**信息安全工程师每日一练试题（2017/1/9）**

试题**1**： 组织回顾信息系统灾难恢复计划时应：（）  
A.每半年演练一次B.周期性回顾并更新C.经首席执行官(CEO)认可D.与组织的所有部门负责人沟通  
  
试题**2**： 下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（）    
A、对安全违规的发现和验证是进行惩戒的重要前提B、惩戒措施的一个重要意义在于它的威慑性  
C、出于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训  
D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

试题**3**： 我们在日常生活和工作中，为什么需要定期修改电脑、邮箱、网站的各类密码?()  
A、 遵循国家的安全法律B、 降低电脑受损的几率C、 确保不会忘掉密码D、 确保个人数据和隐私安全  
  
试题**4**： 下面哪个口令的安全性最高( )  
A、 integrity1234567890B、 !@7es6RFE,,,d195ds@@SDa  
C、 passW@odassW@odassW@odD、 ichunqiuadmin123456

试题**5**： 以下关于“最小特权”安全管理原则理解正确的是:（）  
A、组织机构内的敏感岗位不能由一个人长期负责B、对重要的工作进行分解，分自己给不同人员完成  
C、一个人有且仅有其执行岗位所足够的许可和权限

D、防止员工由一个岗位变动到另一个岗位，累积越来越多的权限

试题**6**： 下列哪项不是SSECMM中规定的系统安全工程过程类：（）  
A.工程B.组织C.项目D.资产  
  
试题**7**： 下述选项中对于"风险管理"的描述正确的是:（）  
A.安全必须是完美无缺、面面俱到的。B.最完备的信息安全策略就是最优的风险管理对策  
C.在应对信息安全风险时,要从经济、技术、管理的可行性和有效性上做出权衡和取舍.  
D.防范不足就会造成损失:防范过多就可以避免损失。  
试题**8**：    
试题**9**： 以下有关信息安全管理员职责的叙述，不正确的是（）  
A、信息安全管理员应该对网络的总体安全布局进行规划

B、信息安全管理员应该对信息系统安全事件进行处理  
C、信息安全管理员应该负责为用户编写安全应用程序  
D、信息安全管理员应该对安全设备进行优化配置  
  
试题**10**： 数字签名最常见的实现方法是建立在（）的组合基础之上  
A、公钥密码体制和对称密码体制B、对称密码体制和MD5摘要算法  
C、公钥密码体制和单向安全散列函数算法D、公证系统和MD4摘要算法

**信息安全工程师每日一练试题（2017/1/10）**

试题**1**： 常用对称加密算法不包括  （ ）  。  
A、DES  B、RC-5  C、IDEA  D、RSA

试题**2**： 基于网络的入侵检测系统一般不部署在以下位置()。  
A、防火墙内B、防火墙外C、主机上D、防火墙内外都有   
  
试题**3**： 任何组织或个人不得利用互联网电子邮件从事传播淫秽色情信息、窃取他人信息或者等违法犯罪活动，否则构成犯罪的，依法追究刑事责任，尚不构成犯罪的，由公安机关等依照有关法律、行政法规的规定予以处罚；电信业务提供者从事上述活动的，并由电信管理机构依据\_\_\_\_\_有关行政法规处罚。  
A、故意传播计算机病毒  
B、发送商业广告  
C、传播公益信息  
  
试题**4**： 以下哪种技术用来描述异步传输模式（ATM）？()  
A、报文交换；B、信元交换；C、电路交换；D、无连接服务  
  
试题**5**： 公司甲做了很多政府网站安全项目，在为网游公司乙的网站设计安全保障方案时，借鉴以前项目经验，为乙设计了多重数据加密安全措施，但用户提出不需要这些加密措施，理由是影响了网站性能，使用户访问量受限，双方引起争议。下面说法哪个是错误的：  
A.乙对信息安全不重视，低估了黑客能力，不舍得花钱&  
B．甲在需求分析阶段没有进行风险评估，所部署的加密针对性不足，造成浪费  
C．甲未充分考虑网游网站的业务与政府网站业务的区别  
D．乙要综合考虑业务、合规性和风险，与甲共同确定网站安全需求

