便后续登录  
B．在该主机上安装木马或后门程序，方便后续登录  
C．在该主机上启动远程桌面程序，方便后续登录  
D．在该主机上安装网络蠕虫程序以便入侵公司网络中的其他主机  
(4)A．尽快把机密数据发送出去  
B．在主机中留一份机密信息的副本，以后方便时来取  
C．删除主机系统中的相关日志信息，以免被管理员发现  
D．删除新建用户，尽快退出，以免被管理员发现  
(5)A．尽量保密公司网络的所在位置和流量信息  
B．尽量减少公司网络对外的网络接口  
C．尽量关闭主机系统上不需要的服务和端口  
D．尽量降低公司网络对外的网络接口速率  
(6)A．安装网络防病毒软件，防止病毒和木马的入侵  
B．及时对网络内部的主机系统进行安全扫描并修补相关的系统漏洞  
C．加大公司网络对外的网络接口速率  
D．在公司网络中增加防火墙设备  
(7)  A．入侵检测系统 B．VPN系统 C．安全扫描系统 D．防火墙系统   
  
试题**3**： ISO／IBC27001《信息技术 安全技术 信息安全管理体系要求》的内容是基于 （）。  
A．BS7799-1《信息安全实施细则》B．BS7799-2《信息安全管理体系规范》  
C．信息技术安全评估准则(简称ITSEC)D．信息技术安全评估通用标准(简称CC)  
  
试题**4**： 系统上线前应当对系统安全配置进行检查，不包括下列哪种安全检查（）  
A.主机操作系统安全配置检查B.网络设备安全配置检查C.系统软件安全漏洞检查D.数据库安全配置检查  
  
试题**5**： 某单位通过防火墙进行互联网接入，外网口地址为202.101.1.1，内网口地址为192.168.1.1，这种情况下防火墙工作模式为：（）  
A.透明模式B.路由模式C.代理模式D.以上都不对  
  
试题**6**： 在RSA算法中，公钥为PU=｛e，n｝，私钥为PR=｛d，n｝，下列关于e，d，n，的说法正确的是。（）  
A、收发双方均已知n B、收发双方均已知d C、由e 和n可以很容易地确定d D、只有接收方已知e  
  
试题**7**： A technical lead who was working on a major project has left the organization. The project manager reports suspicious system activities on one of the servers that is accessible to the whole team. What would be of GREATEST concern if discovered during a forensic investigation?   
A、Audit logs are not enabled for the system B、A logon ID for the technical lead still exists   
C、Spyware is installed on the system D、A Trojan is installed on the system   
  
试题**8**： An organization is using an enterprise resource management (ERP) application. Which of the following would be an effective access control?   
A、User-level permissions   
B、Role-based   
C、Fine-grained   
D、Discretionary   
  
试题**9**： To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:   
A、Secure Shell (SSH-2) tunnel for the duration of the problem.   
B、two-factor authentication mechanism for network access.   
C、dial-in access.   
D、virtual private network (VPN) account for the duration of the vendor support contract.   
  
试题**10**： Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?   
A、Multiple cycles of backup files remain available.   
B、Access controls establish accountability for e-mail activity.   
C、Data classification regulates what information should be communicated via e-mail.   
D、Within the enterprise, a clear policy for using e-mail ensures that evidence is available.   
  
试题**11**： The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:   
A、achieve performance improvement. B、provide user authentication.   
C、ensure availability of data. D、ensure the confidentiality of data.   
  
试题**12**： 在一个非屏蔽双绞线（UTP）网络中的一根以太网电缆长于100米。这个电缆长度可能引起下列哪一种后果？  
A、电磁干扰B、串扰C、离散D、衰减  
  
试题**13**： 下面哪一个是IT绩效评估流程的主要目标？（）  
A.使错误最小化B.收集绩效数据C.建立绩效基准D.优化绩效  
  
试题**14**： 灾难性恢复计划 (DRP) 基于: （）  
A、技术方面的业务连续性规划. B、进行一块业务连续性规划.

C、功能方面的业务连续性规划. D、总体协调的业务连续性规划.   
  
