注册信息安全专业人员考试（补充100题）

1.软件存在漏洞和缺陷是不可避免的,实践中常使用软件缺陷密度(Defectm/KLOC)来衡量软件的安全性,假设某大软件共有296 万行源代码,总共被检测出145 个缺陷,则可以计算出其软件缺陷密度值是()
A.0.00049　　B. 0.049　　C.0.49　　D.49
答案：B

2.GB/T18336《信息技术安全性评估准则》是测评标准类中的重要标准，该标准定义了保护轮期(ProtectionProfile.PP)和安全目标(Security Target.ST)的评估准则，提出了评估保证级(Evaluation Aanurane Level，EAL)，其评估保证级共分为()个递增的评估保证等级。
A.4　B.5　C.6　D7
答案：D

3.Gery McGraw博士及其合作者提出BSI软件安全应由三根支柱来支撑。这三个支柱是
A.源代码审核、风险分析和渗透测试
B.应用风险管理、软件安全接触点和安全知识
C.威胁建模、渗透测试和软件安全接触点
D.威胁建模、源代码审核和模糊测试
答案：B

4 国际标准化组织(Intermtional Organization for Standardization.ISO)对信息安全的定义为() A.保护信息和信息系续不被未经授权的访问、使用、泄露、修改和破坏，为信息和信息系统提供保密性、完整性 可用性、可控性和不可否认性
B. 信息安全，有时编写为 InfoSec，是防止未经授权的访网、使用、被露、中断、修改、检查、记录成破坏信息的做法。它是一个可以用于任何形式数据(例如电子、物理)的通用术语
C.在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力，这些事件和行为将威胁所存储或传输的数据以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和机密性
D.为数据处理系统建立和采取技术、管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而受到破坏、更改、泄露
答案：D

5.对信息安全事件的分级参考下列三个要素:信息系统的重要程度、系统损失和社会影响。依据信息系统的重要程度对信息系统进行划分，不属于正确划分级别的是()。
A.特别重要信息系统　　B.重要信息系统　　C.一般信息系统　　D.关键信息系统
答案：D

6.恢复时间目标(Recovery Time Objective ，RTO)和恢复点目标(Recovery Point Objective，RPO)是业务连续性和灾难恢复工作中的两个重要指标，随着信息系统越来越重要和信息技术越来越先进，这两个指标的数值越来越小。小华准备为其工作的信息系统拟定RTO和RPO指标，则以下描述中。正确的是()。
A.RTO 可以为0，RPO 也可以为0　　B. RTO 可以为0，RPO 不可以为0
C. RTO 不可以为 0，RPO 可以为0　　D.RTO 不可以为0，RPO 也不可以为0
答案：A

7,为了保障系统安全，某单位需要对其跨地区大型网络实时应用系统进行渗透测试，以下关于渗透测试过程的说法不正确的是()。
A.由于在实际渗透测试过程中存在不可预知的风险，所以测试前要提醒用户进行系统和数据备份，以便出现问题时可以及时恢复系统和数据
B.渗透测试从“逆向”的角度出发，测试软件系统的安全性，其价值在于可以测试软件在实际系统中运行时的安全状况
C.渗透测试应当经过方案制定、信息收集、漏洞利用、完成渗透测试报告等步骤
D.为了深入发掘该系统存在的安全威胁，应该在系统正常业务运行高峰期进行渗透测试
答案：D

8.小李在检查公司对外服务网站的源代码时，发现程序在发生诸如没有找到资源、数据库连接错误、写临时文件错误等问题时，会将详细的错误原因在结果页面上显示出来。从安全角度考虑，小李决定修改代码，将详细的错误原因都隐藏起来，在页面上仅仅告知用户“抱歉，发生内部错误!”。请问，这种处理方法的主要目的是()。
A.避免缓冲区溢出　B.安全处理系统异常　C.安全使用临时文件　D.最小化反锁信息
答案：D

9.王工是某单位的系统管理员。他在某次参加了单位组织的风险管理工作时。根据任务安排。他依据已有的资产系表，逐个分析可能危害这些资产的主体、动机、途径等多种因素，分析这些因素出现及造成损失的可能性大乐产为其赋值。请问，他这个工作属于下面要一个阶段的工作()
A.资产识别并赋值 B.脆弱性识别并赋值　C.威胁识别并赋值 D.确认已有的安全措施并赋值
答案：C

10.2016年10月21日，美国东部地区发生大规模断网事件，此次事件是由于美国主要 DNS 服务商 Dyn 遭遇大规模 DDos 攻击所致，影响规模惊人，对人们生产生活造成严重影响。DDoS 攻击的主要目的是破坏系统的()
A.保密性　B.可用性　C.不可否认性　D. 抗抵赖性
答案：B

11.某社交网站的用户点击了该网站上的一个广告。该广告含有一个跨站脚本，会将他的浏览器定向到旅游网文旅游网站则了他的社交网络信息。虽然该用户没有主动访问该旅游网站，但旅游网站已经截获了他的社交网信息(还有他的好友们的信息)，于是犯罪分子便可以躲藏在社交网站的广告后面，截获用户的个人信息宁。这种向 Web 页面插入恶意 html 代码的攻击方式称为()
A.分布式拒绝服务攻击 B,跨站脚本攻击 C. SQL 注入攻击 D.缓冲区溢出攻击
答案：B

12有关能力成熟度模型(CMM)，错误的理解是()。
A.CMM 的思想不关注结果，而是强调了过程的控制，过程如果是高质量的，结果通常会是高质量的
B.CMM 的思想来源于项目管理、质量管理和过程管理
C.CMM 是一种衡量工程实施能力的方法，是一种面向工程过程的方法
D.CMM 是建立在统计过程控制理论基础上的，它基于这样一个假设，即“生产过程的高质量和在过程中组织实施的成熟性可以低成本地生产出高质量产品”
答案：A

13.操作系统用于管理计算机资源，控制整个系统运行，是计算机软件的基础。操作系统安全是计算、网络及信息系统安全的基础。一般操作系统都提供了相应的安全配置接口。小王新买了一台计算机，开机后首先对自带的 Windows 操作系统进行配置。他的主要操作有:(1)关团不必要的服务和端口;(2)在“本地安全策略”中配置账号策略、本地策略、公钥策略和 IP 安全策略;(3)备份敏感文件，禁止建立空连接，下载最新补丁;(4)关闭审核策略，开启口令策略，开启账户策略。这些操作中错误的是()。
A.操作(1)，应该关闭不必要的服务和所有端口
B.操作(2)，在“本地安全策略”中不应该配置公钥策略，而应该配置私钥策略
C.操作(3)，备份敏感文件会导致这些文件遭到窃取的几率增加
D.操作(4)，应该开启审核策略
答案：D

14.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

答案：D

15.北京某公司利用 SSE-CMM 对其自身工程队伍能力进行自我改善，其理解正确的是()。
A.系统安全工程能力成熟度模型(SSE-CMM)定义了 6 个能力级别，当工程队伍不能执行一个过程域中的基本实践时，该过程域的过程能力是 0 级
B.达到 SSE-CM 最高级以后，工程队伍执行同一个过程，每次执行的结果质量必须相同
C.系统安全工程能力成熟度模型(SSE-CMM)定义了 3 个风险过程:评价威胁，评价脆弱性，评价影响
D.SSE-QM 强调系统安全工程与其他工程学科的区别性和独立性
答案：A

16.由于 Internet 的安全问题日益突出，基于 TCP/IP 协议，相关组织和专家在协议的不同层次设计了相应的安全通信协议，用来保障网络各层次的安全。其中，属于或依附于传输层的安全协议是()。
A.PP2P　B.L2TP　C.SSL　D.IPSec
答案：C