试题**6**： 来自终端的电磁泄露风险，因为它们:（）  
A.导致噪音污染B.ν 破坏处理程序C.ν 产生危险水平的电流D.ν 可以被捕获并还原  
  
试题**7**： 2DR模型通过传统的静态安全技术和方法提高网络的防护能力，这些技术包括？（）  
A.实时监控技术。B.访问控制技术。C.信息加密技术。D.身份认证技术。  
  
试题**8**： 下面哪一项最好地描述了组织机构的安全策略？ （）  
A、定义了访问控制需求的总体指导方针B、建议了如何符合标准  
C、表明管理者意图的高层陈述D、表明所使用的技术控制措施的高层陈述  
  
试题**9**： 哪一类防火墙具有根据传输信息的内容（如关键字、文件类型）来控制访问连续的能力？（）  
A、包过滤防火墙B、状态监测防火墙C、应用网关防火墙D、以上都不是  
  
试题**10**： 以下对访问控制表和访问访问能力表说法正确的是（）  
A、访问能力表表示每个客体可以被访问的主体及其权限  
B、访问控制表说明了每个主体可以访问的客对于非集中访问控制中“域”说法正确的体现  
C、访问控制表一般随主体一起保存  
D、访问能力表更容易实现访问权相的传递，单回收访问权限较困难

**信息安全工程师每日一练试题（2017/1/11）**

试题**1**： 采用 Kerberos 系统进行认证时，可以在报文中加入 （ ）来防止重放攻击。  
A、会话密钥 B、时间戳 C、用户 ID D、私有密钥  
  
试题**2**： 许多黑客利用软件实现中的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软件 D、安装防病毒软件  
  
试题**3**： ARP攻击造成网络无法跨网段通信的原因是（）。  
A.发送大量ARP报文造成网络拥塞B.伪造网关ARP报文使得数据包无法发送到网关  
C. ARP攻击破坏了网络的物理连通性D. ARP攻击破坏了网关设备

试题**4**： 关于信息安全策略文件以下说法不正确的是哪个？（）  
A.信息安全策略文件应由管理者批准、发布。B.信息安全策略文件并传达给所有员工和外部相关方。  
C.信息安全策略文件必须打印成纸质文件进行分发。  
D.信息安全策略文件应说明管理承诺，并提出组织的管理信息安全的方法。

试题**5**： 正常情况下，应急计划应该至少多久进行一次针对正确性和完整性的检查（）  
A.1年B.2年C.半年D.5年  
  
试题**6**： 黑客造成的主要危害是（）  
A.  破坏系统、窃取信息及伪造信息B. 攻击系统、获取信息及假冒信息  
C.      进入系统、损毁信息及谣传信息D.    进入系统，获取信息及伪造信息

试题**7**： 在Linux操作系统中，为了授权用户具有管理员的某些个性需求的权限所采取的措施是什么？（）  
A.告诉其他用户root密码B.将普通用户加入到管理员组

C.使用visudo命令授权用户的个性需求D.创建单独的虚拟账户  
  
试题**8**： 下列哪项是多级安全策略的必要组成部分？（）  
A.主体、客体的敏感标签和自主访问控制。B.客体敏感标签和强制访问控制。  
C.主体的安全凭证、客体的安全标签和强制访问控制。

D.主体、客体的敏感标签和对其“系统高安全模式”的评价  
  
试题**9**： 下面有关我信息安全管理体制的说法错误的是?（）  
A.目前我国的信息安全保障工作是相关部门各司其职、相互配合、齐抓共管的局面  
B.我国的信息安全保障工作综合利用法律、管理和技术的手段  
C.我国的信息安全管理应坚持及时检测、快速响应、综合治理的方针  
D.我国对于信息安全贵任的原则是谁主管、谁负责；谁经营、谁负责  
  
试题**10**： 关于业务连续性计划（BCP）以下说法最恰当的是：（）  
A.组织为避免所有业务功能因重大事件而中断，减少业务风险而建立的  
B.组织为避免关键业务功能因重大事件而中断，减少业务风险而建立的一个控制过程；  
C.组织为避免所有业务功能因各种事件而中断，减少业务风险而建立的一个控制过程；  
D.组织为避免信息系统功能因各种事件而中断，减少信息系统而建立的一个控制过程。