试题**15**： 下列哪个选项是网络服务器最通常用的CGI(普通网关接口)？（）  
A.传输数据到应用程序又返回到用户B.电影电视的电脑图像处理  
C.网络设计的用户图形界面D.访问个人网管域的接口  
  
试题**16**： 以下关于备份站点的说法哪项是正确的（）  
A、应与原业务系统具有同样的物理访问控制措施B、应容易被找到以便于在灾难发生时以备紧急情况的需要  
C、应部署在离原业务系统所在地较近的地方D、不需要具有和原业务系统相同的环境监控等级  
  
试题**17**： 一家公司采用动态主机配置协议。假设下列情形存在，哪项最值得关注？（）  
A、大多数员工使用膝上电脑.B、一个包过滤防火墙被使用.  
C、IP地址范围小于PC的数量D、对网络端口的访问没有限制

试题**18**： 某第三方应用作为多个外部系统的接口。在该应用中发现安全漏洞后，大量的模块被打上了补丁。IS审计员应建议执行以下哪个测试（）  
A、Stress 负载B、Black box 黑盒C、Interface 接口D、System 系统  
  
试题**19**： 以下哪个数据库管理员的操作应由另外一个人来执行？  
A、删除数据库操作日志B、优化数据库工具C、检测数据库的使用情况D、定义备份及恢复流程  
  
试题**20**： 在电子邮件中让数字签名生效会：（）  
A、帮助检测广告邮件B、提供机密性C、会给网关服务器增加负载D、明显减少带宽的有效性

**信息安全工程师每日一练试题（2017/3/2）**

试题**1**： 设数据码字为10010011，采用海明码进行校验，则必须加入  （ ）  比特冗余位才能纠正一位错。  
A、2 B、3 C、4 D、5  
  
试题**2**： 以下关于软件安全测试说法正确的是？（）  
A.软件安全测试就是黑盒测试。B.Fuzz测试是经常采用的安全测试方法之一。  
C.软件安全测试关注的是软件的功能。D.软件安全测试可以发现软件中产生的所有安全问题。  
  
试题**3**： To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?   
A、O/S and hardware refresh frequencies B、Gain-sharing performance bonuses   
C、Penalties for noncompliance D、Charges tied to variable cost metrics   
  
试题**4**： Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?   
A、Test data run B、Code review C、Automated code comparison D、Review of code migration procedures   
  
试题**5**： The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:   
A、comply with regulatory requirements.   
B、provide a basis for drawing reasonable conclusions.   
C、ensure complete audit coverage.   
D、perform the audit according to the defined scope.   
  
试题**6**： Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:   
A、change the company's security policy.   
B、educate users about the risk of weak passwords.   
C、build in validations to prevent this during user creation and password change.   
D、require a periodic review of matching user ID and passwords for detection and correction.   
  
试题**7**： Which of the following attacks targets the Secure Sockets Layer (SSL)?   
A、Man-in-the middle B、Dictionary C、Password sniffing D、Phishing   
  
试题**8**： IS审计师在为公司考虑其外包计算机系统业务需要复核并检查每个供应商的业务连续性计划是否合适?（）  
A、是的, 因为IS审计师会评估服务商计划的充分性并且协助他们的公司实施一项补充计划.   
B、是的, 因为基于计划, 系统审计师会评估服务尚的财务状况及其履行合同的能力  
C、不, 因为提供的备份已在合同中充分说明.   
D、不,因为服务商的业务连续性计划是专有信息 .  
  
试题**9**： 从终端发现未授权输入的信息最好是由（）提供  
A.控制台日志输出B.事务处理日志C.自动化的不确定文件清单D.用户错误报告  
  
试题**10**： 下面哪个是在决策支持系统中的实施风险？（）  
A.管理控制B.半结构化的维度C.没办法定义目标和使用模式D.决策过程的变更

**信息安全工程师每日一练试题（2017/3/3）**

试题**1**： 在信息系统安全技术体系中，环境安全只要指中心机房的安全保护。以下不属于该体系环境安全内容的是（ ）。  
A．设备防盗器B．接地和防雷击C．机房控制D．防电磁泄漏