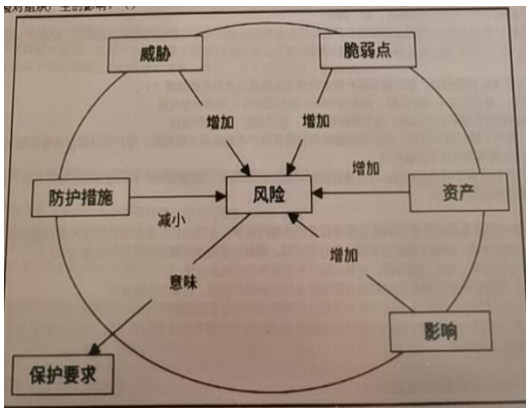
17,以下哪项的行为不属于违反国家保密规定的行为()
A.将涉密计算机、涉密存储设备接入互联网及其他公共信息网络
B.通过普通邮政等无保密措施的渠道传递国家秘密载体
C 在私人交往中涉及国家秘密
D.以不正当手段获取商业秘密
答案：D

18.关于计算机取证描述不正确的是()
A 计算机取证是使用先进的技术和工具，按照标准规程全面地检查计算机系统，以提取和保护有关计算机犯罪的相关证据的活动
B.取证的目的包括:通过证据查找策事者、通过证据推断犯罪过程、通过证据判断受害者损失程度及收集证据提供法律支持
C.电子证据是计算机系统运行过程中产生的各种信息记录及存储的电子化资料及物品。对于电子证据，取证工作主要围绕两方面进行:证据的获取和证据的保护
D.计算机取证的过程可以分为准备、保护、提取、分析和提交 5 个步骤
答案：C

19,在某信息系统的设计中，用户登录过程是这样的:(1)用户通过 HTTP 协议访问信息系统:(2)用户在登录页面输入用户名和口令:(3)信息系统在服务器端检查用户名和密码的正确性，如果正确，则鉴别完成。可以出，这个鉴别过程属于()。
A. 单向鉴别　B.双向鉴别　C.三向鉴别　D.第三方鉴别
答案：A

20.以下关于检查评估和自评估说法错误的是()。
A.信息安全风险评估分自评估、检查评估两形式。应以检查评估为主，自评估和检查评估相互结合、互为补充
B.检查评估可以依据相关标准的要求，实施完整的风险评估，也可以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.信息安全风险评估应贯穿于网络和信息系统建设运行的全过程
D.自评估只能由组织自身发起并实施，对信息系统及其管理进行风险评估活动
答案：A

21.风险，在 GB/T 22081 中定义为事态的概率及其结果的组合。风险的目标可能有很多不同的方面，如财务目标、健康和人身安全目标、信息安全目标和环境目标等;目标也可能有不同的级别，如战略目标、组织目标、项目目标、产品目标和过程目标等。ISO/IBC13335-1 中揭示了风险各要素关系模型，如图所示。请结合此图，怎么才能降低风险对组织产生的影响?()



A. 组织应该根据风险建立响应的保护要求，通过构架防护措施降低风险对组织产生的影响
B. 加强防护措施，降低风险
C. 减少威胁和脆弱点，降低风险
D. 减少资产降低风险
答案：A

22 小张新购入了一台安装了 Windows 操作系统的笔记本电脑。为了提升操作系统的安全性，小张在 Windowa 系统中的-本地安全策略中，配置了四类安全策略，账号策略、本地策略、公份策略和 IP 安全策略。那么该操作于操作系统安全配置内容中的()。
A. 关闭不必要的服务 B.关闭不必要的端口 C.制定安全策略 D 查看日志记录
答案：C

23.有关系统安全工程-能力成熟度模型(SSE-CM)，错误的理解是()
A.SSE-CMM 要求实施组织与其他组织相互作用，如开发方、产品供应商、集成商和咨询服务商等
B.SSE-CMM 可以使安全工程成为一个确定的、成熟的和可度量的科目。
C.基于 SSE-CMM 的工程是独立工程，与软件工程、硬件工程、通信工程等分别规划实施
D.SSE-CMM 覆盖整个组织的活动，包括管理、组织和工程活动等，而不仅仅是系统安全的工程活动
答案：C

24.关于 Wi-Fi 联盟提出的安全协议 WPA 和 WPA2 的区别，下面描述正确的是()。
A.WPA 是有线局域安全协议，而 WPA2 是无线局域网协议
B. WPA 是适用于中国的无线局域安全协议，而 WPA2 是适用于全世界的无线局域网协议 C. WPA 没有使用密码算法对接入进行认证，而 WPA2 使用了密码算法对接入进行认证
D.WPA 是依照 802. 11i 标准草案制定的，而 WPA2 是依照 802. 11i 正式标准制定的
答案：D

25.二十世纪二十年代，德国发明家亚瑟谢尔比乌斯(arthur Scherbius)发明了 Enigma 密码机，按照密码学发展历史阶段划分，这个阶段属于()。
A.古典密码阶段。这一阶段的密码专家常常靠直觉和技巧来设计密码，而不是凭借推理和证明，常用的密码运算方法包括替代方法和置换方法
B 近代密码发展阶段。这一阶段开始使用机械代替手工计算，形成了机械式密码设备和更进一步的机电密码设备
C.现代密码学的早期发展阶段。这一阶段以香农的论文“保密系统的通信理论”(“The Communication Theory of Secret Systems”)为理论基础，开始了对密码学的科学探索
D.现代密码学的近期发展阶段。这一阶段以公钥密码思想为标志，引发了密码学历史上的革命性的变革，同时，众多的密码算法开始应用于非机密单位和商业场合
答案：B

26.以下关于项目的含义，理解错误的是()。
A.项目是为达到特定的目的、使用一定资源、在确定的期间内、为特定发起人而提供独特的产品、服务或成果而进行的一次性努力
B.项目有明确的开始日期，结束日期由项目的领导者根据项目进度来随机确定

C.项目资源指完成项目所需要的人、财、物等
D.项目目标要遵守 SMART 原则，即项目的目标要求具体(Specific)、可测量(Measurable)、需相关方的一致同意(Agree to)、现实(Realistic)、有一定的时限(Time-oriented)
答案：B

27. 以下关于 Web 传输协议、服务端和客户端软件的安全问题说法不正确的是()。
A. HTTP 协议主要存在明文传输数据、弱验证和缺乏状态跟踪等方面的安全问题
B.HTTP 协议缺乏有效的安全机制，易导致拒绝服务、电子欺骗、嗅探等攻击
C.Cookie 是为了辨别用户身份，进行会话跟踪而存储在用户本地终端上的数据，用户可以随意查看存储在 Cookie 中的数据，但其中的内容不能被修改
D. 针对 HTP 协议存在的安全问题，使用 HTTPS 具有较高的安全性，可以通过证书来验证服务器的身份，并为浏览器和服务器之间的通信加密
答案：C

28.小李在某单位是负责信息安全风险管理方面工作的部门领导,主要负责对所在行业的新人进行基本业务素质培训.一次培训的时候,小李主要负责讲解风险评估方法.请问小李的所述论点中错误的是哪项()
A.风险评估方法包括:定性风险分析、定量风险分析以及半定量风险分析
B.定性风险分析需要凭借分析者的经验和直觉或者业界的标准和惯例，因此具有随意性
C.定量风险分析试图在计算风险评估与成本效益分析期间收集的各个组成部分的具体数字值，因此更具客观性
D.半定量风险分析技术主要指在风险分析过程中综合使用定性和定量风险分析技术对风险要素的赋值方式，实现对风险各要素的度量数值化
答案：B

29.以下关于网络安全设备说法正确的是()。
A.防火墙既能实现内外网物理隔离，又能实现内外网逻辑隔离
B.安全隔离与信息交换系统也称为网闸,需要信息交换时,同一时间可以和两个不同安全级别的网络连接
C.入侵检测系统的主要作用是发现并报告系统中未授权或违反安全策略的行为
D.虚拟专用网是在公共网络中。利用隧道技术，建立一个永久、安全的通信网络
答案：C