**信息安全工程师每日一练试题（2017/1/12）**

试题**1**： ( )属于信息安全管理国际标准。  
A、ISO9000-2000 B、SSE-CMM C、ISO17799 D、ISO15408  
  
试题**2**： （）不是对称加密算法的优点。  
A、加/解密速度快B、密钥管理简单C、加密算法复杂、加密强度高D、适宜一对一的信息加密传输过程  
  
试题**3**： 为了保障数据的存储和传输安全，需要对一些重要数据进行加密。由于对称密码算法（1），所以特别适合对大量的数据进行加密。国际数据加密算法IDEA的密钥长度是（2）位。  
（1）A、比非对称密码算法更安全 B、比非对称密码算法密钥长度更长   
C、比非对称密码算法效率更高 D、还能同时用于身份认证  
（2）A、56 B、64 C、128 D、256   
试题**4**： 等级保护四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、强制访问控制C、隐蔽信道分析、可信路径  
  
试题**5**： 文件型病毒可以通过以下途径传播()  
A、文件交换B、邮件C、网络D、系统引导  
  
试题**6**： 在软件保障成熟度模型(Software Assurance Maturity ldode，SAMM)中，规定了软件开发过程中的核心业务功能，下列哪个选项不属于核心业务功能：（）  
A．治理，主要是管理软件开发的过程和活动  
B．构造，主要是在开发项目中确定目标并开发软件的过程与活动  
C．验证，主要是测试和验证软件的过程与活动  
D．购置，主要是购买第三方商业软件或者采用开源组件的相关管理过程与活动部署

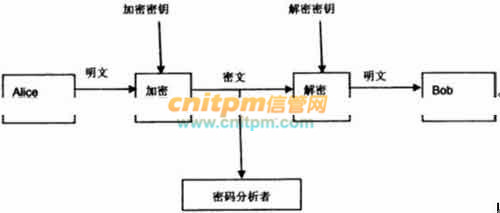
试题**7**： 作为信息安全管理人员，你认为变更管理过程最重要的是？（）  
A.变更过程要留痕B.变更申请与上线提出要经过审批  
C.变更过程要坚持环境分离和人员分离原则D.变更要与容灾预案同步

试题**8**： 下列哪一项体现了适当的职责分离？（）  
A.磁带操作员被允许使用系统控制台。B.操作员是不允许修改系统时间。  
C.允许程序员使用系统控制台。D.控制台操作员被允许装载磁带和磁盘。  
  
试题**9**： Chinese Wall模型的设计宗旨是：（）  
A.用户只能访问那些与已经拥有的信息不冲突的信息B.用户可以访问所有信息  
C.用户可以访问所有已经选择的信息D.用户不可以访问那些没有选择的信息

试题**10**： 在戴明环(PDCA)模型中，处置(ACT)环节的信息安全管理活动是：（）  
A．建立环境B．实施风险处理计划C．持续的监视与评审风险D．持续改进信息安全管理过程

**信息安全工程师每日一练试题（2017/1/13）**

试题**1**： 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  
  
试题**2**： 公司总部与分部之间需要传输大量数据，在保障数据安全的同时又要兼顾密钥算法效率，最合适的加密算法是（）。  
A. RC-5 B. RSA C. ECC D. MD5  
  
试题**3**： 以下关于对称密钥加密说法正确的是：（   ）。  
A．加密密钥和解密密钥必须是相同的B．加密密钥和解密密钥可以是不同的  
C．加密方和解密方可以使用不同的算法        D．密钥的管理非常简单

试题**4**： 针对DNS服务器发起的查询DoS攻击，属于下列哪种攻击类型？()   
A、syn flood      B、ack flood        C、 udpflood        D、Connection flood     
  
试题**5**： 网络监控实施所要考虑的主要内容包括\_\_\_\_\_\_、\_\_\_\_\_\_ 、\_\_\_\_\_\_、工程建设实施、售后服务保障()  
A、明确监控对象、监控技术选择、相关产品确定B、选择监控节点、监控技术选择、选择服务单位  
C、明确监控对象、制订监控计划、测试相关产品  
  