试题**2**： 信息网络的物理安全要从（）两个角度来考虑。  
  A．软件安全和设备安全  C．环境安全和软件安全  B．环境安全和设备安全  D．软件安全和硬件安全

试题**3**： 如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf文件，查看是否包含如下设置，选出一个正确的（）。  
A、audit=filename B、sys=filename C、event=filename D、log=filename  
  
试题**4**： 安全的运行环境是软件安全的基础，操作系统安全配置是确保运行环境安全必不可少的工作，某管理员对即将上线的Windows 操作系统进行了以下四项安全部署工作，其中哪项设置不利于提高运行环境安全?（）  
A．操作系统安装完成后安装最新的安全补丁，确保操作系统不存在可被利用的安全漏洞  
B．为了方便进行数据备份，安装Windows 操作系统时只使用一个分区C，所有数据和操作系统都存放在C 盘  
C．操作系统上部署防病毒软件，以对抗病毒的威胁  
D．将默认的管理员账号Administrator 改名，降低口令暴力破解攻击的发生可能  
  
试题**5**： 信息系统保护轮廓（ISPP）定义了（）  
A、某种类型信息系统的与实现无关的一组系统级安全保障要求  
B、某种类型信息系统的与实现相关的一组系统级安全保障要求  
C、某种类型信息系统的与实现无关的一组系统级安全保障目的  
D、某种类型信息系统的与实现相关的一组系统级安全保障目的  
  
试题**6**： 某单位信息安全岗位员工，利用个人业余时阀，在社交网络平台上向业内同不定期发布信息安全相关知识和前沿动态资讯，这一行为主要符合以下哪一条注册信息安全专业人员（CISP）职业道德准则：（）  
A．避免任何损害CISP声誉形象的行为  
B．自觉维护公众信息安全，拒绝并抵制通过计算机网络系统泄露个人隐私的行为  
C．帮助和指导信息安全同行提升信息安全保障知识和能力  
D．不在公众网络传播反动、暴力、黄色、低俗信息及非法软件  
  
试题**7**： 下列那一条是椭圆曲线加密方法相对于RSA加密方法最大的优势？  
A、计算速度B、支持数字签名的能力C、密钥发布更简单D、给定密钥长度的情况下（保密性）更强  
  
试题**8**： Which of the following is an example of a passive attack initiated through the Internet?   
A、Traffic analysis B、Masquerading C、Denial of service D、E-mail spoofing   
  
试题**9**： 信息系统管理人员告诉信息系统审计师组织最近达到了软件能力成熟度模型（CMM）的最高水平，则最近组织增加的软件质量流程是:（）  
A、持续改进B、量化的质量目标C、文档化流程D、为某一特殊项目定制的流程  
  
试题**10**： 在制訂災難恢復計劃時，決定可接受停機時間的標准是：（）  
A、年度損失期望值B、服務交付目標C、孤兒數據的數據D、最大可容忍損失

**信息安全工程师每日一练试题（2017/3/4）**

试题**1**： 网上营业中间件如果启用了SSl，应采用不低于（）版本的SSL，采用经国家密码管理局认可的密码算法。  
A、2.0 B、2.5 C、3.0 D、3.1  
  
试题**2**： 以下哪些是信息资产无需明确的（）  
A.所有者B.管理者C.厂商D.使用者  
  
试题**3**： 以下哪个选项是缺乏适当的安全控制的表现（）  
A.威胁B.脆弱性C.资产D.影响  
  
试题**4**： 计算机病毒会对下列计算机服务造成威胁，除了：（）  
A.完整性B.有效性C.保密性D.可用性  
  
试题**5**： 智能卡是指粘贴或嵌有集成电路芯片的一种便携式卡片塑胶，智能卡的片内操作系统（COS）是智能卡芯片内的一个监控软件，以下不属于COS组成部分的是（）  
A、通讯管理模块B、数据管理模块C、安全管理模块D、文件管理模块  
试题**6**： After reviewing its business processes, a large organization is deploying a new web application based on a VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?   
A、Fine-grained access control B、Role-based access control (RBAC)   
C、Access control lists D、Network/service access control   
  
试题**7**： Due to changes in IT, the disaster recovery plan of a large organization has been changed. What is the PRIMARY risk if the new plan is not tested?   
A、Catastrophic service interruption   
B、High consumption of resources   
C、Total cost of the recovery may not be minimized   
D、Users and recovery teams may face severe difficulties when activating the plan   
  
试题**8**： Applying a digital signature to data traveling in a network provides:   
A、confidentiality and integrity. B、security and nonrepudiation.   
C、integrity and nonrepudiation. D、confidentiality and nonrepudiation.   
  
