注册信息安全专业人员考试（精选 300 题）

1. 自 2004 年 1 月起,各有关部门在申报信息安全国家标准计划项目时,必须经由以下哪个组织提出工作情况,协调一致后由该组织申报。(B)

A.全国通信标准化技术委员会(TC485)

B.全国信息安全标准化技术委员会(TC260)

C.中国通信标准化协会(CA)

D.网络与信息安全技术工作委员会

2、安全管理体系,国际上有标准(Information technology Security tech nformation systems)(ISO/IEC 27001-2013),而我国发布了《信息技术信息安全管理体系要求》(GBT 22080-2008)请问,这两个标准的关系是 (D)

A.IDT(等同采用),此国家标准等同于该国际标准,仅有或没有编辑性修改

B.EQV(等效采用),此国家标准等效于该国家标准,技术上只有很小差异

C.AEQ(等效采用),此国家标准不等效于该国家标准

D.没有采用与否的关系,两者之间版本不同,不应直接比较

3、“cc”标准是测评标准类的重要标准,从该标准的内容来看,下面哪项内容是针对具体的被测评对象描述了该对象的安全要求及其相关安全功能和安全措施,相当于从厂商角度制定的产品或系统实现方案（C）

A.评估对象(TOE)

B.保护轮廓(PP)

C.安全目标(ST)

D.评估保证级(EAL)

4、信息安全等级保护分级要求,第三级适用正确的是 （B）

A.适用于一般的信息和信息系统,其受到破坏后,会对公民、法人和其他组织的权益有一定影响,但不危害国家安全、社会秩序、经济建设和公共利益

B.适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统,其受到破坏后,会对国家安全、社会秩序、经济建设和公共利益造成一定损害

C.适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统,其受到破坏后会对国家安全、社会秩序、经济建设和公共利益造成较大损害

D.适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统,其受到破坏后,会对国家安全、社会秩序、经济建设和公共利益造成特别严重

5、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:(C)

A.国家秘密及其密级的具体范围,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机关规定

B.各级国家机关、单位对所产生的国家秘密事项,应当按照国家秘密及其密级具体范围的规定确定密级

C.对是否属于国家机密和属于何种密级不明确的事项,可由各单位自行参考国家要求确定和定级,然后报国家保密工作部门确定

D.对是否属于国家秘密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。

6、为了保障网络安全,维护网络空间主权和国家安全、社会公共利益,保护公民、法人和其他组织的合法权益,促进经济社会信息化健康发展,加强在中华人民共和国境内建设、运营、维护和使用网络,以及网络安全的监督管理。2015 年 6 月,第十二届全国人大常委会第十五次会议初次审议了一部法律草案,并于 7 月 6 日

起在网上全文公布,向社会公开征求意见,这部法律是(B)
A.《中华人民共和国保守国家秘密法》
B.《中华人民共和国网络安全法》
C.《中华人民共和国国家安全法》
D.《中华人民共和国互联网安全法》

7、为了进一步提高信息安全的保障能力和防护水平,保障和促进信息化建设的健康发展,公安部等四部门联合发布《关于信息安全等级保护工作的实施意见》(公通字[2004166 号),对等级保护工作的开展提供宏观指导和约束。明确了等级保护工作的基本内容、工作要求和实施计划,以及各部门工作职责分工等。关于该文件,下面理解正确的是 (A)
A.该文件是一个由部委发布的政策性文件,不属于法律文件。
B.该文件适用于 2004 年的等级保护工作。其内容不能约束到 2005 年及之后的工作。
C.该文件是一个总体性指导文件,规定了所有信息系统都要纳入等级保护定级范围
D.该文件适用范围为发文的这四个部门,不适用于其他部门和企业等单位

8、分组密码算法是一类十分重要的密码算法,下面描述中,错误的是(C)
A.分组密码算法要求输入明文按组分成固定长度的块
B.分组密码算法每次计算得到固定长度的密文输出块
C.分组密码算法也称为序列密码算法
D.常见的 DES、IDEA 算法都属于分组密码算法

9、密码学是网络安全的基础,但网络安全不能单纯依靠安全的密码算法,密码协议也是网络安全的个重要组成部分。下面描述中,错误的是 (A)
A 在实际应用中,密码协议应按照灵活性好、可扩展性高的方式制定,不要限制和框住所有的执行步骤,有些复杂的步骤可以不明确处理方式
B.密码协议定义了两方或多方之间为完成某项任务而制定的一系列步骤,协议中的每个参与方都必须了解协议,且按步骤执行
C.根据密码协议应用目的的不同,参与该协议的双方可能是朋友和完全信任的人,也可能是敌人和互相完全不信任的人
D.密码协议(cryptographic protoco1),有时也称安全协议(securityprot oco1)是使用密码学完成某项特定的任务并满足安全需求,其目的是提供安全服务

10、美国计算机协会(ACM)宣布将 2015 年的 ACM 奖授予给 Whitfield Diffiic 和 Artfield 下面哪项工作是他们的贡献 (C)
A.发明并第一个使用 c 语言
B.第一个发表了对称密码算法思想
C.第一个发表了非对称密码算法思想
D.第一个研制出防火墙

11、虚拟专用网络(VPN)通常是指在公共网络中利用隧道技术,建立一个临时的、安全的网络。这里的字母 P 的正确解释是 (C)
A. speciall- purpose,特定的、专用用途的
B. Proprietary,专有的、专卖的
C. Private,私有的、专有的
D. specific,特种的、具体的

12、为防范网络欺诈确保交易安全,网银系统首先要求用户安全登录,然后使用“智能卡+短信证模式进行网上转账等交易。在此场景中用到下列哪些鉴别方法?(A)

A.实体“所知”以及实体“所有”的鉴别方法
B.实体“所有”以及实体“特征”的鉴别方法
C.实体“所知”以及实体“特征”的鉴别方法
D.实体“所有”以及实体“行为”的鉴别方法

13、实体身份鉴别一般依据以下三种基本情况或这三种情况的组合:实体所知的鉴别方法、实体所有的鉴别方法和基于实体特征的鉴别方法。下面选项中属于实体特征的鉴别方法是 (D)
A.将登录口令设置为出生日期
B.通过询问和核对用户的个人隐私信息来鉴
C.使用系统定制的、在本系统专用的 Ic 卡进行鉴别
D.通过扫脸和识别用户的脸部信息来鉴别

14、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)
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扩展性
C.强制访问控制模型要求主题和客体都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

15、在信息系统中,访问控制是重要的安全功能之一。他的任务是在用户对系统资源提供最大限度共享的基础上,对用户的访问权限进行管理,防止对信息的非授权篡改和滥用。访问控制模型将实体划分为主体和客体两类,通过对主体身份的识别来限制其对客体的访问权限。下列选项中,对主体、客体和访问权限的描述中错误的是(D)
A.对文件进行操作的用户是一种主体
B.主体可以接受客体的信息和数据,也可能改变客体相关的信息
C.访问权限是指主体对客体所允许的操作
D.对目录的访问权可分为读、写和拒绝访问

16、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模型的设计思路。如果想要为一个存在大量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)
A.访问控制列表(ACL)
B.能力表(CL)
C.BLP 模型
D.Biba 模型

17、强制访问控制是指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,具有较高的安全性。适用于专用或对安全性要求较高的系统,强制访问控制模型有多种模型,如 BLP、Biba、 clark- Wilson 和 chinesc 等。小李自学了 BLP 模型,并对该模型的特点进行了总结。以下 4 种对 BLP 模型的描述中,正确的是 (B)
A.BLP 模型用于保证系统信息的机密性,规则是向上读,向下写”
B.BLP 模型用于保证系统信息的机密性,规则是“向下读,向上写”
C.BLP 模型用于保证系统信息的完整性,规则是“向上读,向下写
D.BLP 模型用于保证系统信息.的完整性,规则是“向下读,向上写

18、访问控制方法可分为自主访问控制、强制访问控制和基于角色的访问控制,他们具有不同的特点和应用场景。如果需要选择一个访问控制方法,要求能够支持最小特权原则和职责分离原则,而且在不同的系统配置下可以具有不同的安全控制,那么在下列选项中,能够满足以上要求的选项是 (C)

A.自主访问控制

B.强制访问控制

C.基于角色的访问控制

D.以上选项都可以

19、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(D)

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 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 802.111 标准草案制定的,而 WPA2 是依照 802.111 正式标准制定的

20、随着高校业务资源逐渐向数据中心高度集中,Web 成为一种普适平台,上面承载了越来越多的核心业务。Web 的开放性带来丰富资源、高效率、新工作方式的同时,也使机构的重要信息暴露在越来越多的威胁中。去年,某个…网站遭遇 SQL 群注入(Mass SQL Injectior)攻击,网站发布的重要信息被篡改成为大量签名,所以该校在某信息安全公司的建议下配置了状态检测防火墙,其原因不包括 (C)

A.状态检测防火墙可以应用会话信息决定过滤规则

B.状态检测防火墙具有记录通过每个包的详细信息能力

C.状态检测防火墙过滤规则与应用层无关,相比于包过滤防火墙更易安装和使用

D.状态检测防火墙结合网络配置和安全规定做出接纳、拒绝、身份认证或报警等处理动作答

21、异常入侵检测是入侵检测系统常用的一种技术,它是识别系统或用户的非正常行为或者对于计算机资源的非正常使用,从而检测出入侵行为。下面说法错误的是 (B)

A.在异常入侵检测中,观察到的不是已知的入侵行为,而是系统运行过程中的异常现象

B.实施异常入侵检测,是将当前获取行为数据和已知入侵攻击行为特征相比较,若匹配则认为有攻击发生

C.异常入侵检测可以通过获得的网络运行状态数据,判断其中是否含有攻击的企图,并通过多种手段向管理员报警

D.异常入侵检测不但可以发现从外部的攻击,也可以发现内部的恶意行为

22、某集团公司的计算机网络中心内具有公司最重要的设备和信息数据。网络曾在一段时间内依然遭受了几次不小的破坏和干扰;虽然有防火墙但系统管理人员也未找到真正的事发原因。某网络安全公司为该集团部署基于网络的入侵检测系统(NIDS)将 DS 部署在防火墙后,以进行二次防御。那 NIDS 不会在()区域部署。(D)

A.DMZ 区域

B.内网主干

C.内网关键子网

D.外网入口

23、入侵检测系统有其技术优越性,但也有其局限性,下列说法错误的是 (A)

A.对用户知识要求高、配置、操作和管理使用过于简单,容易遭到攻击

B.入侵检测系统会产生大量的警告消息和可疑的入侵行为记录,用户处理负担很重

C.入侵检测系统在应对自身攻击时,对其他数据的检测可能会被抑制或者受到影响

D.警告消息记录如果不完整,可能无法与入侵行为关联

24、安全域是由一组具有相同安全保护需求并相互信任的系统组成的逻辑区域,下面哪项描述是错误的 (A)

A.安全域划分主要以业务需求、功能需求和安全需求为依据,和网络、设备的物理部署位置无关
B.安全域划分能把一个大规模复杂系统的安全问题,化解为更小区域的安全保护问题
C.以安全域为基础,可以确定该区域的信息系统安全保护等级和防护手段,从而使同一安全域内的资产实施统一的保护
D.安全域边界是安全事件发生时的抑制点,以安全域为基础,可以对网络和系统进行安全检查和评估,因此安全域划分和保护也是网络防攻击的有效防护方式

25、小王是某通信运营商公司的网络安全架构师,为该公司推出的一项新型通信系统项目做安全架构规划,项目客户要求对他们的大型电子商务网络进行安全域的划分,化解为小区域的安全保护,每个逻辑区域有各自的安全访问控制和边界控制策略,以实现大规模电子商务系统的信息保护小王对信息系统安全域(保护对象)的划分不需要考虑的是 （D）
A.业务系统逻辑和应用关联性,业务系统是否需要对外连接
B.安全要求的相似性,可用性、保密性和完整性的要求是否类似
C.现有网络结构的状况,包括现有网路、地域和机房等
D.数据库的安全维护

26、在 Windos7 中,通过控制面板(管理工具——本地安全策略——安全设置——账户策略)可以进入操作系统的密码策略设置界面,下面哪项内容不能在该界面进行设置 (D)
A.密码必须符合复杂性要求
B.密码长度最小值
C.强制密码历史
D.账号锁定时间

27、 Linux 系统中常用数字来表示文件的访问权限,假设某文件的访问限制使用了 755 来表示,则下面哪项是正确的 (B)
A.这个文件可以被任何用户读和写
B.这个可以被任何用户读和执行
C.这个文件可以被任何用户写和执行
这个文件不可以被所有用户写和执行

28、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)关闭不必要的服务和端口;(2)在“在本地安全策略”重配置账号策略、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,开启账号策略。这些操作中错误的是 (D)
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

29、在 Windows 系统中,存在默认共享功能,方便了局域网用户使用,但对个人用户来说存安全风险。如果电脑联网,网络上的任何人都可以通过共享使用或修改文件。小刘在装有 Windows XP 系统的计算机上进行安全设置时,需要关闭默认共享。下列选项中,不能关闭默认共享的操作是 (A)
A.HKEYLOCALMACHINE\SYSTEM\Currentcontrolset\Services\lenmanserver\paraneters 项中的“ Autodisconnect"项键值改为 0
B. 将“ HKEY LOCAL machinesystemcurrentcontrolset\Services\ lenmanserver \paraneters" 项中的 Autoshareserver"项键值改为 0
C. HKEY LOCAL MACHINE\SYSTEM\Currentcontrolset Services\ lenmanserver\paraneters"I Autosharewks"项

键值改为 0
D.在命令窗口中输入命令,删除 C 盘默认共享: net share C/del

30、从 Linux 内核 21 版开始,实现了基于权能的特权管理机制,实现了超级用户的特权分割,打破了 UNIXLINUX 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 (B)
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某些权能
D.当普通用户的某些操作涉及特权操作时,仍然通过 setuid 实现

31、关于数据库恢复技术,下列说法不正确的是 (D)
A.数据库恢复技术的实现主要依靠各种数据的冗余和恢复机制技术来解决,当数据库中数据被破坏时,可以利用冗余数据来进行修复
B.数据库管理员定期地将整个数据库或部分数据库文件备份到磁带或另一个磁盘上保存起来是数据库恢复中采用的基本技术
C.日志文件在数据库恢复中起着非常重要的作用,可以用来进行事物故障恢复和系统故障恢复,并协助后备副本进行介质故障恢复
D.计算机系统发生故障导致数据未存储到固定存储器上,利用日志文件中故障发生前数据的值,将数据库恢复到故障发生前的完整状态,这一对事务的操作称为提交

32、关系数据库的完整性规则是数据库设计的重要内容,下面关于“实体完整性”的描述正确的 (B)
A.指数据表中列的完整性,主要用于保证操作的数据(记录)完整、不丢项
B.指数据表中行的完整性,主要用于保证操作的数据(记录)非空、唯一且不重复
C.指数据表中列必须满足某种特定的数据类型或约束,比如取值范围、数值精度等约束
D.指数据表中行必须满足某种特定的数据姓雷或约束,比如在更新、插入或删除记录时,更将关联有关的记录一并处理才可以

33、数据在进行传输前,需要由协议自上而下对数据进行封装。 TCP/IP 协议中,数据封装的顺序是 (B)
A.传输层、网络接口层、互联网络层
B.传输层、互联网络层、网路接口层
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

34、安全多用途互联网邮件扩展(Secure Nultipurpose Internet Mail Extension, S/MIME)是指一种保障邮件安全的技术,下面描述错误的是 (C)
A.S/MIME 采用了非对称密码学机制
B.S/MIME 支持数字证书
C.S/MIME 采用了邮件防火墙技术
D.S/MIME 支持用户身份认证和邮件加密

35、ApacheHTTPServer(简称 Apache)是一个开放源码的 Web 服务运行平台,在使用过程中,该软件默认会将自己的软件名和版本号发送给客户端。从安全角度出发,为隐藏这些信息,应当采取以下哪种措施 (B)
A.不选择 Windows 平台,应选择在 Linux 平台下安装使用
B.安装后,修改配置文件 httpd.conf 中的有关参数
C.安装后,删除 ApscheHTTPServer 源码
D.从正确的官方网站下载 ApecheHTTPServer,并安装使用

36、 Internet Explorer,简称三,是微软推出的一款 Web 浏览器,IE 中有很多安全设置选项,用来设置安全上网环境和保护用户隐私数据。以下哪项不是三中的安全配置项目 (C)

A.设置 Cookie 安全,允许用户根据自己安全策略要求者、设置 Cookie 策略,包括从阻止所有 Cookie 到接受所有 Cookie,用户也可以选择删除已经保存过的

B.用自动完成和密码记忆功能,通过设置禁止 IE 自动记忆用户输入过的 Web 地址和表单,也禁止 IE 自动记忆表单中的用户名和口令信息

C.设置每个连接的最大请求数,修改 Mukeepa; ivecquests,如果同时请求数达到阈值就不再响应新的请求,从而保证了系统资源不会被某个链接大量占用

D.为网站设置适当的浏览器安全级别,用户可以将各个不同的网站划分到 Internet、本地 Internet、受信任的站点、受限制的站点等不同安全区域中,以采取不同的安全访问策略

37、下面对”零日(zero-day)漏洞”的理解中,正确的是 (D)