30.若一个组织声称自己的 ISMS 符合 ISO/IEC 27001 或 GB/T22080 标准要求，其信息安全控制措施通常需要在资产管理方面实施常规控制，资产管理包含对资产负责和信息分类两个控制目标。信息分类控制的目标是为了确保信息受到适当级别的保护，通常采取以下哪项控制措施()
A.资产清单　　B.资产责任人　C 资产的可接受使用　　D,分类指南、信息的标记和处理
答案：D

31.具有行政法律责任强制力的安全管理规定和安全制度包括()
(1)安全事件全故)制度 2)安全等级保护制度(3)信息系统安全监控(4)安全专用产品销 许可证制度
A.1，2，4　B.2，3　C.2，3，4　　D.1，2，3
答案：A

32.老王是一名企业信息化负责人，由于企业员工在浏览网页时总导致病毒感染系统，为了解决这一问题，老王求信息安全员给出解决措施，信息安全员给出了四条措施建议，老王根据多年的信息安全管理经验，认为其中不太适合推广，你认为是哪条措施()
A.采购防病毒网关并部署在企业互联网出口中,实现对所有浏览网页进行检测,阻止网页中的病毒进入内网
B.采购并统一部署企业防病毒软件，信息化管理部门统一进行病毒库升级，确保每台计算机都具备有效的病毒检测和查杀能力
C.制定制度禁止使用微软的 IE 浏览器上网，统一要求使用 Chrome 浏览器
D.组织对员工进行一次上网行为安全培训，提高企业员工在互联网浏览时的安全意识

答案：C

33.关于信息安全管理体系(Information Security Management Systems,ISMS)，下面描述错误的是()。
A.信息安全管理体系是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系，包括组织架构、方针、活动、职责及相关实践要素
B.管理体系(Management Systems)是为达到组织目标的策略、程序、指南和相关资源的框架，信息安全管理体系是管理体系思想和方法在信息安全领域的应用
C.概念上，信息安全管理体系有广义和狭义之分，狭义的信息安全管理体系是指按照 ISO27001 标准定义的管理体系，它是一个组织整体管理体系的组成部分
D.同其他管理体系一样，信息安全管理体系也要建立信息安全管理组织机构、健全信息安全管理制度、构建信息安全技术防护体系和加强人员的安全意识等内容
答案：D

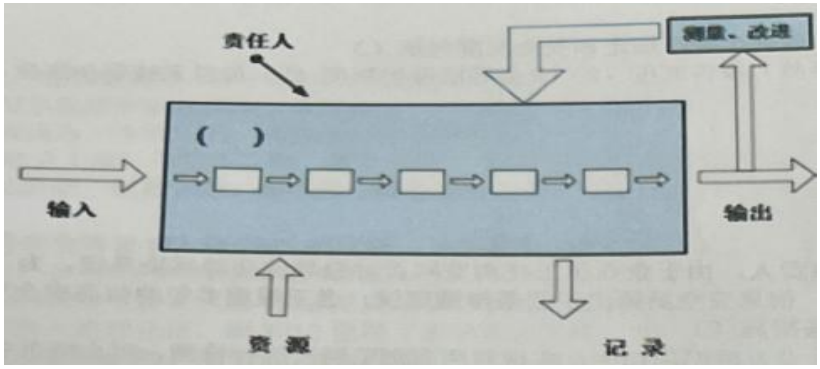
34.Kerberos 协议是一种集中访问控制协议,它能在复杂的网络环境中,为用户提供安全的单点登录服务。单点登录是指用户在网络中进行一次身份认证,便可以访问其授权的所有网络资源，而不再需要其他的身份认证过程,实质是消息 M 在多个应用系统之间的传递或共享.其中消息 M 是指以下选项中的()。
A.安全凭证　　B.用户名　　C. 加密密钥　　D.会话密钥
答案：A

35.下列我国哪一个政策性文件明确了我国信息安全保障工作的方针和总体要求以及加强信息安全保障工作的主要原则()
A.《关于加强政府信息系统安全和保密管理工作的通知》
B.《中华人民共和国计算机信息系统安全保护条例》
C.《国家信息化领导小组关于加强信息安全保障工作的意见》
D.《关于开展信息安全风险评估工作的意见》
答案：C

36.以下关于威胁建模流程步骤说法不正确的是()。
A.威胁建模主要流程包括四步:确定建模对象、识别威胁、评估威胁和消减威胁
B.评估威胁是对威胁进行分析,评估被利用和攻击发生的概率,了解被攻击后资产的受损后果,并计算风险
C.消减威胁是根据威胁的评估结果，确定是否要消除该威胁以及消减的技术措施，可以通过重新设计直接消除威胁，或设计采用技术手段来消减威胁
D.识别威胁是发现组件或进程存在的威胁,它可能是恶意的,也可能不是恶意的,威胁就是漏洞
答案：D

37.某商贸公司信息安全管理员考虑到信息系统对业务影响越来越重要，计划编制本单位信息安全应急响应预案在向主管领导写报告时，他列举了编制信息安全应急响应预案的好处和重要性，在他罗列的四条理由中，其中不适合为理由的一条是（）
A.应急预案是明确关键业务系统信息安全应急响应相挥体系和工作机制的重要方式
B.应预案是提高应对网络和信息系统突发事件能力,减少突发事件造成的损失和危害,保障信息系统运行平稳、安全、有序、高效的手段
C.编制应急预案是国家网络安全法对所有单位的强制要求，因此必须建设
D.应急预案是保障单位业务系统信息安全的重要措施
答案：C

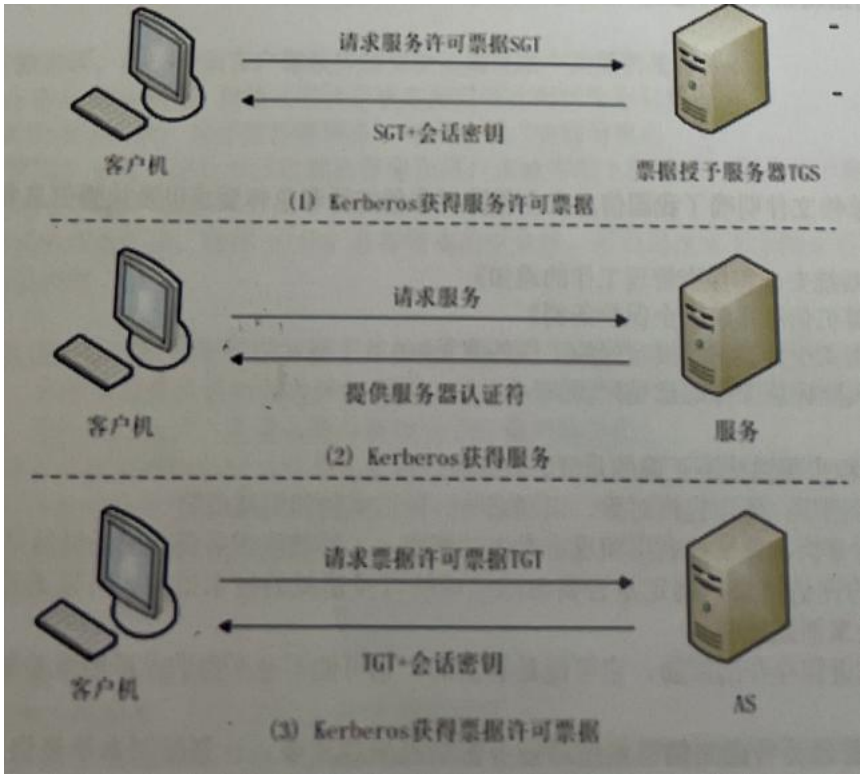
38.ISO0001-2000 标准鼓励在制定.实施质量管理体系以及改进其有效性时采用过程方法,通过满足顾客要求,地进顾客满意度.下图是关于过程方法的示意图，图中括号空白处应填写()。
A.策略 B.管理者 C.组织 D.活动