试题**6**： 如下图所示，Alice 用Bob 的密钥加密明文，将密文发送给Bob。Bob 再用自己的私钥解密，恢复出明文。以下说法正确的是：（）  
  
A．此密码体制为对称密码体制B．此密码体制为私钥密码体制  
C．此密码体制为单钥密码体制D．此密码体制为公钥密码体制  
  
试题**7**： 下面那个不是信息安全风险的要素？（）  
A.资产及其价值B.数据安全C.威胁D.控制措施  
  
试题**8**： 为了达到组织灾难恢复的要求，备份时间间隔不能超过（）；  
A、服务水平目标（SLO）B、恢复时间目标(RTO)C、恢复点目标(RPO)D、停用的最大可接受程度(MAO)

试题**9**： 我国规定商用密码产品的研发、制造、销售和使用采取专控管理，必须经过审批，所依据的是：（）    
A、商用密码管理条例B、中华人民共和国计算机信息系统安全保护条例  
C、计算机信息系统国际联网保密管理规定D、中华人民共和国保密法

试题**10**： 某集团公司根据业务需要，在各地分支机构部署前置机，为了保证安全，集团总部要求前置机开放日志共享，由总部服务器采集进行集中分析，在运行过程中发现攻击者也可通过共享从前置机中提取日志，从而导致部分敏感信息泄露，根据降低攻击面的原则，应采取以下哪项处理措施?（）  
A．由于共享导致了安全问题，应直接关闭日志共享，禁止总部提取日志进行分析  
B．为配合总部的安全策略，会带来一定的安全问题，但不影响系统使用，因此接受此风险  
C．日志的存在就是安全风险，最好的办法就是取消日志，通过设置让前置机不记录日志  
D．只允许特定的IP地址从前置机提取日志，对日志共享设置访问密码且限定访问的时间

**信息安全工程师每日一练试题（2017/1/14）**

试题**1**： 下面哪个操作系统提供分布式安全控制机制()  
A、MS-DOS B、Windows 3.1 C、Windows 98 D、Windows NT  
  
试题**2**： IDS的基本流程是信息收集\_\_\_\_\_、\_\_\_\_\_、\_\_\_\_、执行对策()  
A、分析器、模式匹配器、对策生成B、模式匹配器、分析器、对策生成C、对策生成、分析器、模式匹配器  
  
试题**3**： 我国的信息安全行政法律体系有那几部分组成？()  
A、法律B、行政法规和部门规章C、法律、行政法规和部门规章  
  
试题**4**： 下列对于信息安全保障深度防御模型的说法错误的是：（）  
A．信息安全外部环境：信息安全保障是组织机构安全、国家安全的一个重要组成部分，因此对信息安全的讨论必须放在国家政策、法律法规和标准的外部环境制约下。  
B．信息安全管理和工程：信息安全保障需要在整个组织机构内建立和完善信息安全管理体系，将信息安全管理综合至信息系统的整个生命周期，在这个过程中，我们需要采用信息系统工程的方法来建设信息系统。  
C．信息安全人才体系：在组织机构中应建立完善的安全意识，培训体系也是信息安全保障的重要组成部分。  
D．信息安全技术方案：“从外而内、自下而上、形成边界到端的防护能力”。  
试题**5**： 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**6**： 基本的计算机安全需求不包括下列哪一条：（）  
A.安全策略和标识B.绝对的保证和持续的保护C. 身份鉴别和落实责任D. 合理的保证和连续的保护

试题**7**： 矩阵分析法通常是哪种风险评估采用的方法（）  
A.定性风险评估B.定量分析评估C.安全漏洞评估D.安全管理评估  
  
试题**8**： 一些病毒程序如CIH声称能破坏计算机的硬件，使得计算机彻底瘫痪。其原理是　（ ）　。  
A．生成高电压烧坏器件 B．生成大电流烧坏器件C．毁坏ROMBIOS程序 D．毁坏CMOS中的内容  
  
试题**9**： 下述选项中对于"风险管理"的描述不正确的是:（）  
A、风险管理是指导和控制一个组织相关风险的协调活动，它通常包括风险评估、风险处置、风险接受和风险沟通。  
B、风险管理的目的是了解风险并采取措施处置风险并将风险消除。  
C、风险管理是信息安全工作的重要基础，因此信息安全风险管理必须贯穿到信息安全保障工作、信息系统的整个生命周期中。  
D、在网络与信息系统规划设计阶段，应通过信息安全风险评估进一步明确安全需求和安全目标。  
  