A.指一个特定的漏洞,该漏洞每年 1 月 1 日零点发作,可以被攻击者用来远程攻击,获取主机权限

B.指一个特定的漏洞,特指在 2010 年被发现出来的一种漏洞,该漏洞被“震网”病毒所利用用来攻击伊朗布什尔核电站基础设施

C.指一类漏洞,即特别好被被利用,一旦成功利用该漏洞,可以在 1 天内完成攻击,且成功达到攻击目标

D.指一类漏洞,即刚被发现后立即被恶意利用的安全漏洞。一般来说,那些已经被小部分人发现,但是还未公布、还不存在安全补丁的漏洞都是零日漏洞

38.为达到预期的攻击目的,恶意代码通常会被采用各种方法将自己隐藏起来。关于隐藏方法,下面理解错误的是 (C)

A.隐藏恶意代码进程,即将恶意代码进程隐藏起来,或者改名和使用系统进程名,以更好的躲避检测,迷惑用户和安全检测人员

B.隐藏恶意代码的网络行为,复用通用的网络端口,以躲避网络行为检测和网络监控

C.隐藏恶意代码的源代码,删除或加密源代码,仅留下加密后的二进制代码,以躲避用户和安全检测人员

D.隐藏恶意代码的文件,通过隐藏文件、采用流文件技术或 HOOK 技术、以躲避系统文件检查和清除

39、某网站管理员小邓在流量监测中发现近期网站的入站 ICMP 流量上升 250%尽管网站没有发现任何的性能下降或其他问题,但为了安全起见,他仍然向主管领导提出了应对措施,作为主管负责人,请选择有效的针对此问题的应对措施:(A)

A.在防火墙上设置策略,阻止所有的 ICMP 流量进入(关掉 ping)

B.删除服务器上的 ping.exe 程序

C.增加带宽以应对可能的拒绝服务攻击

D.增加网站服务以应对即将来临的拒绝服务攻击

40、下面四款安全测试软件中,主要用于 WEB 安全扫描的是 (B)

A. Cisco Auditing Tools

B. Acunetix Web Vulnerability Scanner

C.NMAP

D. ISS Database Scanner

41、关于 ARP 欺骗原理和防范措施,下面理解错误的是 (D)

A.AR 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存入到 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

42、在软件保障成熟度模型(Software Assurance Maturity Mode,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 (D)

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

43、针对软件的拒绝服务攻击时通过消耗系统资源是软件无法响应正常请求的一种攻击方式,在软件开发时分析拒绝服务攻击的威胁,以下哪个不是需要考虑的攻击方式 (D)

A.攻击者利用软件存在逻辑错误,通过发送某种类型数据导致运算进入死循环,CPU 资源占用始终 100%

B.攻击者利用软件脚本使用多重账套查询在数据量大时会导致查询效率低,通过发送大量的查询导致数据库相应缓慢

C.攻击者利用软件不自动释放连接的问题,通过发送大量连接的消耗软件并发生连接数,导致并发连接数耗尽而无法访问

D.攻击者买通了 IDC 人员,将某软件运行服务器的网线拔掉导致无法访问

44、某网站为了更好向用户提供服务,在新版本设计时提供了用户快捷登陆功能,用户如果使用上次的 IP 地址进行访问,就可以无需验证直接登录,该功能推出后,导致大量用户账号被盗用,关于以上问题的说法正确的是 (D)

A.网站问题是由于开发人员不熟悉安全编码,编写了不安全的代码导致攻击面增大,产生此安全问题

B.网站问题是由于用户缺乏安全意识导致,使用了不安全的功能,导致网站攻击面增大,产生此问题

C.网站问题是由于使用便利性提高带来网站用户数增加,导致网络攻击面增大,产生此安全问

D.网站问题是设计人员不了解安全设计关键要素,设计了不安全的功能,导致网站攻击面增大,产生此安全问题

45、下面有关软件安全问题的描述中,哪项不是由于软件设计缺陷引起的 (A)

A.设计了用户权限分级机制和最小特权原则,导致软件在发布运行后,系统管理员不能查看系统审计信息

B.设计了采用不加盐(SALT)的 SHA-1 算法对用户口令进行加密存储,导致软件在发布运行后,不同的用户如使用了相同的口令会得到相同的加密结果,从而可以假冒其他用户登录

C.设计了缓存用户隐私数据机制以加快系统处理性能,导致软件在发布运行后,被黑客攻击获取到用户隐私数据

D.设计了采用自行设计的加密算法对网络传输数据进行保护,导致软件在发布运行后,被攻击对手截获网络数据并破解后得到明文

46、某购物网站开发项目经过需求分析进入系统设计阶段,为了保证用户账户的安全,项目开发人员决定用户登录时如用户名或口令输入错误,给用户返回用户名或口令输入错误”信息,输入错误达到三次,将暂时禁止登录该账户,请问以上安全设计遵循的是哪项安全设计原则:(C)

A.最小共享机制原则

B.经济机制原理

C.不信任原则

D.默认故障处理保护原则

47、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 (D)

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

48、小王在学习信息安全管理体系相关知识之后,对于建立信息安全管理体系,自己总结了下面四条要求,其中理解不正确的是 (B)
A.信息安全管理体系的建立应参照国际国内有关标准实施,因为这些标准是标准化组织在总结研究了很多实际的或潜在的问题后,制定的能共同的和重复使用的规则
B.信息安全管理体系的建立应基于最新的信息安全技术,因为这是国家有关信息安全的法律和法规方面的要求,这体现以预防控制为主的思想
C.信息安全管理体系应强调全过程和动态控制的思想,因为安全问题是动态的,系统所处的安全环境也不会一成不变的,不可能建设永远安全的系统
D.信息安全管理体系应体现科学性和全面性的特点,因为要对信息安全管理设计的方方面面实施较为均衡的管理,避免遗漏某些方面而导致组织的整体信息安全水平过低

49、美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)隶属美国商务部,NIST发布的很多关于计算机安全的指南文档。下面哪个文档是由 NIST 发布的 (C)
A. ISO 27001(Information technology−security techniques
Informtion security management systems−requirements)
B. X509 Information Technology−open Systems −The Directory: Authentication Framcwork
C. SP 800−37(Guide for Applying the Risk Management Framcwork to Federal Information Systems》
D. RFC 2402（IP Authenticat Heade）

50、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 (B)
A.降低风险
B.规避风险
C.转移风险
D.放弃风险

51、残余风险是风险管理中的一个重要概念。在信息安全风险管理中,关于残余风险描述错误的是 (D)
A.残余风险是采取了安全措施后,仍然可能存在的风险:一般来说,是在综合考虑了安全成本与效益后不去控制的风险
B.残余风险应受到密切监视,它会随着时间的推移而发生变化,可能会在将来诱发新的安全事件
C.实施风险处理时,应将残余风险清单告知信息系统所在组织的高管,使其了解残余风险的存在和可能造成的后果
D.信息安全风险处理的主要准则是尽可能降低和控制信息安全风险,以最小残余风险值作为风险管理效果评估指标

52、在信息安全管理过程中,背景建立是实施工作的第一步。下面哪项理解是错误的(B)
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
D.背景建立阶段应分析信息系统的体系结构和关键要素,分析信息系统的安全环境和要求,形成信息系统的

安全要求报告

53、降低风险(或减低风险)是指通过对面临风险的资产采取保护措施的方式来降低风险,下面哪个措施不属于降低风险的措施 (B)

A.减少威胁源。采用法律的手段制按计算机犯罪,发挥法律的威慑作用,从而有效遏制威胁源的动机

B.签订外包服务合同。将有技术难点、存在实现风险的任务通过签订外部合同的方式交予第三方公司完成,通过合同责任条款来应对风险

C.减少脆弱性。及时给系统补丁,关闭无用的网络服务端口,从而减少系统的脆弱性,降低被利用的可能性

54、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 A 的 FTP 服务存在高风险漏洞。随后该单位在风险处理时选择了关闭 FTP 服务的处理措施。请问该措施属于哪种风险处理方式 (B)

A.风险降低

B.风险规避

C.风险转移

D.风险接受

55、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 (B)

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有客观性

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

56、信息安全风险评估是信息安全风险管理工作中的重要环节。在国家网络与信息安全协调小组发布的《关于开展信息安全风险评估工作的意见》(国信办[200615 号)中,风险评估分为自评估和检查评估两种形式,并对两种工作形势提出了有关工作原则和要求。下面选项中描述正确的是 (A)

A.信息安全风险评估应以自评估为主,自评估和检查评估相互结合、互为补充

B.信息安全风险评估应以检查评估为主,自评估和检查评估相互结合、互为补充

C.自评估和检查评估时相互排斥的,单位应慎重地从两种工作形式选择一个,并长期使用

D.自评估和检查评估是相互排斥的,无特殊理由的单位均应选择检查评估,以保证安全效果

57、信息安全风险评估是信息安全风险管理工作中的重要环节。在〈关于开展信息安全风险评估工作的意见》(国信办[2006]5 号)中,指出了风险评估分为自评估和检查评估两种形式,并对两种工作形式提出了有关工作原则和要求。下面选项中描述错误的是 (D)

A.自评估是由信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估

B.检查评估是指信息系统上级管理部门组织的国家有关职能部门依法开展的风险评估

C.信息安全风险评估应以自评估为主,自评估和检查评估相互结合、互为补充

D.自评估和检查评估是相互排斥的,单位应慎重地从两种工作形式选择一个,并坚持

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 A2 其中资产 A1 面临两个主要威胁,威胁 T1 和威胁 T2 而资产 A2 面临个主要威胁,威胁『39 威胁 T1 可以利用的资产 A1 存在的两个脆弱性;脆弱性 V 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 存在的两个脆弱性;脆弱性 Vδ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 (C)

A.2

B.3

C.5
D.6

59、在信息安全管理体系的实施过程中,管理者的作用对于信息安全管理体系能否成功实施非常重要,但是以下选项中不属于管理者应有职责的是 (D)

A.制定并颁布信息安全方针,为组织的信息安全管理体系建设指明方向并提供总体纲领,明确总体要求
B.确保组织的信息安全管理体系目标和相应的计划得以制定,目标应明确、可度量,计划应具体、可实施
C.向组织传达满足信息安全的重要性,传达满足信息安全要求、达成信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性
D.建立健全信息安全制度,明确安全风险管理作用,实施信息安全风险评估过程,确保信息安全风险评估技术选择合理、计算正确

60、信息安全管理体系(nformation Security Management System,ISMS)的内部审核和管理审核是两项重要的管理活动。关于这两者,下面描述错误的是 (C)

A.内部审核和管理审评都很重要,都是促进 ISMS 持续改进的重要动力,也都应当按照一定的周期实施
B.内部审核的实施方式多采用文件审核和现场审核的形式,而管理评审的实施方式多采用召开管理审评会议的形式进行
C.内部审核的实施主体由组织内部的 ISMS 内审小组,而管理评审的实施主体是由国家政策指定的第三方技术服务机构
D.组织的信息安全方针、信息安全目标和有关 ISMS 文件等,在内部审核中作为审核准使用,但在管理评审中,这些文件是被审对象

61、随着信息安全涉及的范围越来越广,各个组织对信息安全管理的需求越来越迫切,越来越多的组织开始尝试使用参考 lS27001 介绍的 ISMS 来实施信息安全管理体系,提高组织的信息安全管理能力。关于 ISMS,下面描述错误的是 (A)

A.在组织中,应有信息技术责任部门(如信息中心)制定并颁布信息安全方针,为组织的 ISMS 建设指明方向并提供总体纲领,明确总体要求
B.组织的管理层应确保 ISMS 目标和相应的计划得以制定,信息安全管理目标应明确、可度量,风险管理计划应具体、具备可行性
C.组织的信息安全目标、信息安全方针和要求应传达到全组织范围内,应包括全体员工,同时也应传达客户、合作伙伴和供应商等外部各方
D.组织的管理层应全面了解组织所面临的信息安全风险,决定风险可接受级别和风险可接受准则,并确认接受和相关残余风险

62、在风险管理中,残余风险是指在实施了新的或增强的安全措施后还剩下的风险,关于残余风险,下面描述错误的是 (D)

A.风险处理措施确定以后,应编制详细的残余风险清单,并获得管理层对残余风险的书面批准,这也是风险管理中的一个重要过程
B.管理层确认接受残余风险,是对风险评估工作的一种肯定,表示管理层已经全面了解了组织
所面临的风险,并理解在风险一旦变为现实后,组织能够且必须承担引发的后果
C.接受残余风险,则表明没有必要防范和加固所有的安全漏洞,也没有必要无限制地提高安全保护措施的强度,对安全保护措施的选择要考虑到成本和技术的等因素的限制
D.如果残余风险没有降低到可接受的级别,则只能被动地选择接受风险,即对风险不采取进一步的处理措施,接受风险可能带来的结果

63、GB T22080-2008《信息技术安全技术信息安全管理体系要求》指出,建立信息安全管理体系应参照 PDCA 模型进行,即信息安全管理体系应包括建立 ISMS、实施和运行 SMS、监视和评审 ISMS、保持和改进 ISMS 等过程,并在这些过程中应实施若干活动。请选出以下描述错误的选项(D)

A.“制定 ISMS 方针”是建立 ISMS 阶段工作内容
B.“实施培训和意识教育计划”是实施和运行 ISMS 阶段工作内容
C.“进行有效性测量”是监视和评审 ISMS 阶段工作内容
D.“实施内部审核”是保持和改进 ISMS 阶段工作内容

64、若一个组织声称自己的 ISMS 符合 SO/EC27001 或 GBT22080 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,不包括哪一项(D)
A.信息安全方针、信息安全组织、资产管理
B.人力资源安全、物力和环境安全、通信和操作管理
C.访问控制、信息系统获取、开发和维护、符合性
D.规划与建立 ISMS

65、信息安全组织的管理涉及内部组织和外部各方面两个控制目标,为了实现对组织内部信息安全的有效管理,应该实施常规的控制措施,不包括哪些选项(D)
A.信息安全的管理承诺、信息安全协调、信息安全职责的分配
B.信息处理设施的授权过程、保密性协议、与政府部门的联系
C.与特定利益集团的联系、信息安全的独立评审
D.与外部各方相关风险的识别、处理外部各方协议中的安全问题

66、若一个组织声称自己的 ISMS 符合 ISO 川 EC27001 或 GBT22080 标准要求,其信息安全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 (D)
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

67、应急响应时信息安全事件管理的重要内容之一。关于应急响应工作,下面描述错误的是 (C)
A.信息安全应急响应,通常是指一个组织为了应对各种安全意外事件的发生所采取的防范措施,既包括预防性措施,也包括事业发生后的应对措施
B.应急响应工作有其鲜明的特点:具体高技术复杂性与专业性、强突发性、对知识经验的高依赖性,以及需要广泛的协调与合作
C.应急响应时组织在处置应对突发/重大信息安全事件时的工作,其主要包括两部分工作:安全事件发生时正确指挥、事件发生后全面总结
D.应急响应工作的起源和相关机构的成立和 198 年 11 月发生的莫里斯蠕虫病毒事件有关,基于该事件,人们更加重视安全事件的应急处理和整体协调的重要性

68、我国依照信息系统的重要程度、安全事件造成的系统损失以及带来的社会影响等因素,将信息安全事件分为若干个级别,其中,能够对特别重要的信息系统产生特别严重影响或破坏的信息安全事件,如使特别重要信息系统遭受特别重大的系统损失,如造成系统大面积瘫痪,使其丧失业务处理能力,或系统关键数据的保密性、完整性、可用性遭到严重破坏的,应属于哪一级信息安全事件 (A)
A.I 级
B.皿级
C.W 级
D.特别级

69、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)

A.RTO 可以为 0,RPO 也可以为 0

B.RTO 可以为 0,RPO 不可以为

C.RT0 不可以为 0,RPO 可以为 0

D.RT0 不可以为 0,RPO 也不可以为 0

70、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(C)

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

71、关于信息安全保障技术框架(Information Assurance Tehnical Frameworkat-),下面描述错误的是 (A)

A.IATF 最初由美国国家安全局(NSA)发布,后来由国际标准化组织(IS0)转化为国际标准,供各个国家信息系统建设参考使用

B.IATF 是一个通用框架,可以用到多种应用场景中,通过对复杂信息系统进行解构和描述,然后再以此框架讨论信息系统的安全保护问题

C.IATF 提出了深度防御的战略思想,并提供一个框架进行多层保护,以此防范信息系统面临的各种威胁

D.强调人、技术和操作是深度防御的三个主要层面,也就是说讨论人在技术支持下运行维护的信息安全保障问题

72、关于信息安全保障技术框架(IATF)以下说法不正确的是 (D)

A.分层策略允许在适当的时候采用低安全级保障解决方案以便降低信息安全保障的成本

B.IATF 从人、技术和操作三个层面提供一个框架实施多层保护,使攻击者即使攻破一层也无法破坏整个信息基础设施

C.允许在关键区域(例如区域边界)使用高安全级保障解决方案,确保系统安全性

D.IATF 深度防御战略要求在网络体系结构的各个可能位置实现所有信息安全保障机制

73、2003 年以来,我国高度重视信息安全保障工作,先后制定并发布了多个文件,从政策层面为开展并推进信息安全保障工作进行了规划。下面选项中哪个不是我国发布的文件 (B)

A.《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)

B.《国家网络安全综合计划(CNCI)》(国令[2008]54 号)