答案：D

39.在某次信息安全应急响应过程中，小王正在实施如下措施:消除或阻断攻击源、找到并消除系统的脆弱性/漏洞、修改安全策略、加强防范措施、格式化被感染恶意程序的介质等。请问，按照 PDCERF 应急响应方法，这些工作应处于以下哪个阶段)
A.准备阶段 B.检测阶段 C. 遏制阶段 D.根除阶段
答案：D

40. Kerberos 协议是常用的集中访问控制协议，通过可信第三方的认证服务，减轻应用服务器的负担。Kerberos 的运行环境由密钥分发中心(KDC)、应用服务器和客户端三个部分组成。其中，KDC 分为认证服务器 AS 和票据授权服务器 TGS 两部分。下图展示了 Kerberos 协议的三个阶段，分别为(1)Kerberos 获得服务许可票据，(2) Kerberos 获得服务，(3)Kerberos 获得票据许可票据。下列选项中，对这三个阶段的排序正确的是()。



A.(1)－(2)－(3) B.(3)－(2)－(1) C. (2)－(1)－(3) D.(3)－(1)－(2)
答案：D

41.关于对信息安全事件进行分类分级管理的原因描述不正确的是().
A.信息安全事件的种类很多，产重程度也不尽相同，其响应和处理方式也应各不相同
B.对信息安全事件进行分类和分级管理，是有效防范和响应信息安全事件的基础
C.能够使事前准备、事中应对和事后处理的各项相关工作更具针对性和有效性
D.我国早期的计算机安全事件的应急响应工作主要包括计算机病毒防范和“千年虫”问题的解决，关于网络安全应急响应的起步最早

答案：D

42.某集团公司信息安全管理员根据领导安排制定了下一年度的培训工作计划，提出了四大培训任务和目标，关于这四个培训任务和目标，作为主管领导，以下选项中不合理的是()
A.由于网络安全上升到国家安全的高度，网络安全必须得到足够的重视。因此安排了对集团公司下属单位的总经理(一把手)的网络安全法培训
B.对下级单位的网络安全管理岗人员实施全面安全培训，建议通过 CISP 培训以确保人员能力得到保障
C.对其他信息化相关人员(网络管理员、软件开发人员)也进行安全基础培训，使相关人员对网络安全有所了解
D.对全体员工安排信息安全意识及基础安全知识培训，实现全员信息安全意识教育
答案：C

43.金女士经常通过计算机在互联网上购物，从安全角度看，下面哪项是不好的操作习惯()
A.使用专用上网购物用计算机，安装好软件后不要对该计算机上的系统软件、应用软件进行升级
B.为计算机安装具有良好声誉的安全防护软件，包括病毒查杀、安全检查和安全加固方面的软件
C.在 IE 的配置中，设置只能下载和安装经过签名的、安全的 ActiveX 控件
D.在使用网络浏览器时，设置不在计算机中保留网络历史记录和表单数据
答案：A

44.在国家标准 GB/T 20274.1-2006《信息安全技术信息系统安全保障评估框架第一部分:简介和一般模型》中，信息系统安全保障模型包含哪几个方面?()
A.保障要素、生命周期和运行维护　　B.保障要素、生命周期和安全特征
C.规划组织、生命周期和安全特征　　D.规划组织、生命周期和运行维护
答案：B

45.某信息安全公司的团队对某款名为“红包快抢”的外挂进行分析，发现此外挂是一个典型的木马后门，使黑客能够获得受害者电脑的访问权。该后门程序为了达到长期驻留在受害者的计算机中，通过修改注册表启动项来达到后门程序随受害者计算机系统启动而启动。为防范此类木马后门的攻击，以下做法无用的是()。
A.不下载、不执行、不接收来历不明的软件或文件
B.修改用户名和口令
C.不随意打开来历不明的邮件，不浏览不健康不正规的网站
D.安装反病毒软件和防火墙，安装专门的木马防治软件
答案：B

46.若一个组织声称自己的 ISMS 符合 ISO/IEC27001 或 GB/T22080 标准要求,其信息安全控制措施通常需要在物理和环境安全方面实施常规控制。物理和环境安全领域包括安全区域和设备安全两个控制目标。安全区域的控制目标是防止对组织场所和信息的未授权物理访问、损坏和干扰，关键或敏感的信息及信息处理设施应放在安全区域内,并受到相应保护,该目标可以通过以下控制措施来实现,不包括哪一项()
A.物理安全边界、物理入口控制
B.办公室、房间和设施的安全保护，外部和环境威胁的安全防护
C.通信安全、合规性
D.在安全区域工作，公共访问、交接区安全
答案：C

47.常见的访问控制模型包括自主访问控制模型、强制访问控制模型和基于角色的访问控制模型等。下面描述中错误的是()。
A.从安全性等级来看，这三个模型安全性从低到高的排序是自主访问控制模型、强制访问控制模型和基于角色的访问控制模型
B.自主访问控制是一种广泛应用的方法，资源的所有者(往往也是创建者)可以规定谁有权访问它们的资源，具有较好的易用性和可扩展性
C.强制访问控制模型要求主体和客体都有一个固定的安全属性，系统用该安全属性来决定一个主体是否可以访问某个客体。该模型具有一定的抗恶意程序攻击能力，适用于专用或安全性要求较高的系统

D.基于角色的访问控制模型的基本思想是根据用户所担任的角色来决定用户在系统中的访问权限，该模型便于实施授权管理和安全约束，容易实现最小特权、职责分离等各种安全策略
答案：A

48.PDC 循环又叫戴明环，是管理学常用的一种模型。关于 PDCA 四个字母，下面理解错误的是（）。
A.P 是 Prepare，指准备，包括明确对象、方法，制定活动规划
B.D 是 Do，指实施、月体运作，实现计划中的内容
C.c 是 Check，指检查、总结执行计划的结果，明确效果，找出问题
D.A 是 Act 或 Adjut.指改进、完善和处理,对总结检查的结果进行处理。对成功的经验加以肯定,并予以标准化,总结失败的教训并加以重视,对没有解决的问题，应该交给下一个 PDCA 环解决
答案：A

49.小华在某电子商务公司工作。某天他在查看信息系统设计文档时，发现其中标注该信息系统的 RPO(恢复点目标)指标为 3 小时，请同这意味着()。
A.该信息系统发生重大信息安全事件后，工作人员应在 3 小时内到位，完成问题定位和应急处理工作
B.该信息系统发生重大信息安全事件后，工作人员应在 3 小时内完成应急处理工作，并恢复对外运行
C.若该信总系统发生重大信息安全事件，工作人员在完成处置和灾难恢复工作后，系统至多能丢失 3 小时的业务类
D.若该信息系统发生重大信息安全事件，工作人员在完成处置和灾难恢复工作后，系统运行 3 小时后能恢复全部数
答案：C

50.随机进程名称是恶意代码迷惑管理员和系统安全检查人员的技术手段之一，以下对于随机进程名技术。描述正确的是()。
A.随机进程名技术虽然每次进程名都是随机的，但是只要找到了进程名称，就找到了恶意代码程序本身
B. 恶意代码生成随机进程名称的目的是使进程名称不固定，因为杀毒软件是按进程名称进行病毒进程查杀，
C. 恶意代码使用随机进程名是通过生成特定格式的进程名称，使进程管理器中看不到恶意代码的进程
D 随机进程名技术每次启动时随机生成恶意代码进程名称，通过不确定的进程名称使自己不容易被发现真实的恶意代码程序名称。
答案：D

51.小王在学为定最风险评站方法后，快定试着为单位机房计算火灾的风险大小、假设单位机房的总价值为 400 万元人民币、桑露系数(Exposure Factor,6F)是 25%，年度发生率(Annualined Rate of Oecurrence, ARO)为 0.2、那么小王计算的年度预期损失(Annualined Loss xpectancy， ALE)应该是()、
A.100 万元人民币 B.400 万元人民币 C.20 万元人民币 D.180 万元人民币
答案：C