试题**10**： 计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效应的确定和提取。以下关于计算机取证的描述中，错误的是（）  
A、计算机取证包括对以磁介质编码信息方式存储的计算机证据的提取和归档  
B、计算机取证围绕电子证据进行，电子证据具有高科技性等特点  
C、计算机取证包括保护目标计算机系统，确定收集和保存电子证据，必须在开计算机的状态下进行  
D、计算机取证是一门在犯罪进行过程中或之后收集证据

**信息安全工程师每日一练试题（2017/1/15）**

试题**1**： 下列行为不属于网络攻击的是 （ ） 。  
A、连续不停Ping某台主机 B、发送带病毒和木马的电子邮件

C、向多个邮箱群发一封电子邮件 D、暴力破解服务器密码  
  
试题**2**： 以网络为本的知识文明人们所关心的主要安全是：()  
A、人身安全B、社会安全C、信息安全  
  
试题**3**： DES是使用最广泛的对称密码，它的密钥长度为（）位。  
A. 64            B. 56            C. 128            D. 1024  
  
试题**4**： 在制定控制前，管理层首先应该保证控制（）  
A.满足控制一个风险问题的要求B.不减少生产力C.基于成本效益的分析D.检测行或改正性的

试题**5**： 下面对WAPI描述不正确的是：（）  
A．安全机制由WAI和WPI两部分组成B．WAI实现对用户身份的鉴别  
C．WPI实现对传输的数据加密D．WAI实现对传输的数据加密  
  
试题**6**： 域名注册信息可在哪里找到？  
A．路由表B．DNS 记录C．whois数据库D．MIBs库  
试题**7**： 为了保护 DNS的区域传送（zonetransfer），你应该配置防火墙以阻止:1.UDP,2. TCP,3.53,4.52（）  
A. 1，3 B. 2，3 C. 1，4 D. 2，4  
试题**8**： 以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（）  
A.制度和措施B.漏洞分析C.意外事故处理计划D.采购计划

试题**9**： 相比FAT文件系统，以下那个不是NTFS所具有的优势？（）  
A、NTFS使用事务日志自动记录所有文件和文件夹更新，当出现系统损坏引起操作失败后，系统能利用日志文件重做或恢复未成功的操作。  
B、NTFS的分区上，可以为每个文件或文件夹设置单独的许可权限  
C、对于大磁盘，NTFS文件系统比FAT有更高的磁盘利用率。  
D、相比FAT文件系统，NTFS文件系统能有效的兼容linux下的EXT32文件格式。  
  
试题**10**： 以下网络攻击中，（）属于被动攻击  
A、拒绝服务攻击B、重放C、假冒D、流量分析

**信息安全工程师每日一练试题（2017/1/16）**

试题**1**： 下图所示为一种数字签名方案，网上传递的报文是  (1)  ，防止A抵赖的证据是  (2)  。  
  
（1）A、P B、DA(P) C、EB(DA(P)) D、DA  
（2）A、P B、DA(P) C、EB(DA(P)) D、DA  
  
试题**2**： 2003年上半年发生的较有影响的计算机及网络病毒是什么（）  
A、SARS B、SQL杀手蠕虫 C、手机病毒 D、小球病毒  
  
试题**3**： 信息安全中PDR模型的关键因素是()  
A、人B、技术C、模型D、客体  
  
试题**4**： 以下哪项是 ISMS文件的作用？（）  
A. 是指导组织有关信息安全工作方面的内部“法规”--使工作有章可循。B.是控制措施（controls）的重要部分  
C.提供客观证据--为满足相关方要求，以及持续改进提供依据D.以上所有