C.《国家信息安全战略报告》(国信[2005]2 号)

D.《关于大力推进信息化发展和切实保障信息安全的若干意见》(国发[2012123 号)

74、在信息安全保障工作中,人才是非常重要的因素,近年来,我国一直高度重视我国信息安全人才队伍的培养和建设。在以下关于我国关于人才培养工作的描述中,错误的是 (C)

A.在《国家信息化领导小组关于加强信息安全保障工作的意见》仲办发[2003]27 号)中,针对信息安全人才建设与培养工作提出了“加快新鲜全人才培养,增强全民信息安全意识”的指导精神

B.2015 年,为加快网络空间安全高层次人才培养,经报国务院学位委员会批准,国务院学位委员会、教育部决

定在“工学”门类下增设“网络空间安全”一级学科,这对于我国网络信息安全人才成体系化、规模化、系统化培养起到积极的推动作用

C.经过十余年的发展,我国信息安全人才培养已经成熟和体系化,每年培养的信息安全从业人员的数量较多,基本能同社会实际需求相匹配;同时,高校信息安全专业毕业人才的综合能力要求高、知识更全面,因而社会化培养应重点放在非安全专业人才培养上

D.除正规大学教育外,我国信息安全人才非学历教育已基本形成了以各种认证为核心,辅以各种职业技能培训的信息安全人才培训体系,包括“注册信息安全专业人员(CISP)”资质认证和一些大型企业的信息安全资质认证

75、2008 年 1 月 2 日,美国发布第 54 号总统令,建立国家网络安全综合计划(ComprehensiveNational Cybersecurity Initative,CNcI)。CNCI 计划建立三道防线:第一道防线,减少漏洞和隐患,预防入侵;第二道防线,全面应对各类威胁;第三道防线,强化未来安全环境。从以上内容,我们可以看出以下哪种分析是正确的:(A)

A.CNCI 是以风险为核心,三道防线首要的任务是降低其网络所面临的风险

B.从 CNCI 可以看出,威胁主要是来自外部的,而漏洞和隐患主要是存在于内部的

C.CNCI 的目的是尽快研发并部署新技术和彻底改变其糟糕的网络安全现状,而不是在现在的网络基础上修修补补

D.CNCI 彻底改变了以往的美国信息安全战略,不再把关键基础设施视为信息安全保障重点,而是追求所有网络和系统的全面安全保障

76、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)

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,所部属的加密针对性不足,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

77、为保障信息系统的安全,某经营公共服务系统的公司准备并编制一份针对性的信息安全保障方案,并将编制任务交给了小王,为此,小王决定首先编制出一份信息安全需求报告。关于此项工作,下面说法错误的是(D)

A.信息安全需求是安全方案设计和安全措施的依据

B.信息安全需求应当是从信息系统所有者(用户)的角度出发,使用规范化、结构化的语言来描述信息系统安全保障需求

C.信息安全需求应当基于信息安全风险评估结果、业务需求和有关政策法规和标准的合规性要求得到

D.信息安全需求来自于该公众服务信息系统的功能设计方案

78、从系统工程的角度来处理信息安全问题,以下说法错误的是: (C)

A.系统安全工程旨在了解企业存在的安全风险,建立一组平衡的安全需求,融合各种工程学科的努力将此安全需求转换为贯穿系统整个生存期的工程实施指南

B.系统安全工程需对安全机制的正确性和有效性做出诠释,证明安全系统的信任度能够达到企业的要求,或系统遗留的安全薄弱性在可容许范围之内

C.系统安全工程能力成熟度模型(SSE-CMM)是一种衡量安全工程实践能力的方法,是一种使用面向开发的方法

D.系统安全工程能力成熟度模型(SSE-CMD 是在原有能力成熟度模型(CM 的基础上。通过对安全工作过程进行管理的途径,将系统安全工程转变为一个完好定义的、成熟的、可测量的先进学科

79、某项目的主要内容为建造 A 类机房,监理单位需要根据《电子信息系统机房设计规范》(GB50174-2008)的相关要求,对承建单位的施工设计方案进行审核,以下关于监理单位给出的审核意见错误的是 (D)

A.在异地建立备份机房,设计时应与主要机房等级相同
B.由于高端小型机发热量大,因此采用活动地板下送风,上回风的方式
C.因机房属于 A 级主机房,因此设计方案中应考虑配备柴油发电机,当市电发生故障时所配备的柴油发电机应能承担全部负荷的需要
D.A 级主机房应设置自动喷水灭火系统

80、某公司建设面向内部员工的办公自动化系统和面向外部客户的营销系统,通过公开招标选择 M 公司为实施单位,并选择了 H 监理公司承担该项目的全程监理工作。目前,各个应用系统均已完成开发,M 公司已经提交了验收申请。监理公司需要对 M 公司提交的软件配置文件进行审查,在以下所提交的文档中,哪一项属于开发类文档:(D)
A.项目计划书
B.质量控制计划
C.评审报告
D.需求说明书

81、有关系统安全工程-能力成熟度模型(SEE-CMM)中的基本实施(Base Practices,BP),正确的理解是:(A)
A.BP 不限定于特定的方法或工具,不同的业务背景中可以使用不同的方法
B.BP 不是根据广泛的现有资料、实践和专家意见综合得出的
C.BP 不代表信息安全工程领域的最佳实践
D.BP 不是过程区域(Process Areas,PA)的强制项

82、在使用系统安全工程-能力成熟度模型(SSE-CMM)对一个组织的安全工程能力成熟度进行测量时,有关测量结果,错误的理解是(B)
A.如果该组织在执行某个特定的过程区域时具备某一个特定级别的部分公共特征时,则这个组织在这个过程区域的能力成熟度未达到此级
B.如果该组织某个过程区域(Process Areas,PA)具备了“定义标准过程”、“执行已定义的过程”两个公共特征,则过程区域的能力成熟度级别达到 3 级“充分定义级”
C.如果某个过程区域(Process Areas,PA)包含 4 个基本实施(Base Practices,BP),执行此 PA 时执了 3 个 BP,则此过程区域的能力成熟度级别为 0
D.组织在不同的过程区域的能力成熟度可能处于不同的级别上

83、从历史演进来看,信息安全的发展经历了多个阶段。其中,有一个阶段的特点是:网络信息系统逐步形成,信息安全注重保护信息在存储、处理和传输过程中免受非授权的访问,开始使用防火墙、防病毒 PKI 和 VPN 等安全产品。这个阶段是 (C)
A.通信安全阶段
B.计算机安全阶
C.信息系统安全阶段
D.信息安全保障阶段

84、下面关于信息系统安全保障模型的说法不正确的是 (D)
A.国家标准《信息系统安全保障评估框架第一部分:简介和一般模型》(GB/T20274.1 2006)中的信息系统安全保障模型将风险和策略作为基础和核心
B.模型中的信息系统生命周期模型是抽象的概念性说明模型,在信息系统安全保障具体操作时,可根据具体环境和要求进行改动和细化
C.信息系统安全保障强调的是动态持续性的长效安全,而不仅是某时间点下的安全
D.信息系统安全保障主要是确保信息系统的保密性、完整性和可用性,单位对信息系统运行维护和使用的人员在能力和培训方面不需要投入

85、《信息安全保障技术框架》(Information Assurance Technical Framework,IATF)是由哪个下面哪个国家发布的(B)

A 中国

B.美国

C.俄罗斯

D.欧盟

86、我国信息安全保障工作先后经历了启动、逐步展开和积极推进,以及深化落实三个阶段,我国信息安全保障各阶段说法不正确的是 (C)

A.2001 年,国家信息化领导小组重组,网络与信息安全协调小组成立,我国信息安全保障工作正式启动

B 2003 年 7 月,国家信息化领导小组制定出台了《关于加强信息安全保障工作的意见》(中办发 27 号文件),明确了“积极防御、综合防范”的国家信息安全保障工作方针

C.2003 年,中办发 27 号文件的发布标志着我国信息安全保障进入深化落实阶段

D.在深化落实阶段,信息安全法律法规、标准化,信息安全基础设施建设,以及信息安全等级保护和风险评估取得了新进展

87、我国信息安全保障建设包括信息安全组织与管理体制、基础设施、技术体系等方面,以下关于信息安全保障建设主要工作内容说法不正确的是 (C)

A.健全国家信息安全组织与管理体制机制,加强信息安全工作的组织保障

B.建设信息安全基础设施,提供国家信息安全保障能力支撑

C.建立信息安全技术体系,实现国家信息化发展的自主创新

D.建立信息安全人才培养体系,加快信息安全科学建设和信息安全人才培养

88、某银行信息系统为了满足业务发展的需要准备进行升级改造,以下哪一项不是此次改造中信息系统安全需求分析过程需要考虑的主要因素 (C)

A.信息系统安全必须遵循的相关法律法规,国家以及金融行业安全标

B.信息系统所承载该银行业务正常运行的安全需求

C.消除或降低该银行信息系统面临的所有安全风险

D.该银行整体安全策略

89.信息安全测评是指依据相关标准,从安全功能等角度对信息技术产品、信息系统、服务提供商以及人员进行测试和评估,以下关于信息安全测评说法不正确的是(B)

A.信息产品安全评估是测评机构对产品的安全性做出的独立评价,增强用户对已评估产品安全的信任

B.目前我国常见的信息系统安全测评包括信息系统风险评估和信息系统安全保障测评两种类型

C.信息安全工程能力评估是对信息安全服务提供者的资格状况、技术实力和实施服务过程质量保证能力的具体衡量和评价

D.信息系统风险评估是系统地分析网络与信息系统所面临的威胁及其存在的脆弱性,评估安全事件可能造成的危害程度,提出有针对性的安全防护策略和整改措施

90、美国的关键信息基础设施(critical nformation nfrastructure,CI)包括商用核设施、政府设施、交通系统、饮用水和废水处理系统、公共健康和医疗、能源、银行和金融、国防工业基地等等,美国政府强调重点保障这些基础设施信息安全,其主要原因不包括(C)

A.这些行业都关系到国计民生,对经济运行和国家安全影响深远

B.这些行业都是信息化应用广泛的领域

C.这些行业信息系统普遍存在安全隐患,而且信息安全专业人士缺乏的现象比其他行业更突出

D.这些行业发生信息安全事件,会造成广泛而严重的损失

91、在设计信息系统安全保障方案时,以下哪个做法是错误的 (C)

A.要充分切合信息安全需求并且实际可行
B.要充分考虑成本效益,在满足合规性要求和风险处置要求的前提下,尽量控制成本
C.要充分采取新技术,在使用过程中不断完善成熟,精益求精,实现技术投入保值要求
D.要充分考虑用户管理和文化的可接受性,减少系统方案实施障碍

92、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 (C)
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

93、某单位系统管理员对组织内核心资源的访问制定访问策略,针对每个用户指明能够访问的资源,对于不在指定资源列表中的对象不允许访问。该访问控制策略属于以下哪一种: (C)
A.强制访问控制:BLP BIBA CLARK-WILSON CHINESE-WALL
B.基于角色的访问控制:RBAC
C.自主访问控制: ACL CL
D.基于任务的访问控制

94、主体和客体是访问控制模型中常用的概念。下面描述种错误的是 (C)
A.主体是访问的发起者,是一个主动的实体,可以操作被动实体的相关信息或数据
B.客体也是一种实体,是操作的对象,是被规定需要保护的资源
C.主体是动作的实施者,比如人、进程或设备等均是主体,这些对象不能被当作客体使用
D.一个主体为了完成任务,可以创建另外的主体,这些主体可以独立运行

95、以下场景描述了基于角色的访问控制模型(Role- based Access control,RBAC)F 根据组织的业务要求或管理要求,在业务系统中设置若干岗位、职位或分工。管理员负责将权限(不同类别和级别的)分别赋予承担不同工作职责的用户。关于 RBAC 模型,下列说法错误的是 (D)
A.当用户请求访问某资源时,如果其操作权限不再用户当前被激活角色的授权范围内,访问请
求将被拒绝
B.业务系统中的岗位、职位或者分工,可对应 RBAC 模型中的角色
C.通过角色,可实现对信息资源访问的控制
D.RBAC 模型不能实现多级安全中的访问控制

96、自主访问控制模型(DAC)的访问控制关系可以用访问控制(ACL)来表示,该 ACL 利用在客体上附加一个主体明细表的方法来表示访问控制矩阵,通常使用由客体指向的链表来存储相关数据。下面选项中说法正确的是(D)
A.ACL 是 Bell- Lapadula 模型的一种具体实现
B.ACL 在删除用户时,去除该用户所有的访问权限比较方便
C.ACL 对于统计某个主体能访问哪些客体比较方便
D.ACL 在增加客体时,增加相关的访问控制权限较为简单

97、关于 Kerberos 认证协议,以下说法错误的是 (C)
A.只要用户拿到了认证服务器(AS)发送的票据许可票据(TGT)并且该 TGT 没有过期,就可以使用该 TGT 通过票据授权服务器(TGS)完成到任一个服务器的认证而不必重新输入密码
B.认证服务器(AS)和票据授权服务器(TGS)是集中式管理,容易形成瓶颈,系统的性能和安全也严重依赖于 AS 和 TS 的性能和安全

C.该协议通过用户获得票据许可票据、用户获得服务许可票据、用户获得服务三个阶段,仅支持服务器对用户的单向认证
D.该协议是一种基于对称密码算法的网络认证协议,随用户数量增加,密钥管理较复杂

98、传输控制协议(TCP)是传输层协议,以下关于 TCP 协议的说法,哪个是正确的?
(D)
A.相比传输层的另外一个协议 UDP,TCP 既提供传输可靠性,还同时具有更高的效率,因此具有广泛的用途
B.TCP 协议包头中包含了源 IP 地址和目的 IP 地址,因此 TCP 协议负责将数据传送到正确的主机
C.TCP 协议具有流量控制、数据校验、超时重发、接收确认等机制,因此 TCP 协议能完全替代 IP 协议
D.TCP 协议虽然高可靠,但是相比 UDP 协议机制过于复杂,传输效率要比 UDP 低

99、以下关于 UDP 协议的说法,哪个是错误的? (D)
A.UDP 具有简单高效的特点,常被攻击者用来实施流量型拒绝服务攻击
B.UDP 协议包头中包含了源端口号和目的端口号,因此 UDP 可通过端口号将数据包送达正确的程序
C.相比 TCP 协议,UDP 协议的系统开销更小,因此常用来传送如视频这一类高流量需求的应用数据
D.UDP 协议不仅具有流量控制,超时重发机制,还能提供加密等服务,因此常用来传输如视频会话这类需要隐私保护的数据

100、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 (C)
A. PP2P
B.L2TP
C. SSL
D. IPSEC

101、防火墙是网络信息系统建设中常常采用的一类产品,它在内外网隔离方面的作用是 (C)**。**
A.既能物理隔离,又能逻辑隔离
B.能物理隔离,但不能逻辑隔离
C.不能物理隔离,但是能逻辑隔离
D.不能物理隔离,也不能逻辑隔离

102、异常入侵检测系统常用的一种技术,它是识别系统或用户的非正常行为或者对于计算机资源的非正常使用,从而检测出入侵行为。下面说法错误的是 (B)
A.在异常入侵检测中,观察到的不是已知的入侵行为,而是系统运行过程中的异常现象
B.异常入侵检测,是将当前获取行为数据和已知入侵攻击行为特征相比较,若匹配则认为有攻击发生
C.异常入侵检测可以通过获得的网络运行状态数据,判断其中是否含有攻击的企图,并通过多种手段向管理员报警
D.异常入侵检测不但可以发现从外部的攻击,也可以发现内部的恶意行为

103、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,通过专用进行互联互通。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:(C)
A.总部使用服务器、用户终端统一使用 10.0.1.x、各分支机构服务和用户终端使用 192.168.2.x192.168.20.x
B.总部使用服务器使用 10.0.1.111、用户终端使用 10.0.1.12212,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

104、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 (C)

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

105、张主任的计算机使用 Windows7 操作系统,他常登陆的用户名为 zhang,张主任给他个人文件夹设置了权限为只有 zhang 这个用户有权访问这个目录,管理员在某次维护中无意将 zhang 这个用户删除了,随后又重新建了一个用户名为 zhang,张主任使用 zhang 这个用户登录系统后,发现无法访问他原来的个人文件夹,原因是(A)

A.任何一个新建用户都需要经过授权才能访问系统中的文件

B. Windows7 不认为新建立的用户 zhang 与原来的用户 zhang 是同一个用户,因此无权访

C.用户被删除后,该用户创建的文件夹也会自动删除,新建用户找不到原来用户的文件夹,因此无法访问

D.新建的用户 zhang 会继承原来用户的权限,之所以无权访问是因为文件夹经过了加密

106、以下关于 Windows 系统的账号存储管理机制(Security Accounts Manager)的说法哪个是正确的 (D)

A.存储在注册表中的账号数据是管理员组用户都可以访问,具有较高的安全性

B.存储在注册表中的账号数据只有 administrator 账户才有权访问,具有较高的安全性

C.存储在注册表中的账号数据任何用户都可以直接访问,灵活方便

D.存储在注册表中的账号数据有只有 System 账户才能访问,具有较高的安全性

107、口令破解是针对系统进行攻击的常用方法, Windows 系统安全策略中应对口令破解的策略主要是账户策略中的账户锁定策略和密码策略,关于这两个策略说明错误的是 (D)