52.应急响应是信息安全事件管理的重要内容、基于应急响应工作的特点和事件的不规则性，事先制定出事件应急响应方法和过程，有助于一个组织在事件发生时院止混乱的发生成是在混配状态中迅速恢复控制，将损失和负面影响降到最低，应急响应方法和过程并不是唯一的，一种被广为按受的应急响应方法是将应急响应管理过程分为 6 个阶段，为准备>检测>送制>根除>>快复>跟踪总结，请问下列说法有关于信息安全应急响应管理过程错误的是
A.确定重要资产和风险，实施针对风险的防护措施是信息安全应想响应规划过程中最关健的步理
B.在检测阶段，首先要进行监测、报告及信息收集
C.遏制措施可能会因为事件的类别和级别不同而完全不同。常见的遏制措施有:完全关闭所有系统、拔掉网线等
D.应按照应急响应计划中事先制定的业务恢复优先顺序和恢复步骤，顺次恢复相关的系统
答案：C

53.某购物网站开发项目经过需求分析进入系统设计阶段，为了保证用户帐户的安全，项目开发人员决定用户登录时除了用户名口令认证方式外，还加入基于数字证书的身份认证功能，同时用户口令使用

SHA-1 算法加密后存放在后台数据库中，请问以上安全设计遵循的是哪项安全设计原则()
A.最小特权原则 B.职责分离原则织 C.深防御原则 D.最少共享机制原则
答案：C

54.在信息安全险管理过程中，背景建立是实施工作的第一步、下面哪项理解是错误的().
A.背景建立的依据是国家、地区或行业的相关政策、法律、法规和标准，以及机构的使命、信息系统的业务目标和特性
B.背景建立阶段应识别需要保护的资产、面临的威胁以及存在的脆弱性，并分别赋值，同时确认已有的安全措施，形成需要保护的资产清单
C.背景建立阶段应调查信息系统的业务目标、业务特性、管理特性和技术特性，形成信息系统的描述报告求报告
D.背景建立阶段应分析信息系统的体系结构和关健要索，分析信息系统的安全环境和要求，形成信息系统的安全要
答案：B

55.超文本传输协议(HyperText Transfer Protocol，HTTP)是互联网上广泛使用的一种网络协议。下面哪种协议基于 HTIP 并结合 SSL 协议，具各用户鉴别和通信数据加密等功能()、
A.HTTP 1.0 协议 B.HTTP 1.1 协议 C.HTTPS 协议 D. HTTPD 协议
答案：C

56.“统一威胁管理”是将防病毒、入侵检测和防火墙等安全需求统一管理，目前市场上已经出现了多种此类安全设备，这里“统一威胁管理”常常被简称为()。
A.UTM B.FW C. IDS D.SOC
答案：A

57.以下关于 Windows 操作系统身份标识与签别，说法不正确的是().
A.本地安全授权机构(LSA)生成用户账户在该系统内唯一的安全标识符(SID)
B.用户对鉴别信息的操作，如更改密码等都通过一个以 Administrator 权限运行的服务“Security Account Manager”来实现
C.Windows 操作系统远程登录经历了 SMB 签别机制、LM 签别机制、NTLM 鉴别机制、Kerberos 签别体系等阶段
D.完整的安全标识符(SID)包括用户和组的安全描述，48 比特的身份特权、修订版本和可变的验证值
答案：B

58.王工是某单位的系统管理员，他在某次参加了单位组织的风险管理工作时，发现当前案例中共有两个重要资产:资产 A1 和资产 2:其中资产 A1 面临两个主要威胁:威胁 T1 和威胁 T2;而资产 A2 面临一个主要胁:威胁 T3:威胁 T1 可以利用的资产 A1 存在的两个脆弱性:脆弱性 V1 和脆弱性 V2:威胁 T2 可以利用的资产 A1 存在的三个脆弱性,脆弱性 V3、脆弱性 V4 和脆弱性 V5:威胁 T3 可以利用的资产 A2 存在的两个脆性:脆弱性 V6 和脆弱性 V7. 根据上述条件，请问:使用相乘法时，应该为资产 A1 计算几个风险值()
A.2 B.3 C.5 D.6
答案：C
59.以下有关系统工程说法错误的是()。
A.系统工程不属于基本理论，也不属于技术基础，它研究的重点是方法论
B.系统工程的目的是实现总体效果最优化，即从复杂问题的总体入手，认为总体大于各部分之和，各部分虽然存在不足，但总体可以优化
C.系统工程只需使用定量分析的方法，通过建立实际对象的数学模型，应用合适的优化算法对模型求解，解决实际问题
D.霍尔三维结构将系统工程整个活动过程分为前后紧密衔接的 7 个阶段和 7 个步骤
答案：C

60.某单位根据业务需要准备立项开发一个业务软件，对于软件开发安全投入经费研讨时开发部门和信息中心就发生了分歧，开发部门认为开发阶段无需投入，软件开发完成后发现问题后再针对性的解决，

比前期安全投入要成本更低;信息中心则认为应在软件安全开发阶段投入，后期解决代价太大，双方争执不下，作为信息安全专家，请选择对软件开发安全投入的准确说法()
A.双方的说法都正确,需要根据具体情况分析是开发阶段投入解决问题还是在上线后再解决问题费用更低
B.双方的说法都错误，软件安全问题在任何时候投入解决都可以，只要是一样的问题，解决的代价相同
C.信息中心的考虑是正确的，在软件开发需求分析阶段开始考虑安全问题，总体经费投入比软件运行后的费用要低
D.软件开发部门的说法是正确的，因为软件出现安全问题后更清楚问题所在，安排人员进行代码修订更简单，因此费用更低
答案:C

61.某单位门户网站开发完成后，测试人员使用模糊测试进行安全性测试，以下关于模糊测试过程的说法正确的是()
A.模拟正常用户输入行为，生成大量数据包作为测试用例
B.数据处理点、数据通道的入口点和可信边界点往往不是测试对象
C.监测和记录输入数据后程序正常运行的情况
D 深入分析网站测试过程中产生崩溃或异常的原因，必要时需要测试人员手工重现并分析
答案：D

62.我国等级保护政策发展的正确顺序是()。
1 等级保护相关政策文件颁布
2 计算机系统安全保护等级划分思想提出
3 等级保护相关标准发布
4 网络安全法将等级保护制度作为基本国策
5 等级保护工作试点
A.12345　　B.23154　　C 25134　　D.12435
答案：C

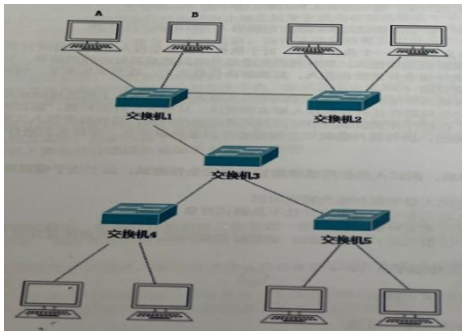
63.<国家信息化领等小组关于加强信息安全保障工作的意见》中办发[2003127 号明的了我国信息安全保障工作的()、加强信息安全保障工作的()、需要重点加强的信息安全保障工作。27 号文的重大意义是,它标志着我医信息安全保障工作有了、我国最近十余年的信息安全保障工作都是围绕此政策性文件来()的、促进了我国()的各项工作。
A.方针;主要原则，总体纲领;展开和推进:信息安全保障建设总体要求:
B.总体要求:主要原则;展开;信息安全保障建设
C.方针和总体要求:主要原则;总体纲领:展开和推进;信息安全保障建设
D.总体要求:主要原则;总体纲领;展开;信息安全保建设
答案：C

64.Linux 系统的安全设置主要从磁盘分区、账户安全设置、禁用危险服务、远程登录安全、用户鉴别安全、审计策略、保护 root 账户、使用网络防火墙和文件权限操作共 10 个方面来完成。小张在学习了 Linux 系统安全的相关知识后，分试为自己计算机上的 Linux 系统进行安全配置。下列选项是他的部分操作，其中不合理的是()。
A.编辑文件/etc/passwd，检查文件中用户 1D，禁用所有用户 ID=0 的用户
B.编辑文件/etc/ssh/sshd_config，将 PermitRootLogin 设置为 no
C.编辑文件/ete/pam.d/systemauth，设置 auth required pam_tally.so onerrufail deny 6 unlock_time-300
D.编辑文件/etc /profile，设置 TMOUT-600
答案：A