试题**9**： 一个程序员恶意地修改了生产程序代码以改变数据，随后又恢复了源代码。下列哪一项是发现这个恶意行为的最有效的：（）  
A、比较源代码B、检查系统日志文件C、比较目标代码D、比较可执行代码和源代码的完整性  
  
试题**10**： 在网络传输中应用数字签名技术可以保证：（）  
A．机密性和完整性B．安全性和不可否认性C．完整性和不可否认性D．机密性和不可否认性

**信息安全工程师每日一练试题（2017/3/5）**

试题**1**： 公安机关负责对互联网上网服务营业场所经营单位的()  
A、设立审批B、信息网络安全的监督管理C、登记注册D、接入网络  
  
试题**2**： 本课程中所讨论的黑客分为：()  
A、6类B、5类C、4类  
  
试题**3**： VPN是指()  
A、虚拟的专用网络B、虚拟的协议网络C、虚拟的包过滤网络  
  
试题**4**： 数字签名是一种认证技术，它保证消息的来源与（）。  
A. 保密性 B. 完整性 C. 可用性 D. 不可重放  
  
试题**5**： "在选择外部供货生产商时，评价标准按照重要性的排列顺序是：（）

1. 供货商与信息系统部门的接近程度 2. 供货商雇员的态度

3. 供货商的信誉、专业知识、技术 4. 供货商的财政状况和管理情况

A.4，3，1，2 B.3，4，2，1 C.3，2，4，1 D.1，2，3，4   
  
试题**6**： 在数据中心使用稳压电源，以保证:（）  
A.ν 硬件免受电源浪涌B.ν 主电源被破坏后的完整性维护

C.主电源失效后可以立即使用D.针对长期电力波动的硬件包含  
  
试题**7**： 以下哪个是恶意代码采用的隐藏技术：（）  
A．文件隐藏B．进程隐藏C．网络连接隐藏D．以上都是  
  
试题**8**： The PRIMARY objective of implementing corporate governance by an organization's management is to:   
A、provide strategic direction. B、control business operations.

C、align IT with business. D、implement best practices.   
  
试题**9**： Which of the following is the MOST robust method for disposing of magnetic media that contains confidential information?   
A、Degaussing B、Defragmenting C、Erasing D、Destroying   
  
试题**10**： 下列哪一项条件可能增加欺骗的可能性？（）  
A、应用程序员对正式程序实施更改B、应用程序员对测试程序实施更改  
C、操作支持人员对补丁计划实施更改D、数据库管理员对数据结构实施更改

**信息安全工程师每日一练试题（2017/3/6）**

试题**1**： 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  
  
试题**2**： 下面哪一项情景符合即时消息服务的功能()  
A、上网浏览网页B、从Internet下载或上传文件C、用ICQ或QQ和朋友聊天D、网上购物  
  
试题**3**： 存储过程是SQL语句的一个集合，在一个名称下存储，按独立单元方式执行。以下哪一项不是使用存储过程的优点：（）  
A．提高性能，应用程序不用重复编译此过程  
B．降低用户查询数量，减轻网络拥塞  
C．语句执行过程中如果中断，可以进行数据回滚，保证数据的完整性和一致性  
D．可以控制用户使用存储过程的权限，以增强数据库的安全性  
  
试题**4**： 以下对PDCA循环特点描述不正确的是：（）  
A、按顺序进行，周而复始，不断循环  
B、组织中的每个部分,甚至个人,均可以PDCA循环,大环套小环,一层一层地解决问题  
C、每通过一次PDCA循环,都要进行总结,提出新目标,再进行第二次PDCA 循环  
D、可以由任何一个阶段开始，周而复始，不断循环  
  
试题**5**： Effective IT governance requires organizational structures and processes to ensure that:   
A、the organization's strategies and objectives extend the IT strategy.   
B、the business strategy is derived from an IT strategy.   
C、IT governance is separate and distinct from the overall governance.   
D、the IT strategy extends the organization's strategies and objectives.   
  