A.密码策略的主要作用是通过策略避免用户生成弱口令及对用户的口令使用进行管控

B.密码策略对系统中所有的用户都有效

C.账户锁定策略的主要作用是应对口令暴力破解攻击,能有效的保护所有系统用户被口令暴力破解攻击

D.账户锁定策略只适用于普通用户,无法保护管理员 administrator 账户应对口令暴力破解攻击

108、 Windows 文件系统权限管理访问控制列表(Access Control List,ACL)机制,以下哪个说法是错误的 (C)

A.安装 Windows 系统时要确保文件格式使用的是 NTFS,因为 Windows 的 ACL 机制需要 NTFS 文件格式的支持

B.由于 Windows 操作系统自身有大量的文件和目录,因此很难对每个文件和目录设置严格的访问权限,为了使用上的便利, Windows 上的 ACL 存在默认设置安全性不高的问题

C. Windows 的 ACL 机制中,文件和文件夹的权限是与主体进行关联的,即文件夹和文件的访问权限信息是写在用户数据库中

D.由于 ACL 具有很好的灵活性,在实际使用中可以为每一个文件设定独立用户的权限

109、由于发生了一起针对服务器的口令暴力破解攻击,管理员决定对设置账户锁定策略以对抗口令暴力破解。他设置了以下账户锁定策略如下:复位账户锁定计数器 5 分钟账户锁定时间 10 分钟账户锁定阈值 3 次无效登录以下关于以上策略设置后的说法哪个是正确的 (B)

A.设置账户锁定策略后,攻击者无法再进行口令暴力破解,所有输错了密码的用户就会被锁住

B.如果正常用户不小心输错了 3 次密码,那么该账户就会被锁定 10 分钟,10 分钟内即使输入正确的密码,也无法登录系统

C.如果正常用户不小心连接输入错误密码 3 次,那么该用户账户就被锁定 5 分钟,5 分钟内即使提交了正确的密码,也无法登录系统

D.攻击者在进行口令破解时,只要连续输错 3 次密码,该账户就被锁定 10 分钟,而正常用户登陆不受影响

110、某 Linux 系统由于 root 口令过于简单,被攻击者猜解后获得了 root 口令,发现被攻击后,管理员更改了 root 口令,并请安全专家对系统进行检测,在系统中发现有一个文件的权限如下-r-s-X-x1 test test 10704 Apr 15 2002 /home/test/sh 请问以下描述哪个是正确的:(C)
A.该文件是一个正常文件,是 test 用户使用的 shell1,test 不能读该文件,只能执行
B.该文件是一个正常文件,是 test 用户使用的 shel1,但 test 用户无权执行该文件
C.该文件是一个后门程序,该文件被执行时,运行身份是 root,test 用户间接获得了 root 权限
D.该文件是一个后门程序,可由于所有者是 test,因此运行这个文件时文件执行权限为 test

111、加密文件系统(Encrypting File System,EFS)是 Windows 操作系统的一个组件。以下说法错误的是 (C)
A.EFS 采用加密算法实现透明的文件加密和解密,任何不拥有合适密钥的个人或者程序都不能加密数据
B.EFS 以公钥加密为基础,并利用了 Windows 系统中的 Cryptoapi 体系结构
C.EFS 加密系统适用于 NTFS 文件系统和 FAT32 文件系统(Windows7 环境下)
D.EFS 加密过程对用户透明,ES 加密的用户验证过程是在登录 Windows 时进行

112、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据库的安全。以下关于数据库常用的安全策略理解不正确的是: (B)
A.最小特权原则,是让用户可以合法的存取或修改数据库的前提下,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,最大程度也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

113、数据在进行传输前,需要由协议機自上而下对数据进行封装。TCP/IP 协议中,数据封装的顺序是:(B)
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

114、以下关于 SMTP 和 POP3 协议的说法那个是错误的 (D)
A.SMTP 和 POP3 协议是一种基于 ASCI 编码的请求/响应模式的协议
B.SMTP 和 POP3 协议明文传输数据,因此存在数据泄露的可能
C.SMP 和 POP3 协议缺乏严格的用户认证,因此导致了垃圾邮件问题
D.SMTP 和 POP3 协议由于协议简单,易用性更高,更容易实现远程管理邮件

115、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)
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 Active 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

116、应用安全,一般是指保障应用程序使用过程和结果的安全,以下内容中不属于应用安全防护考虑的是 (D)
A.身份鉴别,应用系统应对登陆的用户进行身份鉴别,只有通过验证的用户才能访问应用系统资源
B.安全标记,在应用系统层面对主体和客体进行标记,主体不能随意更改权限,增加访问控制的力度,限制非法访问
C.剩余信息保护,应用系统应加强硬盘、内存或缓冲区中剩余信息的保护,防止存储在硬盘、内存或缓冲区中的信息被非授权的访问

D 机房与设施安全,保证应用系统处于有一个安全的环境条件,包括机房环境、机房安全等级、机房的建造和机房的装修等

117、下面对信息安全漏洞的理解中,错误的是 (B)

A.讨论漏洞应该从生命周期的角度出发,信息产品和信息系统在需求、设计、实现、配置、维护和使用等阶段中均有可能产生漏洞

B.信息安全漏洞是由于信息产品和信息系统在需求、设计、开发、部署或维护阶段,由于设计、开发等相关人员无意中产生的缺陷所造成的

C.信息安全漏洞如果被恶意攻击者成功利用,可能会给信息产品和信息系统带来安全损害,甚至带来很大的经济损失

D.由于人类思维能力、计算机计算能力的局限性等因素,所以在信息产品和信息系统中产生信息安全漏洞是不可避免的

118、某单位发生的管理员小张在繁忙的工作中接到了一个电话,来电者:小张吗?我是科技处李强,我的邮箱密码忘记了,现在打不开邮件,我着急收个邮件,麻烦你先帮我把密码改成 123,我收完邮件自己修改掉密码。热心的小张很快的满足了来电者的要求。随后李强发现有向系统登录异常。请问以下说法哪个是正确的? (C)

A.小张服务态度不好,如果把李强的邮件收下来亲自教给李强就不会发生这个问题

B.事件属于服务器故障,是偶然事件,影响单位领导申请购买新的服务器

C.单位缺乏良好的密码修改操作流程或者小张没按操作流程工作

D.事件属于邮件系统故障,是偶然事件,应向单位领导申请升级邮件服务软件

119、某网站管理员小邓在流量监测中发现近期网站的入站 ICMP 流量上升了 250%,尽管网站没有发现任何的性能下降或其他问题,但为了安全起见,他仍然向主管领导提出了应对措施,作为主管负责人,请选择有效的针对此问题的应对措施 (A)

A.在防火墙上设置策略,组织所有的 ICMP 流量进入(关掉 ping)

B.删除服务器上的 ping.exe 程序

C.增加带宽以应对可能的拒绝服务攻击

D.增加网站服务器以应对即将来临的拒绝服务攻击

120、某单位计划在今年开发一套办公自化(OA)系统,将集团公司各地的机构通过互联网进行协同办公,在 OA 系统的设计方案评审会上,提出了不少安全开发的建议,作为安全专家,请指出大家提供的建议中不太合适的一条 (C)

A.对软件开发商提出安全相关要求,确保软件开发商对安全足够的重视,投入资源解决软件安全问题

B.要求软件开发人员进行安全开发培训,是开发人员掌握基本软件安全开发知识

C.要求软件开发商使用 Java 而不是 ASP 作为开发语言,避免产生 SQL 注入漏洞

D.要求软件开发商对软件进行模块化设计,各模块明确输入和输出数据格式,并在使用前对输入数据进行校验

121、某软件公司准备提高其开发软件的安全性,在公司内部发起了有关软件开发生命周期的讨论,在下面的发言观点中,正确的是 (B)

A.软件安全开发生命周期较长、阶段较多,而其中最重要的是要在软件的编码阶段做好安全措施就可以解决 90%以上的安全问题

B.应当尽早在软件开发的需求和设计阶段就增加一定的安全措施,这样可以比在软件发布以后进行漏洞修复所花的代价少得多

C.和传统的软件开发阶段相比,微软提出的安全开发生命周期(Security Development Lifecycle,SDL)的最大特点是增加了一个专门的安全编码阶段

D.软件的安全测试也很重要,考虑到程序员的专业性,如果该开发人员已经对软件进行了安全性测试,就没有

必要在组织第三方进行安全性测试

122、下面有关软件安全问题的描述中,哪项应是由于软件设计缺陷引起的 (C)

A.设计了三层 WEB 架构,但是软件存在 SQL 注入漏洞,导致被黑客攻击后直接访问数据库

B.使用 C 语言开发时,采用了一些存在安全问题的字符串处理函数,导致存在缓冲区溢出漏洞

C.设计了缓存用户隐私数据机制以加快系统处理性能,导致软件在发布运行后,被黑客攻击获取到用户隐私数据

D.使用了符合要求的密码算法,但在使用算法接口时,没有按照要求生成密钥,导致黑客攻击后能破解并得到明文数据

123、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发日志共享,有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,根据降低攻击面的原则,应采取哪项处理措施 (D)

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,对日志共享设置访问密码且限定访问的时间

124、针对软件的拒绝服务攻击是通过消耗系统资源是软件无法响应正常请求的一种攻击方式,在软件开发时分析拒绝服务攻击的威胁,以下哪个不是需要考虑的攻击方式: (D)

A.攻击者利用软件存在逻辑错误,通过发送某种类型数据导致运算进入死循环,CPU 资源占用始终 100%

B.攻击者利用软件脚本使用多重嵌套查询,在数据最大时会导致查询效率低,通过发送大量的查询导致数据库响应缓慢

C.攻击者利用软件不自动释放连接的问题,通过发送大量连接消耗软件并发连接数,导致并发连接数耗尽而无法访问

D.攻击者买通了 IDC 人员,将某软件运行服务器的网线拔掉导致无法访问

125、最小特权是软件安全设计的基本原则,某应用程序在设计时,设计人员给出了以下四种策略,其中有一个违反了最小特权的原则,作为评审专家,请指出是哪一个?(D)

A.软件在 Alinux 下按照时,设定运行时使用 nobody 用户运行实例

B.软件的日志备份模块由于需要备份所有数据库数据,在备份模块运行时,以数据库备份操作员账号连接数据库

C.软件的日志模块由于要向数据库中的日志表中写入日志信息,使用了一个日志用户账号连接数据库,该账号仅对日志表拥有权限

D.为了保证软件在 Windows 下能稳定的运行,设定运行权限为 system,确保系统运行正常,不会因为权限不足产生运行错误

126、某网站为了开发的便利,使用 SA 连接数据库,由于网站脚本中被发现存在 SQL 注入漏洞,导致攻击者利用内置存储过程 cmd shell 删除了系统中一个重要文件,在进行问题分析时,作为安全专家,你应该指出该网站设计违反了以下哪项原则: (B)

A.权限分离原贝

B.最小特权原则

C.保护最薄弱环节的原则

D.纵深防御的原则

127、微软提出了 STRIDE(6 种威胁) 三模型,其中,R 是 Repudiation(抵赖)的缩写,关于此项安全要求,下面描述错误的是(C)

A.某用户在登录系统并下载数据后,却声称“我没有下载过数据”,软件系统中的这种威胁就属于 R 威胁

B.解决 R 威胁,可以选择使用抗抵赖性服务技术来解决,如强认证、数字签名、安全审计等技术措施
C.R 威胁是 STRIDE 六种威胁中第三严重的威胁,比 D 威胁和 E 威胁的严重程度更高
D.解决 R 威胁,也应按照确定建模对象、识别威胁、评估威胁以及消减威胁等四个步骤来进行

128、关于信息安全管理,下面理解片面的是 (C)
A.信息安全管理是组织整体管理的重要、固有组成部分,它是组织实现其业务目标的重要保障
B.信息安全管理是一个不断演进、循环发展的动态过程,不是一成不变的
C.在信息安全建设中,技术是基础,管理是拔高,及有效的管理依赖于良好的技术基础
D.坚持管理与技术并重的原则,是我国加强信息安全保障工作的主要原则之一

129、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有效地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。(B)
A.信息安全管理体系(ISMS
B.信息安全等级保护
C. NIST SP800 系列
D. ISO270000 系列

130、小王是某大学计算科学与技术专业的毕业生,大四上学期开始找工作,期望谋求一份技术管理的职位一次面试中,某公司的技术经理让小王读一读信息安全风险管理中的背景建立”的基本概念与认识。小明的主要观点包括:(1)背景建立的目的是为了明确信息安全风险管理的范围和对象,以及对象的特性和安全要求,完成信息安全风险管理项目的规划和准备(2)背景建立根据组织机构相关的行业经验执行,雄厚的经验有助于达到事半功倍的效果;(3)背景建立包括:风险管理准备、信息系统调查、信息系统分析和信息安全分析;(4)背景建立的阶段性成果包括:风险管理计划书、信息系统的描述报告、信息系统的分析报告、信息系统的安全要求报告。请问小王的论点中错误的是哪项: (B)
A.第一个观点,背景建立的目的只是为了明确信息安全风险管理的范围和对象
B.第二个观点,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
C.第三个观点,背景建立中的信息系统调查与信息系统分析是同一件事的两个不同名字
D.第四个观点,背景建立的阶段性成果中不包括有风险管理计划书

131、关于风险要素识别阶段工作内容叙述错误的是 (D)
A.资产识别是指对需要保护的资产和系统等进行识别和分类
B.威胁识别是指识别与每项资产相关的可能威胁和漏洞及其发生的可能性
C.脆弱性识别以资产为核心,针对每一项需要保护的资产,识别可能被威胁利用的弱点,并对脆弱性的严重程度进行评估
D.确认已有的安全措施仅属于技术层面的工作,牵涉到具体方面包括:物理平台、系统平台、网络平台和应用平台

132、某单位的信息安全主管部门在学习我国有关信息安全的政策和文件后,认识到信息安全风险评估分为自评估和检查评估两种形式。该部门将有关检查评估的特点和要求整理成如下四条报告给单位领导,其中描述错误的是 (B)
A.检查评估可依据相关标准的要求,实施完整的风险评估过程;也可在自评估的基础上,对关键环节或重点内容实施抽样评估
B.检查评估可以由上级管理部门组织,也可以由本级单位发起,其重点是针对存在的问题进行检查和评测
C.检查评估可以由上级管理部门组织,并委托有资质的第三方技术机构实施
D.检查评估是通过行政手段加强信息安全管理的重要措施,具有强制性的特点

133、规范的实施流程和文档管理,是信息安全风险评估性能否取得成果的重要基础。按照规范的风险评估实施流程,下面哪个文档应当是风险要素识别阶段的输出成果(B)

A.《风险评估方案》
B.《需要保护的资产清单》
C.《风险计算报告》
D.《风险程度等级列表》

134、关于业务连续性计划(BCP)以下说法最恰当的是 (B)
A.组织为避所有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
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,减少信息系统风险而建立的一个控制过程

135、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 PDCER-应急响应方法这些工作应处于以下哪个阶段(D)
A.准备阶段
B.检测阶段
C.遏制阶段
D.根除阶段

136、关于信息安全事件管理和应急响应,以下说法错误的是(B)
A.应急响应是指组织为了应对突发/重大信息安全事件的发生所做的准备,以及在事件发生后所采取的措施
B.应急响应方法,将应急响应管理过程分为遏制、根除、处置、恢复、报告和跟踪 6 个阶段
C.对信息安全事件的分级主要参考信息系统的重要程度、系统损失和社会影响三方面因素
D.根据信息安全事件的分级参考要素,可将信息安全事件划分为 4 个级别:特别重大事件(I 级)、重大事件(II 级)、较大事件(III 级)和一般事件(IV 级)

137、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(D)
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

138、恢复时间目标(RTO)和恢复点目标(RPO)是信息系统灾难恢复中的重要概念,关于这两个值能否为零,正确的选项是 (A)
A.RTO 可以为 0,RPO 也可以为 0
B.RTO 可以为 0,RPO 不可以为
C.RTO 不可以为 0,但 RPO 可以为 0
D.RTO 不可以为 0,RP0 也不可以为

139、以下关于灾难恢复和数据备份的理解,说法正确的是 (C)
A.增量备份是备份从上次完全备份后更新的全部数据文件
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.数据备份按数据类型划分可以划分为系统数据备份和用户数据备份
D.如果系统在一段时间内没有出现问题,就可以不用再进行容灾演练了

140、某政府机构拟建设一机房,在工程安全监理单位参与下制定了招标文件,项目分二期,一期目标为年底前实现系统上线运营;二期目标为次年上半年完成运行系统风险的处理;招标文件经管理层审批后发布。就此

工程项目而言,下列选项正确的是(C)

A.此项目将项目目标分解为系统上线运营和运行系统风险处理分期实施,具有合理性和可行性

B.在工程安全建理的参与下,确保了此招标文件的合理性

C、工程规划不符合信息安全工程的基本原则

D、招标文件经管理层审批,表明工程目标符合业务发展规划

141、对系统工程(Systems Engineering, SE)的理解,以下错误的是 (C)

A.系统工程偏重于对工程的组织与经营管理进行研究

B.系统工程不属于技术实现,而是一种方法论

C.系统工程不是一种对所有系统都具有普遍意义的科学方法

D.系统工程是组织管理系统规划、研究、制造、试验、使用的科学方法

142、系统工程的模型之一霍尔三维结构模型由时间维、逻辑维和知识维组成。有关此模型,错误的是 (C)