试题**5**： 以下哪项不是信息安全的主要目标（）  
A.确保业务连续性B.保护信息免受各种威胁的损害

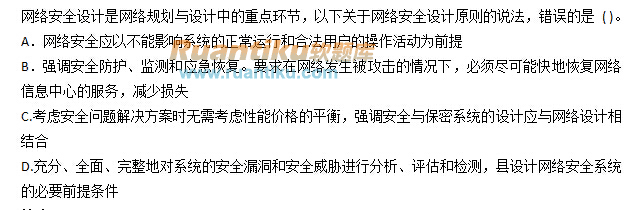
C.防止黑客窃取员工个人信息D.投资回报和商业机遇最大化  
  
试题**6**： 某个客户的网络现在可以正常访问Internet 互联网，共有200台终端PC但此客户从ISP（互联网络服务提供商）里只获得了16个公有的IPv4地址，最多也只有16台PC可以访问互联网，要想让全部200 台终端PC访问Internet互联网最好采取什么方法或技术：（）  
A．花更多的钱向ISP申请更多的IP地址B．在网络的出口路由器上做源NAT  
C．在网络的出口路由器上做目的NATD．在网络的出口处增加一定数量的路由器

试题**7**： 在风险管理准备阶段“建立背景”（对象确立）过程中不应该做的是：（）  
A.分析系统的体系结构B.分析系统的安全环境C.制定风险管理计划D.调查系统的技术特性

试题**8**： 以下哪一项不是IDS 可以解决的问题？（）  
A.弥补网络协议的弱点B.识别和报告对数据文件的改动  
C.统计分析系统中异常活动模式D.提升系统监控能力  
试题**9**： 以下哪一项不是《信息安全事件分级分类指南》中信息安全事件分级需要参考的三个重要因素之一？（）  
A.信息系统的重要程度B.信息系统的用户数量C.事件造成的系统损失D.事件造成的社会影响  
  
试题**10**： SYN Flood攻击是利用（）协议缺陷进行攻击  
A、网络接口层B、互联网络层C、传输层D、应用层

**信息安全工程师每日一练试题（2017/1/17）**

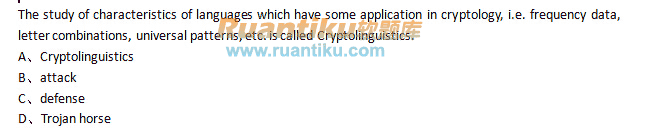
试题**1**： 在采用公开密钥密码体制的数字签名方案中，每个用户有一个私钥，可用它进行(1)；同时每个用户还有一个公钥，可用于(2)．。  
(1)A．解密和验证 B．解密和签名 C．加密和签名 D．加密和验证  
(2)A．解密和验证 B．解密和签名 C．加密和签名 D．加密和验证   
  
试题**2**： IDS发现网络接口收到来自特定IP地址的大量无效的非正常生成的数据包，使服务器过于繁忙以至于不能应答请求，IDS会将本次攻击方式定义为（）  
A、拒绝服务攻击B、地址欺骗攻击C、会话劫持D、信号包探测程序攻击  
  
试题**3**： 路由协议如果没有认证功能，就可以伪造路由信息，导致路由表混乱，从而使网络瘫痪()  
A、对B、错  
  
试题**4**： 一个备份站点包括电线、空调和地板，但不包括计算机和通讯设备，那么它属于（）  
A.冷站 B.温站 C.直线站 D.镜像站点  
  
试题**5**： 文件型病毒传染的对象主要是（）.  
A、 .DOE和.EXE B、 .DBF C、 .WPS D、 .EXE和.DOC  
  
试题**6**： U盘病毒的传播是借助Windows系统的什么功能实现的？  
A.自动播放B.自动补丁更新C.服务自启动D.系统开发漏洞  
  
试题**7**： 当浏览器用户输入：https:/www.example.com/home.html,向服务器方发出访问请求，请问支持这种访问至少要求具备下列哪一个条件。（）  
A、浏览器和web服务器都必须支持SSL/TSL协议B、浏览器单方支持SSL/TSL协议  
C、web服务器单方支持SSL/TSL 协议D、浏览器和web服务器都不必支持SSL 协议  
  
