1. 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（ ）

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 ISO9001 认证

答案：D

2. 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（）。

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有冗余空间，满足业务高峰期和业务发展需求

答案：C

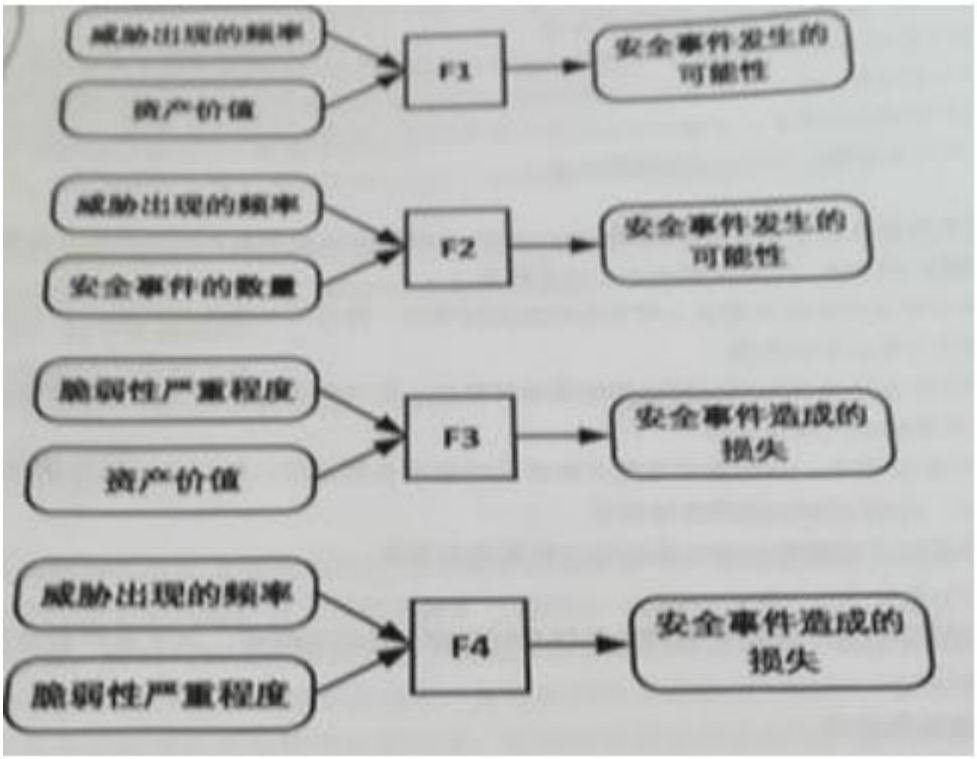
3. 小陈自学了风评的相关国家准则后，将风险的公式用图形来表示，下面 F1，F2，F3，F4 分别代表某种计算函数，四张图中，那个计算关系正确

A

B

C

D



答案：C

4. 在网络信息系统建设中部署防火墙，往往用于提高内部网络的安全防护能力。某公司准备 部署一台防火墙来保护内网主机，下列选项中部署位置正确的是（）

A. 内网主机——交换机——防火墙——外网 B. 防火墙——内网主机——交换机——外网 C. 内网主机——防火墙——交换机——外网 D. 防火墙——交换机——内网主机——外网 答案：A

5. 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（）

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、BSI 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

答案：B

6. 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、ACL 只能由管理员进行管理

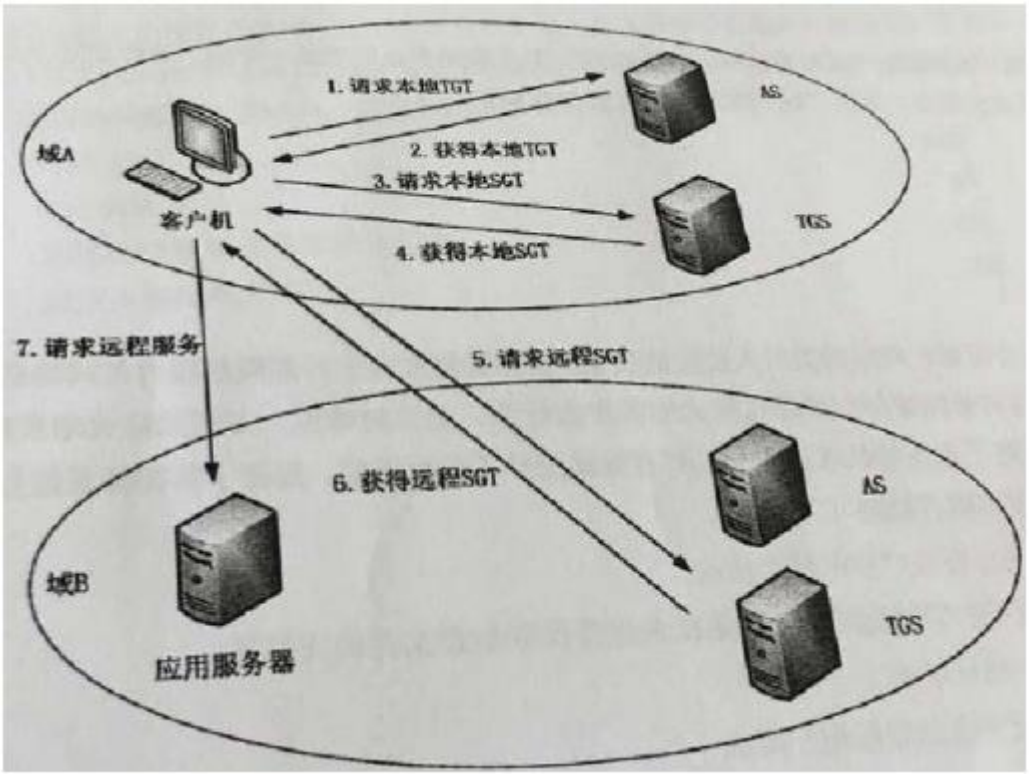
B、ACL 是对象安全描述的基本组成部分，它包括有权访问对象的用户和级的 SID