A.霍尔三维结构体系形象地描述了系统工程研究的框架

B.时间维表示系统工程活动从开始到结束按时间顺序排列的全过程

C.逻辑维的七个步骤与时间维的七个阶段严格对应,即时间维第一阶段应执行逻辑维第一步骤的活动,时间维第二阶段应执行逻辑维第二步骤的活动

D.知识维列举可能需要运用的工程、医学、建筑、商业、法律、管理、社会科学和艺术等各种知识和技能

143、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)

A.系统安全工程能力成熟度模型(SSE-CMD 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-CM)定义了 3 个风险过程:评价威胁,评价脆弱性,评价影响

D.SSE-CM 强调系统安全工程与其他工程学科的区别性和独立性

144、以下哪一项不是信息系统集成项目的特点 (B)

A.信息系统集成项目要以满足客户和用户的需求为根本出发点

B.系统集成就是选择最好的产品和技术,开发相应的软件和硬件,将其集成到信息系统的过程

C.信息系统集成项目的指导方法是“总体规划、分步实施”

D.信息系统集成包含技术,管理和商务等方面,是一项综合性的系统工程

145、信息安全工程监理是信息系统工程监理的总要组成部分,信息安全工程监理适用的信息化工程中,以下选项最合适的是: (D)

A.通用布缆系统工程

B.电子设备机房系统工程

C.计算机网络系统工程

D.以上都适用

146、以下关于信息安全工程说法正确的是 (C)

A.信息化建设中系统功能的实现是最重要的

B.信息化建设可以先实施系统,而后对系统进行安全加固

C.信息化建设中在规划阶段合理规划信息安全,在建设阶段要同步实施信息安全建设

D.信息化建设没有必要涉及信息安全建设

147、有关系统安全工程-能力成熟度模型(SSE-CMM)中的基本实施(Base Practices,BP),正确的理解是 (C)

A.BP 是基于最新技术而制定的安全参数基本配置

B.大部分 BP 是没有经过测试的

C.一项 BP 是用于组织的生存周期而非仅适用于工程的某一特定阶段
D.一项 BP 可以和其他 BP 重叠

148、有关系统安全工程-能力成熟度模型(SSE-CMM)中的通用实施(Generic Practices,GP)错误的理解是 (B)
A.GP 是涉及过程的管理、测量和制度化方面的活动
B.GP 适用于域维中部分过程区域(Process Areas,PA)的活动而非所有 PA 的活动
C.在工程师实施时,GP 应该作为基本实施(Basepractices,BP)的一部分加以执行
D.在评估时,GP 用于判定工程组织执行某个 PA 的能力

149、系统安全工程-能力成熟度模型(Systems Securityengineering- Capability maturitmodel,SSE-CMM)定义的包含评估威胁、评估脆弱性、评估影响和评估安全风险的基本过程领域是 (A)
A.风险过程
B.工程过程
C.保证过程
D.评估过程

150、以下行为不属于违反国家保密规定的行为:(D)
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

151、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 (A)
1>安全事件(包括安全事故)报告制度
2>安全等级保护制度
3>信息系统安全监控
4>安全专用产品销售许可证制度

A.1,2,4
B.2,3
C.1,2,3,4
D.1,2,3

152、信息系统建设完成后,(A)的信息系统的运营使用单位应当选择符合国家规定的测评机构进行测评合格后方可投入使用 (A)
A.二级以上
B.三级以上
C.四级以上
D.五级以上

153、为了进一步提供信息安全的保障能力和防护水平,保障和促进信息化建设的健康发展,公安部等四部门联合发布《关于信息安全等级保护工作的实施意见》(公通字[2004166 号),对等级保护工作的开展提供宏观指导和约束,明确了等级保护工作的基本内容、工作要求和实施计划,以及各部门工作职责分工等。关于该文件,下面理解正确的是 (A)
A.该文件是一个由部委发布的政策性文件,不属于法律文件
B.该文件适用于 2004 年的等级保护工作,其内容不能约束到 2005 年及之后的工作
C.该文件是一个总体性指导文件,规定所有信息系统都要纳入等级保护定级范围

D.该文件适用范围为发文的这四个部门,不适用于其他部门和企业等单位

154、CC 标准是目前系统安全认证方面最权威的标准,以下哪一项没有体现 CC 标准的先进性? (C)
A.结构的开放性,即功能和保证要求都可以在具体的“保户轮廓”和“安全目标”中进一步细化和扩展
B.表达方式的通用性,即给出通用的表达表示
C.独立性,它强调讲安全的功能和保证分离
D.实用性,将 CC 的安全性要求具体应用到 IT 产品的开发、生产、测试和评估过程中

155、对于数字证书而言,一般采用的是哪个标准?(D)
A ISO/IEC15408
B.802.1
C.GB/T20984
D.X.509

156、在可信计算机系统评估准则(TCSEC)中,下列哪一项是满足强制保护要求的最低级别?(D)
A. C2
B. Cl
C. B2
D. B1

157、关于标准,下面哪项理解是错误的(B)
A.标准是在一定范围内为了获得最佳秩序,经协商一直制定并由公认机构批准,共同重复使用的种规范性文件。标准是标准化活动的重要成果
B.国际标准是由国家标准组织通过并公开发布的标准。同样是强制性标准,当国家标准和国际标准的条款发生冲突时,应以国际标准条款为准
C.行业标准是针对没有国家标准而又需要在全国某个行业范围内统一的技术要求而制定的标准。同样是强制性标准,当行业标准和国家标准的条款发生冲突时,应以国家标准条款为准
D.行业标准由省、自治区、直辖市标准化行政主管部门制定,并报国务院标准化行政主管部门和国务院有关行政主管部门备案,在公布国家标准之后,该地方标准即应废止

158, 20054F, RFC4301 (Request for Comments4301 Security Architecture for theInternet Protocol)发布,用以取代原先的 RFC2401,该标准建议规定了 Psec 系统基础架构,描述如何在 IP 层(IPv4IPv6)位流量提供安全业务。请问此类 RFC 系列标准建议是由下面哪个组织发布的 (D)
A.国际标准化组织(International Organization for Standardization,IS0)
B.国际电工委员会(Int erna tio nal Elec trot echnical Commission,IEC)
C.国际电信联盟远程通信标准化组织(ITU Telecommunication Standardization
Sector, ITU-T
D.Internet 工程任务组(Internet Engineering Task Force,IETF)

159、GBT1836《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廓 Protection Proffile,PP)和安全目标(Security Target,ST)的评估准则,提出了评估保证级(Evaluation Assurance Level,EAL),其评估保证级共分为(D)个递增的评估保证等级。(D)
A.4
B.5
C.6
D.7

160、关于我国信息安全保障的基本原则,下列说法中不正确的是 (A)

A.要与国际接轨,积极吸收国外先进经验并加强合作,遵循国际标准和通行做法,坚持管理与技术并重
B.信息化发展和信息安全不是矛盾的关系,不能牺牲一方以保证另一方
C.在信息安全保障建设的各项工作中,既要统筹规划,又要突出重点
D.在国家信息安全保障工作中,要充分发挥国家、企业和个人的积极性,不能忽视任何一方的作用。

161、有关系统工程的特点,以下错误的是 (B)
A.系统工程研究问题一般采用先决定整体框架,后进入详细设计的程序
B.系统工程的基本特点,是需要把研究对象解构为多个组成部分分别独立研究
C.系统工程研究强调多学科协作,根据研究问题涉及到的学科和专业范围,组成一个知识结构合理的专家体系
D.系统工程研究是以系统思想为指导,采取的理论和方法是综合集成各学科、各领域的理论和方法

162、以下关于项目的含义,理解错误的是(B)
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)>需相关方的致同意(Agree to)、现实(Realistic)>有一定的时限(Time- oriented)

163、以下说法正确的是 (C)
A.验收测试是同承建方和用户按照用户使用手册执行软件验收
B.软件测试的目的是为了验证软件功能是否正确
C.监理工程师应按照有关标准审查提交的测试计划,并提出审查意见
D.软件测试计划开始于软件设计阶段,完成于软件开发阶段

164、在某网络机房建设项目中,在施工前,以下哪一项不属于监理需要审核的内容:(A)
A.审核实施投资计划
B.审核实施进度计划
C.审核工程实施人员
D.企业资质

165、以下系统工程说法错误的是 (A)
A.系统工程是基本理论的技术实现
B.系统工程是一种对所有系统都具有普片意义的科学方法
C.系统工程是组织管理系统规划、研究、制造、试验、使用的科学方法
D.系统工程是一种方法论

166.关于密钥管理,下列说法错误的是 (B)
A.科克霍夫原则指出算法的安全性不应基于算法的保密,而应基于密钥的安全性
B 保密通信过程中,通信方使用之前用过的会话钥建立会话,不影响通信安全
C 密钥管理需要考虑密钥产生、存储、备份、分配、更新撤销等生命周期过程的每一个环节
D、在网络通信过程中通信双方可利用 diffie- hell man 协议商出会话密钥

167、 PDCERF 方法是信息安全应急响应工作中常用的一种方法,它将应急响应分成六个阶段。其中,主要执行如下工作应在哪一个阶段关闭信息系统、和或修改防火墙和路由器的过滤规则,拒绝来自发起攻击的嫌疑主机流量、或封锁被攻破的登录账号等(B)
A.准备阶段

B.遏制阶段
C.根除阶段
D.检测阶段

168、在网络信息系统中对用户进行认证识别时,口令是一种传统但仍然使用广泛的方法,口令认证过程中常常使用静态口令和动态口令。下面找描述中错误的是(C)
A.所谓静态口令方案,是指用户登录验证身份的过程中,每次输入的口令都是固定、静止不变的
B.使用静态口令方案时,即使对口令进行简单加密或哈希后进行传输,攻击者依然可能通过重放攻击来欺骗信息系统的身份认证模块
C.动态口令方案中通常需要使用密码算法产生较长的口令序列,攻击者如果连续地收集到足够多的历史口令,则有可能预测出下次要使用的口令
D.通常,动态口令实现方式分为口令序列、时间同步以及挑战/应答等几种类型

169、“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)
A. UTM
B. FW
C. IDS
D. SAC

170、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(C)
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

171、 Gary Mcgraw 博士及其合作者提出软件安全模型 BSI，该模型应由三根支柱来支撑,这三个支柱是(B)
A.源代码审核、风险分析和渗透测试
B.应用风险管理、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

172、某电子商务网站最近发生了一起安全事件,出现了一个价值 1000 元的商品用 1 元被买走的情况,经分析是由于设计时出于性能考虑,在浏览时时使用 Http 协议,攻击者通过伪造数据包使得向购物车添加商品的价格被修改。利用此漏洞,攻击者将价值 1000 元的商品以 1 元添加到购物车中,而付款时又没有验证的环节导致以上问题。对于网站的这个问题原因分析及解决措施,最正确的说法应该是? (A)
A.该问题的产生是由于使用了不安全的协议导致的,为了避免再发生类似的问题,应对全网站进行安全改造,所有的访问都强制要求使用 https
B.该问题的产生是由于网站开发前没有进行如威胁建模等相关工作或工作不到位,没有找到该威胁并采取相应的消减措施
C.该问题的产生是由于编码缺陷,通过对网站进行修改,在进行订单付款时进行商品价格验证就可以解决
D.该问题的产生不是网站的问题,应报警要求寻求警察介入,严惩攻击者即可

173、某网站在设计时经过了威胁建模和攻击面分析,在开发时要求程序员编写安全的代码,但是在部署时由于管理员将备份存放在 Web 目录下导致了攻击者可直接下载备份,为了发现系统中是否存在其他类似问题,

以下哪种测试方式是最佳的测试方式 (C)

A.模糊测试

B.源代码测试

C.渗透测试

D.软件功能测试

174、以下哪一项不是常见威胁对应的消减措施:(C)

A.假冒攻击可以采用身份认证机制来防范

B.为了防止传输的信息被篡改,收发双方可以使用单向 Hash 函数来验证数据的完整性

C.为了防止发送方否认曾经发送过的消息,收发双方可以使用消息验证码来防止抵赖

D.为了防止用户提升权限,可以采用访问控制表的方式来管理权限

175、以下关于模糊测试过程的说法正确的是(C)

A.模糊测试的效果与覆盖能力,与输入样本选择不相关

B 为保障安全测试的效果和自动化过程,关键是将发现异常进行现场保护记录,系统可能无法恢复异常状态进行后续的测试

C.通过异常样本重视异常,人工分析异常原因,判断是否为潜在的安全漏洞,如果是安全漏洞,就需要进一步分析其危害性、影响范围和修复建议

D.对于可能产生的大量异常报告,需要人工全部分析异常报告

176、有关危害国家秘密安全的行为,包括:(A)

A.严重违反保密规定行为、定密不当行为、公共信息网络运营商及服务商不履行保密义务的行为、保密行政管理部门的工作人员的违法行为

B.严重违反保密规定行为、公共信息,网络运营商及服务商不履行保密义务的行为、保密行政管理部门的工作人员的违法行为,但不包括定密不当行为

C.严重违反保密规定行为、定密不当行为、保密行政管理部门的工作人员的违法行为,但不包括公共信息网络运营商及服务商不履行保密义务的行为

D.严重违反保密规定行为、定密不当行为、公共信息网络运营商及服务商不履行保密义务的行为,但不包括保密行政管理部门的工作人员的违法行为

177、国务院信息化工作办公室于 2004 年 7 月份下发了《关于做好重要信息系统灾难备份工作的通知》,该文件中指出了我国在灾备工作原则,下面哪项不属于该工作原则(B)

A.统筹规划

B.分组建设

C.资源共享

D.平战结合

178、小陈学习了有关信息安全管理体系的内容后,认为组织建立信息安全管理体系并持续运行,比起简单地实施信息安全管理,有更大的作用,他总结了四个方面的作用,其中总结错误的是(D)

A.可以建立起文档化的信息安全管理规范,实现有“法”可依,有章可循,有据可查

B.可以强化员工的信息安全意识,建立良好的安全作业习惯,培育组织的信息安全企业文化

C.可以增强客户、业务伙伴、投资人对该组织保障其业务平台和数据信息的安全信心

D.可以深化信息安全管理,提高安全防护效果,使组织通过国际标准化组织的 IS09001 认证

179、不同的信息安全风险评估方法可能得到不同的风险评估结果,所以组织机构应当根据各自的实际情况,选择适当的风险评估方法。下面的描述中,错误的是(B)

A.定量风险分析试图从财务数字上对安全风险进行评估,得出可以量化的风险分析结果,以度量风险的可能性和损失量

B.定量风险分析相比定性风险分析能得到准确的数值,所以在实际工作中应使用定量风险分析,而不应选择定性风险分析

C.定性风险分析过程中,往往需要凭借分析者的经验和直接进行,所以分析结果和风险评估团队的素质、经验和知识技能密切相关

D.定性风险分析更具主观性,而定量风险分析更具客观性

180、 Windows 系统中,安全标识符(SID)是标识用户、组和计算机账户的唯一编码,在操作系统内部使用。当授予用户、组、服务或者其他安全主体访问对象的权限时,操作系统会把 SID 和权限写入对象的 ACI 中,小刘在学习了 SID 的组成后,为了现固所学知识,在自己计算机的 Windows 操作系统中使 whoami/ users 操作查看当前用户的 SID。得到的 SlID 为 S-1-5-21-1534169462-1651380828-111620651-500,下列选项中,关于此 SID 的理解错误的是(D)

A.前三位 S-1-5 表示此 SID 是由 Windows NT 颁发的

B.第一个子颁发机构是 21

C. Windows NTE 的 SID 的三个子颁发机构是 1534169462、1651380828、11620651

D.此 SID 以 500 结尾,表示内置 guest 账户

181、 letc/passwd 文件是 Unxlinux 安全的关键文件之一。该文件用于用户登录时校验用户的登录名、加密的口令数据项、用户 ID(UID)、默认的用户分组 ID(GID)、用户信息、用户登录目录以及登录后使用的 shell 程序。某黑客设法窃取了银行账户管理系统的 passwd 文件后,发现每个用户的加密的口令数据项都显示为 x。下列选项中,对此现象的解释正确的是(C)

A.黑客窃取的 passwd 文件是假的

B.用户的登录口令经过不可逆的加密算法加密结果为'x

C.加密口令被转移到了另一个文件里

D.这些账户都被禁用了

182、 Linux 系统文件中访问权限属性通过 9 个字符来表示,分别表示文件属主、文件所属组用户和其他用户对文件的读(r)、写(w)及执行(x)的权限。文件 usr/bin/ passwd 的属性信息如下图所示,在文件权限中还出现了一位 S,下列选项中对这一位 s 的理解正确的是()

- r-s --x - x 1 root root10704Apr2011: 55/usr/bin/passwd (D)

A.文件权限出现了错误,出现 s 的位应该改为 x

B.S 表示 sticky.位,设置 sticky 位后,就算用户对目录具有写权限,也不能删除该文件

C.S 表示 SGID 位,文件在执行阶段具有文件所在组的权限

D.S 表示 SUID 位,文件在执行阶段具有文件所有者的权限

183、 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 个面来完成。小张在学习了 Linux 系统安全的相关知识后,尝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)