试题**8**： S公司在全国有20个分支机构，总部有10台服务器、200个用户终端，每个分支机构都有一台服务器、100个左右用户终端，通过专网进行互联互通。公司招标的网络设计方案中，四家集成商给出了各自的IP地址规划和分配的方法，作为评标专家，请给S公司选出设计最合理的一个：（）  
A．总部使用服务器、用户终端统一作用10.0.1.X、各分支机构服务器和用户终端使用192.168.2.X~192.168.20.X  
B．总部使用服务器使用10.0.1.1~11、用户终端使用10.0.1.12~212，分支机构IP地址随意确定即可  
C．总部服务器使用10.0.1.X、用户终端根据部门划分使用10.0.2.X、每个分支机构分配两个A类地址段，一个用做服务器地址段、另外一个做用户终端地址段  
D．因为通过互联网连接，访问的是互联网地址，内部地址经NAT映射，因此IP地址无需特别规划，各机构自行决定即可

试题**9**：   
试题**10**： 包过滤技术防火墙在过滤数据包时，一般不关心（）  
A、数据包的源地址B、数据包的协议类型C、数据包的目的地址D、数据包的内容

**信息安全工程师每日一练试题（2017/1/18）**

试题**1**： 网络入侵检测系统和防火墙是两种典型的信息系统安全防御技术，下面关于入侵检测系统和防火墙的说法正确的是（）  
A、防火墙是入侵检测系统之后的又一道防线，防火墙可以及时发现入侵检测系统没有发现的入侵行为  
B、入侵检测系统通常是一个旁路监听设备，没有也不需要跨接在任何链路上，无须网络流量流经它便可以工作  
C、入侵检测系统可以允许内部的一些主机被外部访问，而防火墙没有这些功能，只是监视和分析系统的活动  
D、防火墙必须和安全审计系统联合使用才能达到应用目的，而入侵检测系统是一个独立的系统，不需要依赖防火墙和安全审计系统  
  
试题**2**： 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  
  
试题**3**： 依据（2007）43号《信息安全等级保护管理办法》，我国对信息系统的安全保护等级分为（ ）级  
A、三B、五C、四D、二  
  
试题**4**： 目前的防火墙防范主要是()  
A、主动防范B、被动防范C、不一定  
  
试题**5**： 某单位在实施信息安全风险评估后，形成了若干文挡，下面()中的文挡不应属于风险评估中“风险评估准备”阶段输出的文档。（）  
A．《风险评估工作计划》，主要包括本次风险评估的目的、意义、范围、目标、组织结构、角色及职责、经费预算和进度安排等内容  
B．《风险评估方法和工具列表》。主要包括拟用的风险评估方法和测试评估工具等内容  
C．《已有安全措施列表》，主要包括经检查确认后的已有技术和管理各方面安全措施等内容  
D．《风险评估准则要求》，主要包括风险评估参考标准、采用的风险分析方法、风险计算方法、资产分类标准、资产分类准则等内容  
  
试题**6**： 电子邮件地址上的@是（）的意思  
A、 互联网B、 邮件服务器C、 在……上D、 发送……上  
  
试题**7**： 某公司正在进行信息安全风险评估,在决定信息资产的分类与分级时,谁负有最终责任？（）  
A、部门经理B、高级管理层C、信息资产所有者D、最终用户  
  
试题**8**： 关于PKI/CA证书，下面那一种说法是错误的？（）  
A、证书上具有证书授权中心的数字签名B、证书上列有证书拥有者的基本信息  
C、证书上列有证书拥有者的公开密钥D、证书上列有证书拥有者的秘密密钥

试题**9**： 以下关于信息安全法治建设的意义，说法错误的是：（）  
A．信息安全法律环境是信息安全保障体系中的必要环节  
B．明确违反信息安全的行为，并对该行为进行相应的处罚，以打击信息安全犯罪活动  
C．信息安全主要是技术问题，技术漏洞是信息犯罪的根源  
D．信息安全产业的逐渐形成，需要成熟的技术标准和完善的技术体系

试题**10**： 

**2017/1/9 1~5 B C D B C 6~10 D C A C C**

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

**2017/1/11 1~5 B C B C A 6~10 A C C C B**

**2017/1/12 1~5 C C CC C ABC 6~10 D B B A D**

**2017/1/13 1~5 D A A C A 6~10 D B C A D**

**2017/1/14 1~5 D A C D D 6~10 B A D B C**

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

**2017/1/16 1~5 CB B 无 D C 6~10 B C A B C**

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

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