65.某单位在一次信息安全风险管理活动中，风险评估报告提出服务器的 FIP 服务存在高风险漏洞。随后该单位在风险处理时选择了安装 FTP 服务洞补丁程序并加固 FTP 服务安全措施，请问该措施属于哪种风险处理方式
A.风险降低　　B. 风险规避　　C.风险转移　　D.风险接受

答案：A

66.某银行有5台交换机连接了大量交易机构的网络(如图所示)，在基于以太网的通信中，计算机A需要与计算机B通信，A必须先广播“ARP 请求信息”，获取计算机B的物理地址。每到月底时用户发现该银行网络服务速度极其缓慢、银行经调查后发现为了当其中一台交换机收到ARP 请求后，会转发给接收端口以外的其他所有端口,ARP 请求会被转发到网络中的所有客户机上.为降低网络的带宽消耗,将广播流限制在固定区域内,可以采用的技术是()



A.配置虚拟专用网络　B.动态分配地址　C.为路由交换设备修改默认口令　D.LAN 划分
答案：D

67 关于ARP欺骗原理和防范措施,下面理解错误的是().
A.ARP欺骗是指攻击者直接向受害者主机发送错误的 ARP 应答报文,使得受害者主机将错误的硬件地址映射关系有入到ARP 缓存中,从而起到冒充主机的目的
B.单纯利用ARP欺骗攻击时,ARP欺骗通常影响的是内部子网，不能跨越路由实施攻击
C,解决ARP欺骗的一个有效方法是采用“静态”的ARP缓存,如果发生硬件地址的更改,则需要人工更新缓存
D.彻底解决ARP欺骗的方法是避免使用ARP协议和ARP缓存，直接采用IP地址和其他主机进行连接
答案：D

68.由于频繁出现软件运行时被照客远程攻击获取数据的现象，某软件公司准备加强软件安全开发管理，在下面做法中，对于解决问题没有直接帮助的是()。
A.要求所有的开发人员参加软件安全意识培调
B.要求规范软件编码，并制定公司的安全编码准则
C.要求增加软件安全测试环节，尽早发现软件安全问题
D.要求用windows10系统做开发
答案：D

69.下列关于软件安全开发中的 BSI(Baild Security In)系列模型说法错误的是 0
A.BSI 含义是指将安全内建到软件开发过程中，而不是可有可无，更不是游离于软件开发生命周期之外
B.软件安全的三根支柱是风险管理、软件安全触点和安全知识
C.软件安全触点是软件开发生命周期中一套轻量缓最优工程化方法，它提供了从不同角度保障安全的行为方式
D.BSI 系列模型强调安全测试的重要性，要求安全测试贯穿整个开发过程及软件生命周期
答案：D

70.关于信息安全应急响应管理过程措述不正确的是()。
A.基于应急响应工作的特点和事件的不规则性，事先制定出事件应急响应方法和过程，有助于一个组织在事件发生时阻止混乱的发生或是在混乱状态中迅速恢复控制，将损失和负面影响降至最低
B.应急响应方法和过程并不是唯一的
C.一种被广为接受的应念响应方法是将应急响应管理过程分为准备、检测、遏制、根除、恢复和跟踪总结 6 个阶段
D.一种被广为接受的应急响应方法是将应急响应管理过程分为准备、检测、遏制、根除、恢复和跟踪总结6个阶段，这6个阶段的响应方法一定能确保事件处理的成功
答案：D

71.按照我国信息安全等级保护的有关政策和标准，有些信息系统只需要自主定级、自主保护，按照要求向公安机关备案即可，可以不需要上级或主管部门来测评和检查。此类信息系续应属于()
A.零级系统 B.一级系统 C.二级系统D.三级系统
答案：C

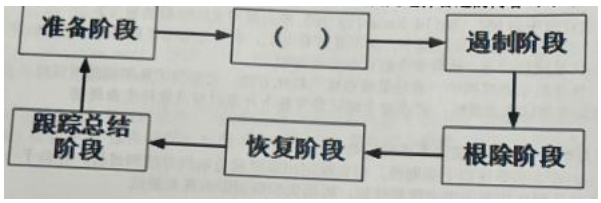
72.由于密码技术都依赖于密钥，因此密钥的安全管理是崔码技术应用中非常重要的环节，下列关于密钥管理说法错误的是()。
A.科克霍夫在《军事密码学》中指出系统的保密性不依载于对加密体制或算法的保密，而依赖于密钥
B.在保密通信过程中，通信双方可以一直使用之前用过的会话密钥，不影响安全性
C.带钥管理需要在安全策略的指导下处理密钥生命周期的整个过程，包括产生、存储、备份、分配、更新、撤销等
D.在保密通信过程中，通信双方也可利用 DiffieHellnan 协议协商出会话密钥进行保密通信
答案：B

73,一个信息管理系统通常会对用户进行分组并实施访问控制。例如，在一个学校的教务系统中，教师能够录入学生的考试成绩，学生只能查看自己的分数，而学校教务部门的管理人员能够对课程信息、学生的选课信息等内容进行修改，下列选项中，对访问控制的作用的理解错误的是()。
A.对经过身份鉴别后的合法用户提供所有服务
B.拒绝非法用户的非授权访问请求
C 在用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理
D.防止对信息的非授权改和滥用
答案：A
74.小赵是某大学计算机科学与技术专业的毕业生，在前往一家大型企业应聘时，面试经理要求他给出该企业信息系统访问控制模型的设计思路。如果想要为一个存在大最用户的信息系统实现自主访问控制功能，在以下选项中，从时间和资源消耗的角度，下列选项中他应该采取的最合适的模型或方法是()。
A 访问控制列表(ACL) B. 能力表（CL）C.BLP 模型 D.Biba 模型
答案：A

75.以下关于灾鸡恢复和数据备份的理解，说法正确的是()
A.增量备份是备份从上次完全各份后更断的全部数据文件
B.依据具备的灾难恢复资源程度的不同，灾难恢复能力分为 7 个等级
C.数报备份按数据类型划分可以划分为操作系统备份和数据库备份
D.使用差分备份数据恢复时只需最后一次的标准备份，如果每天都有大量数据变化，差分备份工作非常费时
答案：D

76.规范的实施流程和文档管理，是信息安全风险评估能否取得成果的重要基础，某单位在实施风险评估时，按照规范形成了若干文档，其中下面()中的文档应属于风险评估中“风险要素识别一阶段输出的文档。
A.《风险评估方案》，主要包括本次风险评估的目的、范围、目标、评估步、经费预算和进度安持等内容
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八等内容
C.《风险评估准则要求》、主要包括现有风险评估参考标准、采用的风险分析方法、资产分类标准等内容
D.《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
答案：D

77.为了能够合理、有序地处理安全事件，应事先制定出事件应救响成方法和过程，有助于一个组织在事件发生时限止淝乱的发生或是在混乱状态中迅速恢复控制，将损失和负面影响降至最低。PDCERP 方法论是一种广泛使用的方法，其将应急响应分成六个阶段，如下图所示，请为图中括号空白处选择合适的内容()。



A. 培训阶段 B.文档阶段 C. 报告阶段 D.检测阶段
答案：D

78.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, N)和 P 封装安全载荷协议(Encapsulating Security Payload, ESP)都能以传输模式和隧道模式工作
C.在随道模式中，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。
答案：D