A.编辑文件/etc/ passwd.检查文件中用户 ID,禁用所有 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/etc/pam,d/ system-auth,设置 auth required pam tal1y.so

oner=faildeny=unlock time=300

D.编辑文件/etc/ profile,设置 TMOUT=600

184、目前,信息系统面临外部攻击者的悉意攻击威胁,从威胁能力和掌握资源分,这些威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 (B)

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.现固战略优势,执行军事任务、进行目标破坏的信息作战部队

185、以下哪种风险被认为是合理的风险 (D)
A.最小的风险
B.残余的风险
C.未识别的风险
D.可接受的风险

186、规划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”阶段输出的文档 (D)
A.《风险评估方案》,主要包括本次风险评估的目的、范围、目标、评估步骤、经费预算和进离安排等内容
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.《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

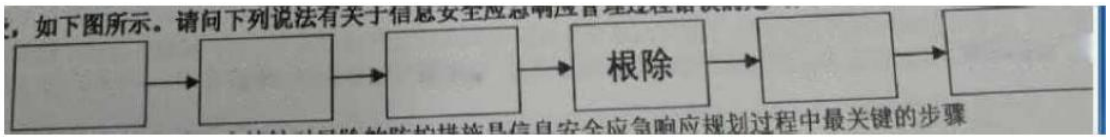
187、以下关于互联网协议安全(Internet Protocol Security, Ipsec)协议说法错误的是 (D)
A.在传送模式中,保护的是 IP 负载
B.验证头协议(Authentication Head,AH)和 IP 圭寸装安全载荷协议(Encapsulating Security Pay load,ESP)都能以传输模式和隧道模式工作
C.在隧道模式中,保护的是整个互联网协议(InternetProtoco1,IP)包,包括 IP 头
D. Ipsec 仅能保证传输数据的可认证性和保密性

188、某个新成立的互联网金融公司拥有 10 个与互联网直接连接的 P 地址,但是该网络内有 15 台个人计算机,这些个人计算机不会同时开机并连接互联网。为解决公司员工的上网问题,公司决定将这 10 个互联网地址集中起来使用,当任意一台个人计算机开机并连接网络时,管理中心从这 10 个地址中任意取出一个尚未分配的 P 地址分配给这个人的计算机。他关机时,管理中心将该地为收回,并重新设置为未分配。可见只要同时打开的个人计算机数量少于或等于可供分配的 P 地址,那么每中个人计算机可获取一个 IP 地址,并实现与互联网的连接,该公司使用的 IP 地址规划方式是(B)
A.静态分配地址
B.动态分配地址
C.静态 MAT 分配地址
D.端口 NAT 分配地址

189、在 inux 系统中,下列哪项内容不包含在/ etc/passwd 文件中(B)
A.用户名
B、用户口令
C.用户主目录
D.用户登录后使用的 SHEL

190、某市环卫局网络建设是当地政府投资的重点项目。总体目标就是用交换式水平布线,由大型的交换机和路由器连通几个主要的工作区域,在各个区域建立通过网络传输到各监控中心。其中对交换机和路由器进行配置是网络安全中的一,和路由器的安全配置,操作错误的是 (A)
A.保持当前版本的操作系统,不定期更新交换机操作系统补丁
B.控制交换机的物理访问端口,关闭空闲的物理端口
C.带外管理交换机,如果不能实现的话,就可以利用单独的 VLAN 号进行带内管理
D.安全配置必要的网络服务,关闭不必要的网络服务

191、应急响应是信息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到最低。应急响应方法和过程并不是唯一的。一种被广为接受的应急响应管理过程分为 6 个阶段为准备—检测—遏制—根除—恢复—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 (C)



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急响应规划过程中最关键的步骤
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
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。

192、小张新购入了一台安装了 words 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 words 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、公钥策略和 IP 安全策略,那么该操作属于操作系统安全配置内容中的(B)
A.关闭不必要的服务
B.制定操作系统的策略
C.关闭不必要的端口
D.开启审核策略

193、随着互联网”概念的普及,越来越多的新兴住宅小区引入了“智能楼宇”的理念,某物业为提供高档次的服务,防止网络主线路出现故障,保证小区内网络服务的可用,稳定、高效,计划通过网络冗余配置的是(B)
A、接入互联网时,同时采用不同电信运营商线路,相互备份且互不影响。
B、核心层、汇聚层的设备和重要的接入层设备均应双机设备。
C、规划网络 IP 地址,制定网络 IP 地址分配策略
D. 保证网络带宽和网络设备的业务处理能力具务冗余空间,满足业务高峰期和业务发展需求

194、下列关于软件安全开发中的 BSI(Build Security In)系列模型说法错误的是(B)
A、BIS 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、软件安全接触点和安全测试
C. 软件安全触点是软件开发生命周期中一套轻量级最优工程化方法,它提供了从不同角度保障安全的行为方式
D、BS I 系列模型强调应该使用工程化的方法来保证软件安全,即在整个软件开发生命周期中都要确保将安全作为软件的一个有机组成部分

195、访问控制是对用户或用户访问本地或网络上的域资源进行法令一种机制。在 Windows2000 以后的操作系统版本中,访问控制是一种双重机制,它对用户的授权基于用户权限和对象许可,通常使用 ACL、访问令牌和授权管理器来实现访问控制功能。以下选项中对 windows 操作系统访问控制实现方法的理解错误的是(A)
A、ACL 只能由管理员进行管理
B、ACL 是对象安全描述的基本组成部分,它包括有权访问对象的用户和级的 SID
C、访问令牌存储着用户的 SID,组信息和分配给用户的权限
D、通过授权管理器,可以实现基于角色的访问控制

196、社会工程学定位在计算机信息安全工作链的一个最脆弱的环节,即人”这个环节上。这些社会工程黑客在某黑客大会上成功攻入世界五百强公司,其中一名自称是 CSO 杂志做安全调查,半小时内,攻击者选择了在公司工作两个月安全工程部门的合约雇员,在询问关于工作满意度以及食堂食物质量问题后,雇员开始

透露其他信息,包括:操作系统、服务包、杀毒软件、电子邮件及测览器。为对抗此类信息收集和分析,公司需要做的是(A)

A、通过信息安全培训,使相关信息发布人员了解信息收集风险,发布信息采取最小化原则

B、减少系统对外服务的端口数量,修改服务旗标

C、关闭不必要的服务,部署防火墙、IDS 等措施

D、系统安全管理员使用漏洞扫描软件对系统进行安全审计

197、某黑客通过分析和整理某报社记者小张的博客,找到一些有用的信息,通过伪装的新闻线索,诱使其执行木马程序,从而控制了小张的电脑,并以她的电脑为攻击的端口,使报社的局域网全部感染木马病毒,为防范此类社会工程学攻击,报社不需要做的是(D)

A、加强信息安全意识培训,提高安全防范能力了解各种社会工程学攻击方法,防止受到此类攻击

B、建立相应的安全相应应对措施,当员工受到社会工程学的攻击,应当及时报告

C、教育员工注重个人隐私保护

D、减少系统对外服务的端口数量,修改服务旗标

198、2016 年 9 月,一位安全研究人员在 Google Cloud IP 上通过扫描,发现了完整的美国路易斯安邦州 290 万选民数据库。这套数据库中囊括了诸如完整姓名、电子邮箱地址、性别与种族、选民状态、注册日期与编号、正党代名和密码,以防止攻击者利用以上信息进行(B)攻击。(B)

A、默认口令

B、字典

C、暴力

D、XSS

199、基于 TCP 的主机在进行一次 TcP 连接时简要进行三次握手,请求通信的主机 A 要与另一台主机 B 建立连接时,A 需要先发一个 SYN 数据包向 B 主机提出连接请示,B 收到后,回复一个 ACK/SYN 确认请示给 A 主机,然后 A 再次回应 ACK 数据包,确认连接请求。攻击通过伪造带有虚假源地址的 SYN 包给目标主机,使目标主机发送的 ACSYN 包得不到确认。一般情况下,目标主机会等一段时间后才会放弃这个连接等待。因此大量虚假SYN包同时发送到目标主机时,目标主机上就会有大量的连接请示等待确认,当这些未释放的连接请示数量超过目标主机的资源限制时。正常的连接请示就不能被目标主机接受,这种 Syn food 攻击属于(A)

A、拒绝服务攻击

B、分布式拒绝服务攻击

C、缓冲区溢出攻击

D、SQL 注入攻击

200、小王是某大学计算机科学与技术专业的学生,最近因为生病缺席了几堂信息安全课程,这几次课的内容是自主访问控制与强制访问控制,为了赶上课程进度,他向同班的小李借来课堂笔记,进行自学。而小李在听课时由于经常走神,所以笔记中会出现一些错误。下列选项是小李笔记中关于强制访问控制模型的内容,其中出现错误的选项是(D)

A、强制访问控制是指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

B、安全属性是强制性的规定,它由安全管理员或操作系统根据限定的规则确定,不能随意修改

C、系统通过比较客体玫主体的安全属性来决定主体是否可以访问客体

D、它是一种对单个用户执行访问控制的过程和措施

201、信息安全是国家安全的重要组成部分,综合研究当前世界各国信息安全保障工作,下面总结错误的是(C)

A、各国普遍将与国家安全、社会稳定和民生密切相关的关键基础设施作为信息安全保障的重点

B、各国普遍重视战略规划工作,逐步发布网络安全战略、政策评估报告、推进计划等文件
C、各国普遍加强国际交流与对话,均同意建立一致的安全保障系统,强化各国安全系统互通
D、各国普遍积极推动信息安全立法和标准规范建设,重视应急响应、安全监管和安全测评

202、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站,旅游网站则获得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络信息(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了,这种向 Web 页面插入恶意 htm 代码的攻击方式称为 (B)
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

203、模糊测试,也称 Fzz 测试,是一种通过提供非预期的输入并监视异常结果来发现软件故障的方法。下面描述正确的是 (A)
A、模糊测试本质上属于黑盒测试
B、模糊测试本质上属于白盒测试
C、模糊测试有时属于黑盒测试,有时属于白盒测试,取决于其使用的测试方法
D、模糊测试既不属于黑盒测试,也不属于白盒测试

204、若一个组织声称自己的 ISMS 符合 SO/=C27001 或 GBT22080 标准要求,其信息安全控制措施通常需要在人力资源安全方面实施常规控制,人力资源安全划分为 3 个控制阶段,不包括哪一项 (D)
A、任用之前
B、任用中
C、任用终止或变化
D、任用公示

205、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的攻击,以下做法无用的是 (C)
A、不下载、不执行、不接收来历不明的软件和文件
B、不随意打开来历不明的邮件,不浏览不健康不正规的网站
C、使用共享文件夹
D、安装反病毒软件和防火墙,安装专门的木马防范软件

206、小华在某电子商务公司工作,某天他在查看信息系统没计文档时,发现其中标注该信息系统的 RPO(恢复点目标)指标为 3 小时。请问这意味着(D)
A、该信息系统发生重大安全事件后,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安全事件后,工作人员应在 3 小时内完整应急处理工作并恢复对外运行
C、该信息系统发生重大安全事件后,工作人员在完成处置和灾难恢复工作后,系统至少能提供 3 小时的紧急业务服务能力
D、该信息系统发生重大安全事件后,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 小时的业务数据

207、 Kerberos 协议是一种集中访问控制协议,他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,而不在需要其他的认证过程,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)
A、安全凭证

B、用户名
C、加密密钥
D、会话密钥

208、若一个组织声称自己的 ISMS 符合 ISO/IEC27001 或 GBT22080 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,资产管理包括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 (D)
A、资产清单
B、资产负责人
C、资产的可接受使用
D、分类指南、信息的标记和处理

209、在使用系统安全工程-能力成熟模型(SSE-CMM)对一个组织的安全工程能力成熟度进行测量时,有关测量结果,错误的理解是:(B)
A、如果该组织在执行某个特定的过程区域时具备了一个特定级别的部分公共特征时,则这个组织在这个过程区域的能力成熟度未达到此级
B、如果该组织某个过程区域(Process Area,PA)具备了定义标准过程”、“执行已定义的过程两个公共特征,则此过程区域的能力成熟度级别达到 3 级充分定义级
C、如果某个过程区域(ProcesPA)包含 4 个基本实施(Base Parctices,BP)执行此 PA 时执行了 3 个 BP,则此过程区域能力成熟度级别为 0
D、组织在不同的过程区域的能力成熟可能处于不同的级别上

210、数据流图（DFD）是用来表示系统的功能的工具表示系统的逻辑模型:描述了数据流在系统中流动的情况;它是种功能模型,是常用的进行软件需求分析的图形工具,其基本图形符号是 (C)
A、输入、输出、外部实体和加工
B、变换、加工、数据流和存储
C、加工数据流、数据存储和外部实体
D、变换、数据存储、加工和数据流

211、把瀑布模型和专家系统结合在一起在开发的各个阶段上都利用相应的专家系统来帮助软件人员完成开发工作。(C)
A、原型模型
B、螺旋模型
C、基于知识的智能模型
D、喷泉模型

212、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(C)
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

213、下面对零日(zero-day)漏洞的理解中,正确的是 (D)

A、指一个特定的漏洞,该漏洞每年1月1日零点发作,可以被攻击者用来远程攻击,获取主机权限

B、指一个特定的漏洞精指在200被发现出来的一种洞,该漏洞被震网病毒所利用,用来攻击伊朗布什尔核电站基础设施

C、指一类漏洞,特别好被利用,一旦成功利用该类漏洞可以在1天内完成攻击且成功达到攻击目标

D、一类漏洞,刚被发现后立即被恶意利用的安全漏洞一般来说,那些已经被儿人发现,但是还未公开、还不存在安全补丁的漏洞都是零日漏洞

214、随着信息安全涉及的范围越来越广,各个组织对信息少全管理的需求来越迫切,越来越多的组织开始尝试使用参考So27001分绍的SMS来实施信息安全管理体系,提高组织的信息安全管理能力,关于ISMS,下面描述错误的是(A)

A在组织中,应由信息技术责任部门(如信息中心)制定并颁布信息安全方针,为组织的ISMS建设指明方向并提供总体物领,明确总体要求

B、组织的管理层应确保SMS目标和相应的计划得以制定,信息个理目标应明确、可度量,风险管理计划应具体,具备可行性

C、组织的信息安全目标,信息安全方针相要求应传达到全组织范围内,应包括全体员工,同时,也应传达到客户。台作伙伴和供应商等外部各方

D、组织的管理层应全面了解组织所面临的信息安全风险,决定风险可接受级别和风险可接受则,并确认接受相关残余风险

215、有关项目管理,错误的理解是 (B)

A、项目管理是一门关于项目资金、时间、人力等资源控制的管理科学

B、项目管理是运用系统的观点、方法、理论,对项目涉及的全部工作进行有效地管理,不受项自资源的约

C、项目管理包括对项目范围、时间成本、质量人力资源、沟通、风险、采购、集成的管理

D、项目管理是系统工程思想针对具体项目的实践应用

216、开发软件所需高成本和产品的低质量之间有着尖锐的矛盾,这种现象称作(C)

A、软件工程

B、软件周期

C、软件危机

D、软件产生

217、GB/T20984-2007《信息安全技术信息安全义批详选规范》、对10个()进行了定义阐述其相关关系,规定了()的原理和()规定了风险评估实施的7个阶段的具体方法和要求,规定了针对信息系统()5个阶段风险评估的常见(),给出了风险评估的一般计算方法和相关工具建议。(A)

A、风险要素;风险评估;实施流程;生命周期;工作形式

B、风险要素;实施流程;风险评估;生命周期:工作形式C

C、风险要素;生命周期:风险评估;实施流程;工作形式D

D、风险要素;工作形式;风险评估;实施流程:生命周期

218、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,他使用了Nessus工具来扫描和发现数据库服务器的漏洞,根据风险管理的相关理论,他这个扫描活动属于下面哪个阶段的工作 (B)

A、风险分析

B、风险要素识

C、风险结果判定

D、风险处理

219、超文本传输协议(HypertextTransferProtocolHTTP)是互联网上广泛使用的一种网络协议,下面哪种协议基于 HTTP 并结合 SSL 协议,具备用户鉴别和通信数据加密等功能 (C)

A、HTTP1.0 协议

B、HTTP1.1 协议

C、HTTPS 协议

D、HTTPD 协议

220、访问控制的实施一般包括两个步骤首先要鉴别主体的合法身份,根据当前系统的访问控制规则授予用户相应的访问权限。在此过涉及主体、客体、访问控制实施部件和访问控制决策部件之间的交互。下图所示的访问控制实施步骤中,标有数字的方框代表了主体、客体、访问控制实施部件和访问控制决策部件。下列选项中,标有数字 1、2、3、4 的方框分别对应的实体或部件正确的是(B)

A、主体、访问控别决策、客体、访问控制实施

B、主体、访问控制实施,客体、访问控制决策

C、客体、访问控制决策、主体、访问控制实施

D、客体、访问控制实施、主体、访问控制决策

221、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、数据庐连接错误、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(D)

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、最小化反馈信息

222、/etc/ passwd 文件是 UN/Linux 安全的关键文件之。该文件用于用户登录时校验用户的登录名、加密的口令数据项、用户 ID(UID)、默认的用户分组 ID(GID)、用户信息、用户登录目录以及登录后使用的 shell i 程序。某黑客设法窃取了银行账户管理系统的 passwd 文件后,发现每个用户的加密的口令数据项都显示为 X。下列选项中,对此现象的解释正确的是(C)