试题**6**： What method might an IS auditor utilize to test wireless security at branch office locations?   
A、War dialing B、Social engineering C、War driving D、Password cracking   
  
试题**7**： An efficient use of public key infrastructure (PKI) should encrypt the:   
A、entire message. B、private key. C、public key. D、symmetric session key.   
  
试题**8**： 决定服务中断事件（安全事件）等级主要标准：（）  
A、恢复成本B、社会负面影响C、地理位置D、停工时间  
  
试题**9**： 当IS审计员履行一个电子资金转账系统审计时，下列哪一项用户情形是其最关心的（）  
A、三个用户有权截获和检验他们自己的消息B、五个用户有权截获和发送他们自己的消息  
C、五个用户有权检验其他用户和发送他们自己的消息  
D、三个用户有权截获和检验其他用户的消息，也有权发送他们自己的消息  
  
试题**10**： 检验一个系统的税务计算准确最佳方法是：（）  
A、计算程序源代码的详细图形化评价和分析B、用通用审计软件再造程序逻辑以计算月度总数  
C、准备模拟事务以处理和比较结果和预决结果D、计算程序源代码的自动化流程图和分析

**信息安全工程师每日一练试题（2017/3/7）**

试题**1**： 某网站向CA申请了数字证书。用户通过 （1） 来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过 （2） 进行加密和验证，该网站通过 （3） 进行解密和签名。  
（1）A、CA的签名 B、证书中的公钥  C、网站的私钥  D、用户的公钥  
（2）A、CA的签名  B、证书中的公钥  C、网站的私钥  D、用户的公钥  
（3）A、CA的签名  B、证书中的公钥  C、网站的私钥  D、用户的公钥  
  
试题**2**： 下列算法中，( )属于摘要算法。  
A、DES  B、MD5  C、Diffie-Hellman  D、AES  
  
试题**3**： 典型的邮件加密的过程一是发送方和接收方交换()  
A、双方私钥B、双方公钥C、双方通讯的对称加密密钥  
  
试题**4**： 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和标准进行  
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**5**： 安全技术评估工具通常不包括（）  
A.漏洞扫描工具B.入侵检测系统C.调查问卷D.渗透测试工具  
  
试题**6**： Which of the following is a technique that could be used to capture network user passwords?   
A、Encryption B、Sniffing C、Spoofing D、Data destruction   
  
试题**7**： Which of the following concerns associated with the World Wide Web would be addressed by a firewall?   
A、Unauthorized access from outside the organization B、Unauthorized access from within the organization   
C、A delay in Internet connectivity D、A delay in downloading using File Transfer Protocol (FTP)   
  
试题**8**： Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?   
A、Virtual private network B、Dedicated line C、Leased line D、Integrated services digital network   
  
试题**9**： In planning an audit, the MOST critical step is the identification of the:   
A、areas of high risk. B、skill sets of the audit staff. C、test steps in the audit. D、time allotted for the audit.   
  
试题**10**： Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:   
A、downtime costs. B、resumption costs. C、recovery costs. D、walkthrough costs.   
**2017/3/1 1~5 D DDBCCBA B C B 6~10 A A B A A**

**11~15 C D D A A 16~20 A D D A A**

**2017/3/2 1~5 C B B C B 6~10 C A A B C**

**2017/3/3 1~5 A C D B B 6~10 C A A A D**

**2017/3/4 1~5 C C B C B 6~10 B A C B C**

**2017/3/5 1~5 B B A B B 6~10A D A D A**

**2017/3/6 1~5 A C B D D 6~10 C D D A C**

**2017/3/7 1~5 ABC B B C C 6~10 B A A A A**