79.目前，信息系统面临外部攻击者的恶意攻击威胁，从威胁能力和掌握资源分，这些或胁可以按照个人威胁、组织威胁和国家威胁三个层面划分，则下面选项中属于组织威胁的是 ()。
A.喜欢恶作剧、实现自我挑战的娱乐型黑客
B.实施犯罪、获取非法经济利益网络犯罪团伙
C.搜集政治、军事、经济等情报信息的情报机构
D.巩固战略优势，执行军事任务、进行目标破坏的信息作战部队
答案：B

80.某电子商务网站在开发设计时，使用了威胁建模方法来分析电子商务网站所面临的威胁。STRIDE 是微软 SDL 中提出的威胁建模方法,将威胁分为六类,为每一类威胁提供了标准的消减措施,Spoofing 是 STRIDE 中欺骗类的威，以下威胁中哪个可以归入此类威胁(()
A.网站竞争对手可能雇佣攻击者实施 DDoS 攻击，降低网站访问速度
B.网站使用使用 http 协议进行浏览等操作，未对数据进行加密，可能导致用户传输信息泄露，例如购买的商品金额等
C.网站使用使用 http 协议进行浏览等操作，无法确认数据与用户发出的是否一致，可能数据被中途篡改
D 网站使用用户名、密码进行登录验证，攻击者可能会利用弱口令或其他方式获得用户密码，以该用户身份登录修改用户订单等信息
答案：D

81.保护-检测-响应(Protection-Detection-Response, PDR)模型是()工作中常用的模型，其思想是承认()中漏洞的存在，正视系统面临的()，通过采取适度防护、加强()、落实对安全事件的响应、建立对威胜的防护来保障系统的安全。
A.信息系统;信息安全保障:威胁;检测工作
B.信息安全保障;信息系统;检测工作;威胁信危安全保障;信息系统;威助;检测工作
C. 信息安全保障;信息系统; 威胁;检测工作
D. 信息安全保障; 威胁; 信息系统; 检测工作
答案：C

82.数据库的安全很复杂,往往需要考虑多种安全策略,才可以更好地保护数捌库的安全，以下关于数据库常用的安用户的工作全策略理解不正确的题()
A.最小特权数则，是让用户可以合法的存取或能改数据库的前提下，分配最小的特权，使得这些信息恰好能够完成 用户的工作
B.最大共享策略,在保证数据库的完整性,保密性和可用性的前提下,最大程度地共享数据库中的信息
C.粒度最小策略,将数据库中的数据项进行划分,粒度越小,安全级别越高,在实际中需要选择最小粒度
D.按内容存取控制策略,不同权限的用户访问数据库的不同部分
答案：B

83.若一个组织声称自己的 1SMS 符合 1SO/1BC 27001 成 GB/T220B0 标准要求，其信息安全控制措施通常在以下方面实施常规控制，以下哪个选项的内容不属于常规控制措施的范围

A.信息安全方针、信息安全组织、资产管理　　B.人力资源安全、物理和环境安全、通信安全

C.安全采购、开发与维护、合规性　　D.安全事件管理、供应商关系、业务安全性审计

答案：D

84.关于《网络安全法》域外适用效力的理解，以下哪项是错误的()

A .当前对于境外的网络攻击，我国只能通过向来源国采取抗议。

B.对于来自境外的网络安全威胁我国可以组织技术力量进行监测、防御和处置

C.对于来自境外的违法信息我国可以加以断传播

D.对于来自境外的网络攻击我国可以追究其法律责任

答案：A

85,信息系统安全保障评估概念和关系如图所示。信息系统安全保障评估，就是在信息系统所处的运行环境中对信息系统安全保障的具体工作和活动进行客观的评估，通过信息系统安全保障评估所搜集的()，向信息系统的所有相关方提供信息系统的()能够实现其安全保障策略，能够将其所面临的风险降低到其可接受的程度的主观信心。信息系统安全保障评估的评估对象是()，信息系统不仅包含了仅讨论技术的信息技术系统，还包括同信息系统所处的运行环境相关的人和管理等领域，信息系统安全保障是一个动态持续的过程，涉及信息系统整个()，因此信息系统安全保障的评估也应该提供一种()的信心。

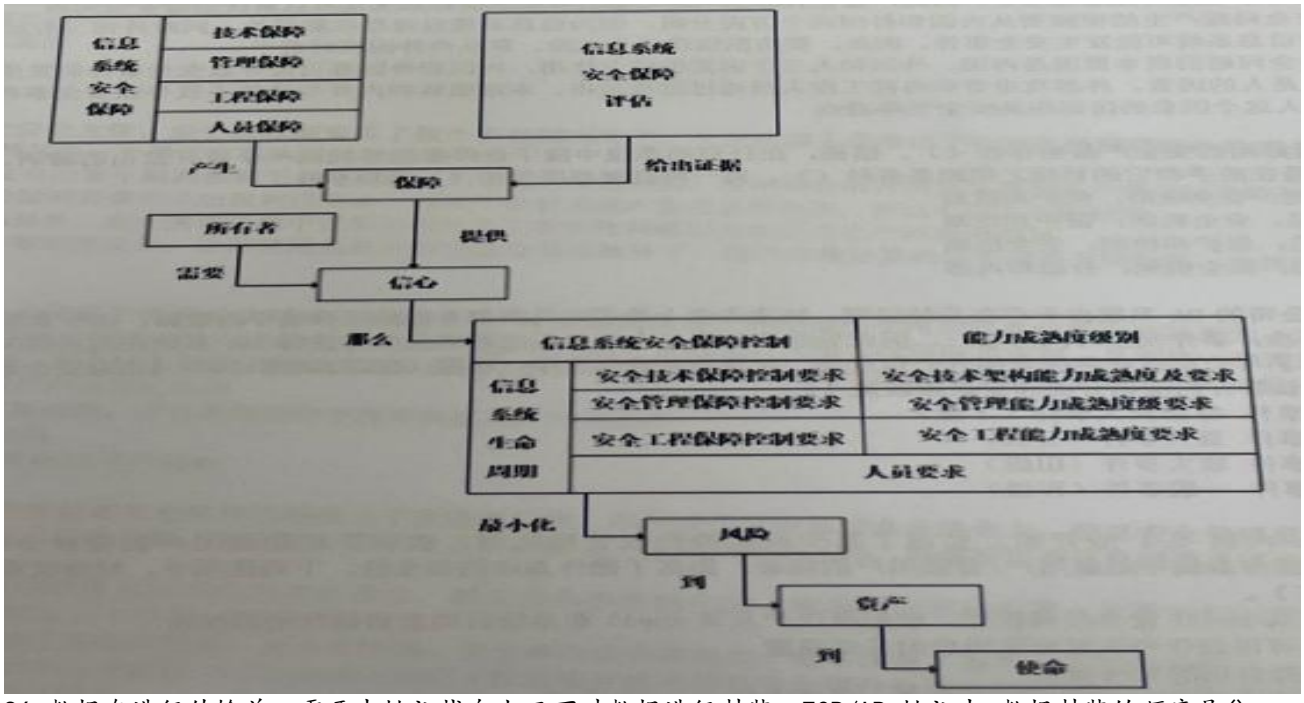
A.　安全保障工作:客观证据:信息系统;生命周期;动态持续

B.　客观证据:安全保障工作;信息系统:生命周期:动态持续

C .　客观证据:　安全保障工作;　生命周期:　信息系统:　动态持续

D.　客观证据:　安全保障工作;　动态持续;　信息系统:　生命周期;

答案：B



86.数据在进行传输前，需要由协议栈自上而下对数据进行封装。TCP/IP 协议中,数据封装的顺序是()

A 传输层、网络接口层、互联网络层　　B.传输层、互联网络层、网络接口层

C.互联网络层、传输层、网络接口层　　D.互联网络层、网络接口层、传输层

答案：B

87. 跟据《信息安全等级保护管理办法》、《关于开展信息安全等级保护测评体系建设试点工作的通知》(公信安(20091812)级保护建设和开展()工作的知(公信安[20101303 号)等文件，由公安部对等级保护测评机构管理，接受测评机构的申请、考核和定期()，对不具备能力的测评机构则()