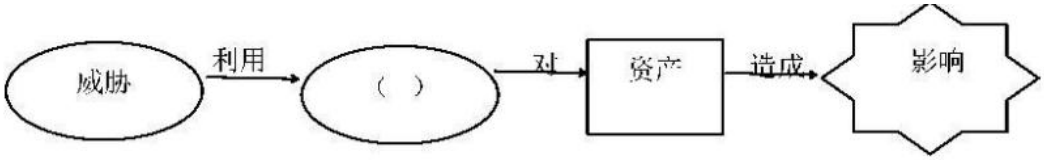
A、黑客窃取的 passwd 文件是假的

B、用户的登录口令经过不可逆的加密算法加密结果为“X”

C、加密口令被转移到了另一个文件里

D、这些账户都被禁用了

223、陈工学习了信息安全风险的有关知识,了解到信息安全风险的构成过程,包括五个方面起源、方式途径、受体和后果。他画了下面这张图来描述信息安全风险的构成过程,图中括号空白处应该填写 (C)



A、信息载体

B、措施

C、脆弱性

224、关于信息安全应急响应管理过程描述不正确的是 (D)

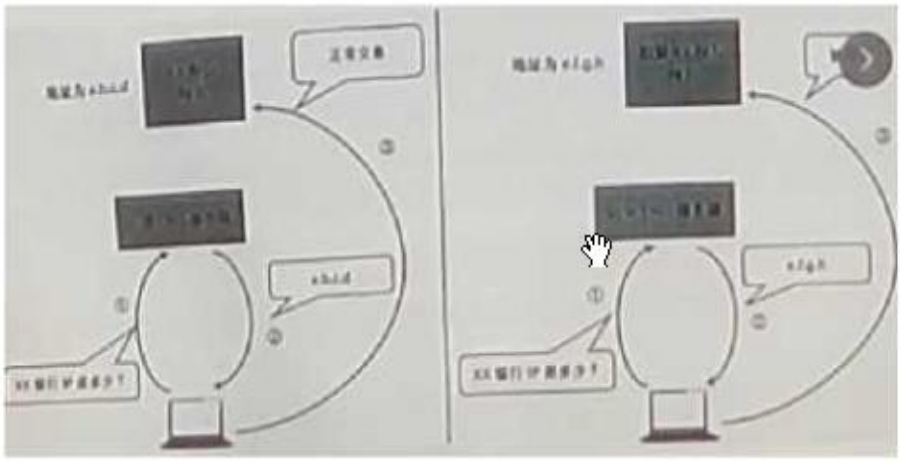
A、基于应急响应工作的特点和事件的不规则性,事先制定出事件应急响应方法和过程,有助于一个组织在事件发生时阻止混乱的发生或是在混乱状态中迅速恢复控制,将损失和负面影响降至最低

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

D、一种校广为接受的应色的应方法是将应色响应管理过程分为准备检刻、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

225、在信息系统中,访问控制是重要的安全功能之一,它的任务是在用)系统资源提供最大限度共享的基础上,对用户的访问权限进行管理,防止对信息的非授权算改和滥用。访问控制模型将实体划分为主体和客体两类,通过对主体身份的识别来限制其对客体的访问权限。下列选项中,对主体、客体和访问权限的描述中错误的是(C)



A.对文件进行操作的用户是一种主体

B 主体可以接收客体的信息和数也可能改变客体相关的信息

C.访问权限是指主体对客体所允许的操作

D.对目录的访问权限可分为读、写

答案:如果如上的 ABCD 的话,则选择 C 是错误的。如果 D 的答案有“拒绝访问”则选择 D 是错误的。

226、根据 3 ell-lapadua 模型安全策略,下图中写和读操作正确的是 (D)

A、可写可读

B、可读不可写

C、可写不可读

D、不可读不可写

227、小李在上网时不小心点开了假冒某银行的钓鱼网站,误输入了银行账号与密码损失上千元,他的操作如右图所示,他所受到的攻击是(B)

A、ARP 欺骗

B、DNS 欺骗

C、IP 欺骗

D、TCP 会话

228、随着互联网+概念的普及,越来越多的新兴住宅小区引入了智能楼宇”的理念,某物业为提供高档次的服务,防止网络主线路出现故障,保证小区内网络服务的可用、稳定、高效,计划通过网络冗余配置确保”智能楼宇”系统的正常运转,下列选项中不属于冗余配置的是 (C)
A、接入互联网时,同时采用不同电信运辜商线路,相互备份且互不影响
B、核心层、汇聚层的设备和重要的接入层设备均应双机热备
C、规划网络 IP 地址,制定网络 IP 地址分配策略
D、保证网络带宽和网络设备的业务处理能力具备冗余空间,满足业务高峰期和业务发展需要

229、根据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,按照要向公安机关备案即可,可以不需向上级或主管部门来测评和检查,此类信息系统应属于(C)
A、零级系统
B、一级系统
C、二级系统
D、三级系统

230、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)
A.信息中心的考虑是正确的,在软件立项投入解决软件安全问题,总体经费投入比软件运行后的费用要低
B.软件开发部门的说法是正确的,因为软件发现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
C.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
D、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

231、20 世纪 20 年代,德国发明家亚瑟·谢尔比乌斯(Auntur scherbius)和理查德,里特(Richard Ritter 发明了 ENIGMA 密码机,看密码学发展历史阶段划分,这个阶段属于(B)
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.现代密码学的早起发展阶段。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

232、某软件在设计时,有三种用户访问模式,分别是仅管理员可访问,所有合法用户可访问和允许匿名访问请问采用这三种访问模式时,攻击面最高的是 (C)
A、仅管理员可访问
B、所有合法用户可访问
C、允许匿名访问
D、三种方式都一样

233、某单位开发了个面向互联网提供服务的应用网站,该单位委托软件测评机构对软件进行了源代码分析、模糊测试等软件安全性测试,在应用上线前,项目经理提出了还需要对应用网站进行一次渗透测试,作为安全主管,你需要提出渗透性测试相比源代码测试、模糊测试的优势给领导做决策,以下哪条是渗透性测试的优势?(A)
A、渗透测试以攻击者的思维模拟真实攻击,能发现如配置错等运行维护所产生的漏洞

渗透测试是用软件代替人工的一种测试方法,因此测试效更高
C、渗透测试使用人工进行测试,不依赖软件,因此测试更准洞更多酒渗透测试中必须要查
D、渗透测试必须查看看软件源代码,因此测试中发现的漏洞更多

234、国家科学技术秘密的密级分为绝密级、机密级、密级,以下娜块属于绝密级的描述?(D)
A、处于国际先进水平、并且有军事用途或者对经济建设具有重要影响的
B、能够局部及应国家防制和治安实力的
C、我国独有不要自己条件因素制约.能体现民族特色的精华,并且社会效益或者经济效益显著的传统工艺
D、国际领先.并且对国防建设或者经济建设具有特别重大影响的

235、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:(C)
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.可委托同一专业机构完成等级测评的风险评估工作,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

236、随着金融电子化的发展,全球金融通信网络已出具规模。某金融单位组建的计算机通信网络覆盖全国,有力的促进了该企业各种金融业务的发展。然而网络技术的普及、网络规模规模的延伸,开始逐步让该企业对网络安全提出了更高的要求。为了进一步促进金融电子化的建设,保障金融网络安全运行,该企业经过前期充分的调研分析与论证,实施了防火墙 NPN 系统建设项目。防火墙不能实现的安全功能是 (D)
A、对出入网络的访问行为进行管理和控制
B、过滤出入网络的数据,强化安全策略
C、隐藏内部网络细节
D、评估系统关键资源和数据完整性,识别已知的攻击行为

237、下面有关软件安全问题的描述中,哪项应是由于软件设计缺陷引起的(C)
A、设计了三层 WEB 架构,但是软件存在 SL 注入漏洞,导致被黑客攻击后能直接访问数据库
B、使用 C 语言开发时,采用了一些存在安全问题的字符串处理函数,导致存在缓冲区溢出漏洞
C、设计了缓存用户隐私数据机制以加快系统处理性能,导致软件在发布运行后,被黑客攻击获取到用户隐私数据
D、使用了符合要求的密码算法,但在使用算法接口时,没有按照要求生成密钥,导致黑客攻击后能破解并得到明文数据

238、GBT18336 的最低级别是(A)
A. ELA1
B、ELA3
C. ELA5
D、ELA7

239、在信息安全管理体系的实施过程中,管理者的作用对于信息安全管理体系能否成功实施非常重要,但是以下选项中不属于管理者应有职责的是(D)
A、制定并颁布信息安全方针、为组织的信息安全管理体系建设指明方向并提供总体纲领,明确总体要求
B、确保组织的信息安全管理体系目标和相应的计划得以制定目标应明确.可度量,计划应具体.可实施
C、向组织传达满足信息安全的重要性,传达满足信息安全要求、达成信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性
D、建立健全信息安全制度,明确安全风险管理作用施信息安全风险评估过程,确保信息安全风险评估技术选择合理、计算正确

240、鉴别是用户进入系统的第一道安全防线。用户登录系统时,和密码就是对用户身份进行鉴别。鉴别通过,即可以实现两的连接。例如,一个用户被服务器鉴别通过后,则被服务器用户,才可以进行后续访问。鉴别是对信息的一项安全属性该属性属于下列选项中的(C)

A、保密性

B、可用性

C、真实性

D、完整性

241、某银行网上交易系统开发项目在设计阶段分析系统运行过程中可能存在的攻击,请问以下哪一项工作不能降低该系统的受攻击面 (D)

A.分析系统功能的重要性

B.分析从哪里可以访问这些功能

C.采取合理措施降低特权

D.分析系统应满足的性能要求

242、小李和小刘需要为公司新建的信息管理系统设计访问控制方法,他们在讨论中针对采用自主访问控制还是强制访问控制产生了分歧小李认为应该采用自主访问控制的方法,他的观点主要有:(1)自主访问控制可为用户提供灵活、可调整的安全策略,具有较好的易用性和可扩展性;(2)自主访问控制可以抵御木马程序的攻击。小刘认为应该采用强制访问控制的方法,他的观点主要有:(3)强制访问控制中,用户不能通过运行程序来改变他自己及任何客体的安全属性,因为安全性较高;(4)强制访问控制能够保护敏感信息。请问以上四种观点中,正确的是 (A)

A 观点(1)

B 观点(2)

C 观点(3)

D 观点(4)

243、在国家标准《信息系统安全保障评估框架第部分:简介和一般模型》(GBT202741-2006)中描述了信息系统安全保障模型,下面对这个模型理解错误的是(D)

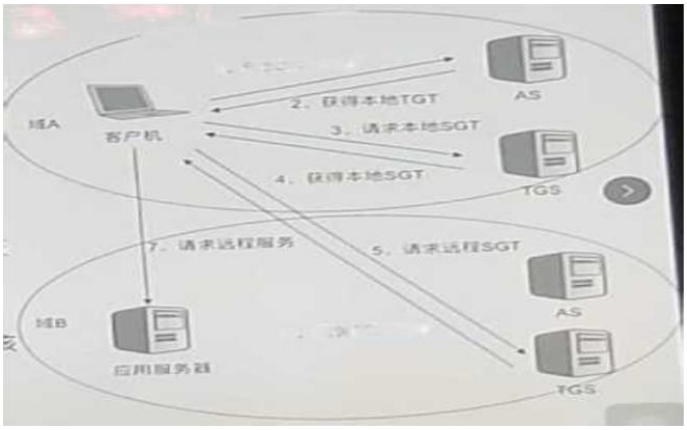
A、该模型强调保护信息系统所创建、传输、存储和处理信息的保密性、完整性和可用性等安全特征不被破坏,从而达到实现组织机构使命的目的

B、该模型是一个强调持续发的动态安全模型即信息系统安全保障应该贯穿于整个信息系统生命周期的全过程

C、该模型强调综合保障的观念,即信息系统的安全保障是通过综合技术、管理、工程和人员的安全保障来实施和实现信息系统的安全保障目标

D、模型将风险和策略作为信息系统安全保障的基础和核心,基于 IATF 模型改进,在其基础上增加了人员要素,强调信息安全的自主性

244、下列选项中,对图中出现的错误描述正确的是(B)



A. 步骤 1 和 2 发生错误,
B. B.步骤 3 和 4 发生错误
C.步骤 5 和 6 发生错误
D.步骤 5 和 6 发生错误

245、TCP/IP 协 X nternetilr=议是 einternet 构成的基础, TCP/IP 通常被认为是一个 N 层协议,每层都使用它的下一层所提供的网络服务来完成自己的功能,这里 N 应等于 (A)
A、4
B、5
C、6
D、7

246、 Linux 系统的安全设置中,对文件的权限操作是一项关键操作。通过对文件权限的设置,能够保障不同用户的个人隐私和系统安全。文具 fib.c 的文件属性信息如下图所示,小张想要修改其文件权限,为文件属主增加执行权限,并删除组外其他用户的写权限,那么以下操作中正确的是(C)
A. #chmod u+x a-w fib. C
B. #chmod ug+x, o-w fib
C. #chmod 764 fib. c
D. Chmod 674 fib.C

247、在工程实施阶段,以下哪一项不属于监理机构的监理重点: (C)
A、督促承建单位严格按照经审批的实施方案进行施工
B、审查承建单位施工人员的身份与资格
C、部署工程实施人员安全管理措施
D、督促承建单位严格遵守业主单位相关安全管理规

248、微软提出了 striderrepudiation(抵赖)的缩写 R,关于此项安全要求,下面说法错误的是 (D)
A.某用户在登录系统并下载数据后,却声称“我没有下载过数据”,软件系统中的这种威胁属于 R 成胁
B.某用户在网络通信中传输完数据后,却声称“这些数据不是我传输的“,软件系统中的这种威胁属于 R 威胁
C、对于 R 成胁,可以选择使用如强认证、数字签名,安全审计等技术措施来解决
D、对于 R 威胁,可以选择使用如隐私保护、过滤、流量控制等技术措施来解决

249、风险分析是风险评估工作中的一个重要内容,GB3T20984-2007 在资料性附录中给出了一种矩阵法来计算信息安全风险大小,其中风险计算矩阵如下图所示,请为途中括号空白处选择合适的内容 (D)

		安全事件发生可能性				
		1	2	3	4	5
	1	3	6	9	12	16
	2	5	8	11	15	18
( )	3	6	9	13	17	21
	4	7	11	16	20	23
	5	9	14	20	23	25

A、安全资产价值大小等级
B、脆弱性严重程度等级
C、安全风险隐患严重等级
D 安全事件造成损失大小

250、 Ipsec(IP Security)协议标准的设计目标是在 IPv4 和 Pv6 环境中为网络层流量提供灵活、透明的安全服务,保护 TCP/IP 通信免遭窃听和改,保证数据的完整性和机密性下面选项中哪项描述是错误的 (A)

A、 Ipsec 协议不支持使用数字证书

B、 I Psec 协议对于 IPv4 和 Pv6 网络都是适用的

C、 II Psec 有两种工作模式:传输模式和隧道模式

D、 Ipsec 协议包括封装安全载荷(ESP)和鉴别头(AH)两种通信保护机制

251、某电子商务网站架构设计时,为了避免数据误操作,在管理员进行订单删除时,需要由审核员进行审核后该操作才能生效,这种设计是遵循了以下哪个原则:(A)

A、权限分离原则

B、最小特权原则

C、保护最薄弱环节的原则

D、纵深防御的原则

252、安全漏洞产生的原因不包括以下哪一点 (D)

A.软件系统代码的复杂性

B.软件系统市场出现的信息不对称现象

C.复杂异构的网络环境

D.攻击者的恶意利用

253、关于计算机取证描述不正确的是 (C)

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:通过证据查找肇事者、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

254、小李是某公司的系统规划师,某天他针对公司信息系统的现状,绘制了一张系统安全建设规划图,如下图所示,请问这个图形是依据下面哪个模型来绘制的 (B)

A、PDRB

B、PPDR

C、PDCA

D. IATF

255、某攻击者想通过远程控制软件潜伏在某监控方的 Unix 系统的计算机中,如果攻击者打算长时间地远程监控某服务器上的存储的敏感数据,必须要能够清除在监控方计算机中存在的系统日志。否则当监控方查看己的系统日志的时候,就会发现被监控以及访问的痕迹。不属于清除痕迹的方法是 (C)

A、窃取 root 权限修改 wtmp/ wtmpxutmpx 和 Q1 astro 三个主要日志文件

B、采用干扰手段影响系统防火墙的审计功能

C、保留攻击时产生的临时文件

D、修改登录日志,伪造成功的登录日志,增加审计难度

256、某公司拟建设面向内部员工的办公自动化系统和面向外部客户的营销系统通过公开招标选择 M 公司为承建单位并选择了 H 监理公司承担该项目的全程监理工作,目前各个应用系统均已完成开发 M 公司已经提交了验收申请监理公司需要对 A 公司提交的软件配置文件进行审查在以下所提交的文档中哪一项属于开发类文档 (D)

A.项目计划

B.质量控制计划

C.评审报告

D.需求说明书

257、以下 SQL 语句建立的数据库对象是 (B)

4 Create View Patients Fordocotors As

◆ Select Patient

FROM Patient. Docotor

◆ Where docotorld=123

A.表

B.视图

258、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 HTP 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。可以看出,这个鉴别过程属于(A)