A.等级测评:测评体系:等级保护评估中心:能力验证;取消授权
B.测评体系:等级保护评估中心:等级测评:能力验证:取消授权
c. 测评体系; 等级测评: 等级保护评估中心: 能力验证:取消授权
D. 测评体系:等级保护评估中心: 能力验证: 等级测评: 取消授权
答案: C

88.若一个组织声称自己的 ISMS 符合 1SO/1BC27001 成 GB/T22080 标准要求，其信息安全控制措施通常需要在符合性方面实施常规控制，符合性常规控制这一领域不包括以下哪项控制目标()
A .符合法律要求　　B.符合安全策略和标准以及技术符合性
C.信息系统审核考虑　　D.访问控制的业务要求、用户访问管理
答案: D

89.随着信息技术的不断发展，信息系统的重要性也越来越突出，而与此同时，发生的信息安全事件也越来越多。综合分析信息安全问题产生的根源，下面描述正确的是(),
A.信息系统自身存在脆弱性是根本原因。信息系统越来越重要,同时自身在开发、部署和使用过程中存在的脆弱性,导致了诸多的信息安全事件发生。因此,杜绝脆弱性的存在是解决信息安全问题的根本所在
B.信息系统面临诸多黑客的威胁，包括恶意攻击者和恶作剧攻击者。信息系统应用越来越广泛，接触信息系统的人越多，信息系统越可能遭受攻击。因此，避免有恶意攻击可能的人接触信息系统就可以解决信息安全问题
C.信息安全问题产生的根源要从内因和外因两个方面分析，因为信息系统自身存在脆弱性，同时外部又有威胁源，从而导致信息系统可能发生安全事件。因此，要防范信息安全风险，需从内外因同时着手
D.信息安全问题的根本原因是内因、外因和人三个因素的综合作用，内因和外因都可能导致安全事件的发生，但最重要的还是人的因素，外部攻击者和内部工作人员通过远程攻击、本地破坏和内外勾结等手段导致安全事件发生。因此，对人这个因素的防范应是安全工作重点
答案: C

90.即使最好用的安全产品也存在()。结果，在任何的系统中散手最终都能够找出一个被开发出的漏洞。一种有效的对策是在敌手和它的目标之间配备多种()。每一种机制都应包括()两种手段。
A.安全机制:安全缺陷;保护和检测　　B.安全缺陷;安全机制:保护和检测
C.安全缺陷;保护和检测:安全机制　　D.安全缺陷;安全机制:外边和内部
答案: B

91.某贸易公司的 OA 系统由于存在系统漏洞，被攻击者上传了木马病毒并删除了系统中的数据，由于系统备份是每周六进行一次,事件发生时间为周三,因此导致该公司三个工作日的数据丢失并使得 OA 系统在随后两天内无法访问，影响到了与公司有业务往来部分公司业务。在事故处理报告中，根据 GB/Z 20986-2007《信息安全事件分级分类指南》，该事件的准确分类和定级应该是()
A.有害程序事件 特别重大事件(I 级)　　B.信息破坏事件 重大事件(II 级)
C.有害程序事件 较大事件(III 级)　　D 信息破坏事件 一般事件(IV 级)
答案: D

92.从 Linux 内核 2.1 版开始，实现了基于权能的特权管理机制，实现了对超级用户的特权分割，打破了 UNIX/LINUX 操作系统中超级用户/普通用户的概念，提高了操作系统的安全性。下列选项中，对特权管理机制的理解错误的是()
A.普通用户及其 shell 没有任何权能，而超级用户及其 shell 在系统启动之初拥有全部权能
B.系统管理员可以剥夺和恢复超级用户的某些权能
C.进程可以放弃自己的菜的权地
D.当普通用户的某些操作设计特权操作时，仍然通过 setuld 实现
答案: B

93.以下哪项制度或标准被作为我国的一项基础制度加以推行，并且有一定强制性，其实施的主要目标是提高我国信息和信息系统安全建设的整体水平，重点保障基础信息网络和重要信息系统的安全。()
A.信息安全管理体系(ISMS)　　B.信息安全等级保护　C.NIST SP800　D.ISO 270000 系列
答案: B

94.小牛在对某公司的信息系统进行风险评估后，因考虑到该业务系统中部分涉及金融交易的功能模块风险太高，他建议该公司以放弃这个功能模块的方式来处理该风险。请问这种风险处置的方法是()。
A. 降低风险 B.规避风险 C.转移风险 D.放弃风险
答案：B

95.部署互联网协议安全虚拟专用网(Internet Protocol Security Virtual Private Network，IPsec VPN)时，以下说法正确的是().
A.配置 MD5 安全算法可以提供可靠地数据加密
B.配置 AES 算法可以提供可靠的数据完整性验证
C.部署 IPsec VPN 网络时,需要考虑 IP 地址的规划,尽量在分支节点使用可以聚合的 IP 地址段,来减少 IPsec 安全关联(Security Authentication,SA)资源的消耗
D.报文验证头协议(Authentication Header，AH)可以提供数据机密性
答案：C

96.私有 IP 地址是一段保留的 IP 地址。只使用在局域网中，无法在 Internet 上使用。关于私有地址，下面描述正确的是()。
A.A 类和 B 类地址中没有私有地址，C 类地址中可以设置私有地址
B.A 类地址中没有私有地址，B 类和 C 类地址中可以设置私有地址
C.A 类、B 类和 C 类地址中都可以设置私有地址
D.A 类、B 类和 C 类地址中都没有私有地址
答案：C

97.PKI 的主要理论基础是()
A.对称密码算法 B.公钥密码算法 C.量子密码 D.摘要算法
答案：B

98.你是单位安全主管，由于微软刚发布了数个系统漏洞补丁，安全运维人员给出了针对此批漏洞修补的四个建议方案，请选择其中一个最优方案执行()
A.由于本次发布的数个漏洞都属于高危漏洞,为了避免安全风险,应对单位所有的服务器和客户端尽快安装补丁
B.本次发布的漏洞目前尚未出现利用工具，因此不会对系统产生实质性危害，所以可以先不做处理
C.对于重要的服务，应在测试环境中安装并确认补丁兼容性问题后再在正式生产环境中部署
D.对于服务器等重要设备，立即使用系统更新功能安装这批补丁，用户终端计算机由于没有重要数据，由终端自行升级
答案：C

99.某网络安全公司基于网络的实时入侵检测技术，动态监测来自于外部网络和内部网络的所有访问行为。当检测到来自内外网络针对或通过防火墙的攻击行为，会及时响应，并通知防火墙实时阻断攻击源，从而进一步提高了系统的抗攻击能力，更有效地保护了网络资源，提高了防御体系级别。但入侵检测技术不能实现以下哪种功能()。
A.检测并分析用户和系统的活动
B.核查系统的配置漏洞，评估系统关键资源和数据文件的完整性
C.防止 IP 地址欺骗
D.识别违反安全策略的用户活动
答案：C，检测系统的作用只能发现问题，无法解决问题。

100.某 IT 公司针对信息安全事件已经建立了完善的预案，在年度企业信息安全总结会上，信息安全管理员对今应急预案工作做出了四个总结，其中有一项总结工作是错误，作为企业的 CSO，请你指出存在问题的是哪个总结
A..公司制定的应急演练流程包括应急事件通报”确定应急事件优先级、应急响应启动实施、应急响应时间后期维、更新现有应急预案五个阶段，流程完善可用
B.公司应急预案包括了基础环境类、业务系统类、安全事件类和其他类，基本覆盖了各类应急事件类型

C.公司应急预案对事件分类依据 GB/220986-2007《信息安全技术信息安全事件分类分级指南》，分为 7 个级别，预案符合国家相关标准
D 公司成立了信息安全应急响应组织，该组织由业务和技术人员组成，划分成应急响应领导小组、技术保障小专家小组、实施小组和日常运行小组
答案：D，D 是针对应急组织的，不是针对预案的。