A、单向鉴别

B、双向鉴别

C、三向鉴别

D、第三方鉴别

259、某银行网上交易系统开发项目在设计阶段分析系统运行过程中可能存在的攻击,请问以下拟采取的安全措施中,哪一项不能降低该系统的受攻击面:(B)

A、远程用户访问需进行身份管

B 远程用户访问时具有管理员权限

C 关闭服务器端不必要的系统服务

D 当用户访问其账户信息时使用严格的身份认证机制

260、某银行有 5 台交换机连接了大量交易机构的网络,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)

A、VLAN 划分

B、动态分配地址

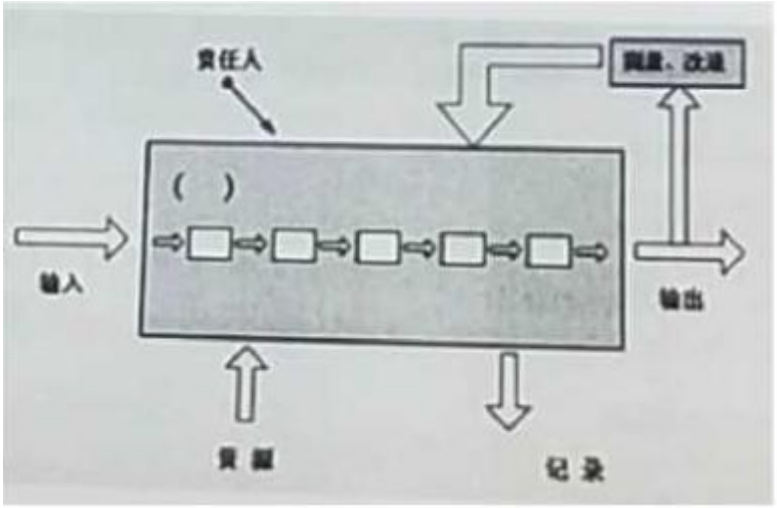
C、为路由交换设备修改默认口令
D、设立入侵防御系统

261、以下哪一项不是我国信息安全保障工作的主要目标(C)
A.保障和促进信息化发展
B.维护企业和公民的合法权益
C.构建高效的信息传播渠道
D.保护互联网知识产权

262、某公司中标了某项软件开发项目后,在公司内部研讨项目任务时,项目组认为之前在 VPN 技术方面积累不够,导致在该项目中难以及时完成 VPN 功能模块,为解决该问题,公司高层决定接受该项目任务,同时将该 VPN 功能模块以合同形式委托另外一家安全公司完成,要求其在指定时间内按照任务需求书完成工作,否则承担相应责任。在该案例中公司高层采用哪种风险处理方式 (C)
A、风险降低
B、风险规避
C、风险转移
D、风险接受

263、在工程实施阶段,监理机构依据承建合同、安全设计方案、实施方案、实施记录、国家或地方相关标准和技术指导文件,对信息化工程进行安全检查,以验证项目是否实现了项目设计目标和安全等级要求 (D)
A、功能性
B、可用性
C、保障性
D、符合性

264、S09001-2000 标准鼓励在制定、实施质量管理体系以及改进其有效性时对采用的过程方法,通过满足顾客要求增进顾客满意,下图是关于过程方法示意图,空白处应填写 (D)



A、策略
B、管理者
C、组织
D、活动

265、作为信息安全从业人员,以下那种行为违反了 CISP 职业道德准则(B)
A.抵制通过网络系统侵犯公众合法权益
B.通过公众网络传播非法软件

C.不在计算机网络系统中进行造谣、欺诈、诽谤等活动
D.帮助和指导信息安全同行提开信息安全保障知识和能力

266、小李在学习信息安全管理体系(nformation Socurity Management System,lSMS)的有关知识后,按照自己的理解画了一张图来描述安全管理过程,但是他还存在一个空白处未填写,请帮他选择一个最合适的选项(B)
A.监控和反馈 ISMS
B.实施和运行 ISMS
C.执行和检查 ISMS
D.沟通和咨询 ISMS

267、规范的实施流程和文档管理,是信息安全风险评估性能否取得成果的重要基础。某单位在实施风险评估时,形成了《风险评估方案》并得到了管理决策层的认可。在风险评估实施的各个阶段中,该《风险评估方案》应是如下()中的输出结果。(A)
A.风险评估准备阶段
B.风险要素识别阶段
C.风险分析阶段
D.风险结果判定阶段

268、若一个组织声称自己的 ISMS 符合 ISO/EC27001 或 GB/T22080 标准要求,其信息安全控制措施通常要在物理和环境安全方面实施规划控制,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,关键或敏感的信息以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实现,下列不包括哪一项(D)
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.在安全区域工作,公共访问、交接区安全
D 人力资源安全

269、IPV4 协议在设计之初并没有过多地考虑安全问题,为了能够使网络方便地进行互联、互通,仅仅依靠 IP 头部的校验和字段来保证 IP 包的安全,因此 P 包很容易被篡改,并重新计算校验和, I=TR-于 1994 年开始制定 Psec 协议标准,其设计目标是在 IPV4 和 PV6 环境中为网络层流量提供灵话、透明的安全服务,保护 TTCP/P 通信免遭窃听和篡改,保证数据的完整性和机密性,有效抵御网络攻击,同时保持易用性,下列选项中说法错误的是(C)
A、对于 IPv4, Ipsec 是可选的,对于 IPv6,ISec 是强制实施的
B. Ipsec 协议提供对 IP 及其上层协议的保护
C. Ipsec 是一个单独的协议。
D.ISec 安全协议给出了封装安全载荷和鉴别头两种通信保护机制

270、在信息系统中,访向控制是重要的安全功能之一。它的任务是在用户对系统资源提供最大限度共享的基础上,对用户的访何权限进行管理,防止对信息的非授权篡改和滥用。访问控制模型将实体划分为主体和客体两类,通过对主体身份的识别来限制其对客体的访问权限。下列选项中,对主体、客体和访问权服的描述中错误的是(D)
A.对文件进行操作的用户是一种主体
B.主体可以接收客体的信息和数据,也可能改变客体相关的信息
C.访向权限是指主体对客体所允许的操作
D.对目录的访问权展可分为读、写和拒绝访问

271、强制访问控制系统是指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,具有较高的安全性,适用于专用或对安全性要求较高的系统,强制访问控制模型有多种类

型,如 BLP、 Clark- Wilison 和 Chinesewall 等。小李自学了 BLP 模型,并对该模型的特点进行了总结,以下四种对 BLP 模型的描述中,正确的是(B)

A.BLP 模型用于保证系统信息.的机密性,规则是“向上读,向下写”

B.BLP 模型用于保证系统信息的机密性,规则是“向下读,向上写

模型用于保证系统信息的完整性,规则是“向上读,向下写”

D.BLP 模型用于保证系统信息的完整性,规则是“向下读,向上写"

272、入侵检测系统有其技术优越性,但也有其局限性,下列说法错误的是(A)

A.对用户知识要求高,配置、操作和管理使用过于简单,容易遭到攻击

B.高虚警率,入侵检测系统会产生大的警告消息和可疑的入慢行为记录,用户处理负担很重

C.入侵检测系统在应对自身攻击时,对其他数据的检测可能会被抑制成者受到影响

D.警告消息记承如果不完整,可能无法与入侵行为关联

273、小王在学习定风险评估方法后,决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值为 400 元人民币,暴漏系数(xposure factor,)是 25%,年度发生率 annualizd rate of Occurrence.ARO)为 0.2 那么小王计算的年度预期损失 Annualized Loss Expectancy, ALE)应该是(C)

A.100 万元人民

B.400 万元人民币

C、20 万元人民币

D、180 万元人民币

274、小王在学习定量风险评估方法后,决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格为 200 万元人民币,暴漏系数(Foposurefactor,EF)是 25%,年度发生率 annualized rate of0 ccurrencearo)为 0.1,那么小王计算的年度预期损失 Annualized Loss Expectancy, AE)应该是(A)

A.5 万元人民币

B.50 万元人民币

C.2.5 万元人民币

D.25 万元人民币

275、GPT18336《信息技术安全性评估准则》是测评标准中的重要标准,该标准定义了保护轮廓(protectionprofile, pp)和安全目标(security target.st)的评估准则。提出了评估保证级(evaluationassurance evel。eal)期评估保证级共分为()个递增的评估保证等级 (D)

A、4

B、5

C、6

D、7

276、某集团公司更具业务需要,在各地分支机构部署前置机,为了保证安全,将集团总部要求前置机开放日志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? (D)

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,但不能响系统使用,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 P 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

277、关于我国加强信息安全保障工作的主要原则,以下说法错误的是:(D)

A.立足国情,以我为主,坚持技术与管理并重

B.正确处理安全和发展的关系,以安全保发展,在发展中求安全

C.统筹规划,突出重点,强化基础工作
D.全面提高信息安全防护能力,保护公众利益,维护国家安全

278、在使用系统安全工程-能力成熟度模型(SSE -CMM)对一个组织的安全工程能力成熟度进行测量时,正确的理解是 (D)
A.测量单位是基本实施(base practices,bp)
B.测量单位是通用实施(Generic practices GP
C.测量单位是过程区域(Process Areas,PA)
D.测量单位是公开特征(common features,cf)

279、信息安全管理体系(ISMS)的建设和实施是一个组织的战略性举措。若一个组织声称自己的 ISKS 符合 1SO/IBC27001 或心 BT22080 标准要求,则需实施准要求,则需实施以下 ISMS 建设的各项工作,哪不属于 ISMS 建设的工作(D)
A.规划与建立 ISMS
B.实施和运行 ISMS
C.监视和评审 ISMS
D.保持和审核 ISMS

280、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)
A.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篡改和滥用

281、目前,很多行业用户在进行信息安全产品选项时,均要求产品高通过安全测评。关于信息安全产品测评的意义,下列说法中不正确的是:(D)
A.有助于建立和实施信息安全产品的市场准入制度
B.对用户采购信息安全产品,设计、建设、使用和管理安全的信息系统提供科学公正的专业指导
C.对信息安全产品的研究、开发、生产以及信息安全服务的组织提供严格的规范引导和质量监督
D.打破市场垄断,为信息安全产业发展创造一个良好的竞争环境

282、风险计算原理可以用下面的范式形式化地加以说明风险值 R(A,T,V)=R(L(TV)F(IaVa)以下关于上式各项说明错误的是 (D)
A.R 表示安全风险计算函数,A 表示资产,T 表示威胁,V 表示脆弱性
B.L 表示成胁利用资产脆弱性导致安全事件的可能性
C.P 表示安全事件发生后造成的损失
D.Ia,Va 风别表示安全事件作用全部资产的价值与其对应资产的严重程度

283、IP 地址用来标识不同的网络、子网以及网络中的主机。所谓 P 地址规划。是推根据 P 编址特点,为所设计的网络中的节点、网络设备分配合适的 P 地址。如某个小型网络拥有 10 个与互联网直接连接的 P 地址,但是该网络内有 15 台个人计算机假如这些计算机不会同时开机并连接互联网,那么可以将这 10 个互联网地址集中起来使用,当任意一台个人计算机开机并连接网络时,管理中心从这10个地址中任意抽取个尚未分配的 IP 地址分配给这台计算机。他关机时,管理中心将该地址收回,并重新设置为未分配。那么上述的 P 地址分配方式属于(A)
A.动态分配地址
B.静态分配地址

C.NAT 池分配地址
D.端口 MT 分配地址

284、P2DR 模型是一个用于描述网络动态安全的模型,这个模型经常使用图形的形式来形象表达,如下图所示,请问图中空白处应填写是(B)

A.执行(do)B.检测(detection)

C.数据(data)
D.持续(duration)

285、小陈某电器城购买了一台冰箱,并留下了个人姓名、电话和电子邮件地址等信息,第二天他收了一封邮件他中奖的邮件,查看该邮件后他按照提示操作缴纳中奖税款后并没有得到中奖金,再成才得知电器城共没有中奖的活动、在此案例中,下面描述量误的是 (D)
A 小陈应当注意保护自已的隐私,没有必要告诉别人的信息不要登记和公和给别人
B.小陈钱被偷走了,这类网络犯罪哪案件也应该向公安局报案
C.邮件服务运营高商通过技术手段,可以在一定程度上阻止此类的钓鱼邮件和明哄骗邮件
D、小陈应当向电器城索,追回损失

286、下列选项中,哪个不是我国信息安全保障工作的主要内容 (B)
A.加强信息安全标准化工作,积极米用“等同采用、修改采用.制定”等多种方式,尽快建立标准体系
B.建立国家信息安全研究中心,加快建立国家急需的信息安全技术体系,实现国家信息安全自主可控目标
C.建设和完善信息安全基础设施,提供国家信息安全保障能力支撑
D.加快信息安全学科建设和信息安全人才培养

287、有关能力成熟度模型(),错误的理解是 (A)
A.CMM 基本思想是,因为问题是由技术落后引起的所以新技术的运用会在一定程度上提高质量.生产率和利润率
B.CM 的思想来源于项目管理和质量管理
C.CM 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.CM 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

288、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? (C)
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列》
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意见》

289、关于恶意代码的守护程序的功能,以下说法正确的是: (A)
A.隐藏恶意代码
B.加大监测力度
C.传播恶意代码
D.监视悉意代码主体程序是否正常

290、实体身份鉴别的方法多种多样,且随着技术的进步,鉴别方法的强度不断提高,常见的方法有利用口令鉴别、令牌鉴别、指纹鉴别等。如图,小王在登录某移动支付平台时,首先需要通过指纹对用户身份进行鉴别。通过鉴别后,他才能作为合法用户使用自己的账户进行支付、转账等 (C)
A、实体所知的鉴别方法
B、实体所有的鉴别方法
C、实体特征的鉴别方法
D、实体所见的鉴别方法

291、某单位门户网站发完成后,测试人员使用模糊测试进行安全性测试,以下关于模糊试过程的说法正确的是 (D)
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

292、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一1 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: (C)
A、最小特权原则
B、职责分离原则
C、纵深防御原则
D、最少共享机制原贝

293、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,形成了《待评估信息系统相关设备及资产清单》。在风险评估实施的各个阶段中,该《待评估信息系统相关设备及资产清单》应是如下0)中的输出结果。(B)
A、风险评估准备
B、风险要素识别
C、风险分析
D、风险结果判定

294、在实施信息安全风险评估时,需要对资产的价值进行识别、分类和赋值,关于资产价值的评估,以下选项中正确的是 (C)
A、资产的价值指采购费用
B、资产的价值指维护费用
C、资产的价值与其重要性密切相关

D、资产的价值无法估计

295、 SO 27002(nformation technology- Securtiy Techniques-code of practice for informationmanagement)是重要的信息安全管理标准之一,下图是关于其演进变化示意图,途中括号空白处应填写?(B)

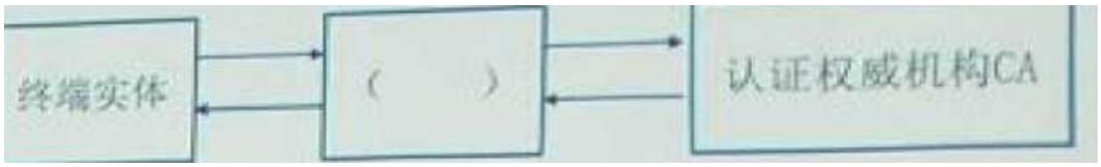
BS7799 —— Bs7799.1 ( ) -------▶ iso27002

A.B.7799.1.3
B.IS017799
C AS/NZS4630
C. NST SP800-17

BS7799 管理措施, BS7799.2 信息安全要求-ISO27001
BS7799 管理措施-BS7799.1->ISO 17799 -> ISO27002

296、由于频繁出现软件运行时被黑客远程攻获取数据的现象,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)
A、要求开发人员采用捷开发型进行开发
B、要求所有的开发人员参加软件安全意识培训
C、要求规范软件编码,并定公司的安全编码准则
D、要求增加软件安全测试环节,早发现软件安全问题

297、公钥基础设施(Public Key Infrastructure,PKI)引入数字证书的概念,用来表示用户的身份。下图简要地描述了终端实体(用户)从认证权威机构 CA 申请、撤销和更新数字证书的流程。请为中间框空白处选择合适的选项 (B)



A、证书库
B、RA
C、OCSP
D、CRL 库

298、软件存在洞和缺陷是不可避免的,实践中常使用软件缺陷密度(Defects/KLOC)来衡量软件的安全性,假设某个软件共有 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(B)
A、0.00049
B、0.049
C.0.49
D.49

299、对《网络安全法》中网络运行安全生产影响的攻击行为主要是对以下那个信息安全属性造成影响?(C)
A、保密性
B、完整性
C、可用性
D、不可抵赖性

300、 TCP/IP 协议族是为实现异构网互联推出的协议规范,具有较好的开放性, internet 是在 TCP/P 协议族的基础上构建的。但由于 TCP/P 协议族在设计初期过于关注其开放性和便利性,对安全性考虑较少,因此

其中很多协议存在安全隐患,例如,攻击者可以利用 TCP 协议的三次握手机制实现 DS 攻击,也可以通过猜测 TCP 会话中的序号来伪造数据包那么上述例子中的情况可能发生在(B)

A、应用层

B、传输层

C、网络层

D、链路层