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

答案：A

7. 在现实的异构网络环境中，越来越多的信息需要实现安全的互操作。即进行跨域信息交换 和处理。Kerberos 协议不仅能在域内进行认证，也支持跨域认证，下图显示的是 Kerberos 协议实现跨域认证的 7 个步骤，其中有几个步骤出现错误，图中错误的描述正确的是：



A.步骤 1 和步骤 2 发生错误，应该向本地 AS 请求并获得远程 TGT

B.步骤 3 和步骤 4 发生错误，应该向本地 TGS 请求并获得远程 TGT

C.步骤 5 和步骤 6 发生错误，应该向远程 AS 请求并获得远程 TGT

D.步骤 5 和步骤 6 发生错误，应该向远程 TGS 请求并获得远程 TGT

答案：B

8. 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（）

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

答案：D

9. 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（） 攻击。

A、默认口令

B、字典

C、暴力

D、XSS

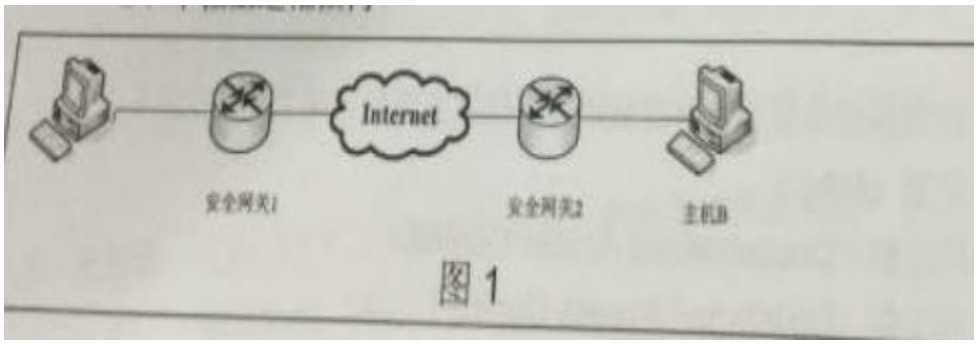
答案：B

10. 下图中描述网络动态安全的 P2DR 模型，这个模型经常使用图形的形式来表达的下图空白 处应填（）

A.策略 B.方针 C.人员 D.项目

答案：A

11.如图所示，主机 A 向主机 B 发出的数据采用 AH 或者 ESP 的传输模式对流量进行保护时， 主机 A 和主机 B 的 IP 地址在应该在下列哪个范围?



A.10.0.0.0~10.255.255.255

B.172.16.0.0~172.31.255.255

C.192.168.0.0~192.168.255.255

D.不在上述范围内

答案：D

12.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（）

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、系统通过比较客体攻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控制措施

答案：D

13.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 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

14.模糊测试，也称 Fuzz 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、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

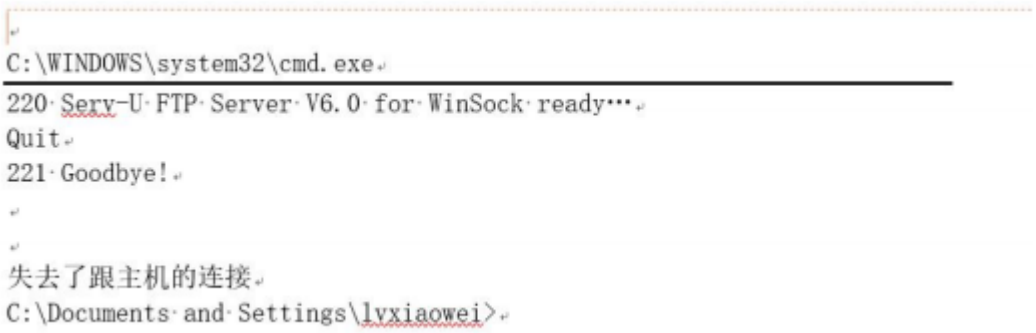
答案：A

15.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（）

A、任用之前 B、任用中 C、任用终止或变化 D、任用后

答案：D

16.下图是安全测试人员连接某远程主机时的操作界面，请您仔细分析该图，下面分析推理正确的是（）



A.安全测试人员链接了远程服务器的 220 端口

B.安全测试人员的本地操作系统是 Linux

C.远程服务器开启了 FTP 服务，使用的服务器软件名 FTP SERVER

D.远程服务器的操作系统是 windows 系统

答案：D

17.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（）

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

答案：C

18.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。请问这意味着（）

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

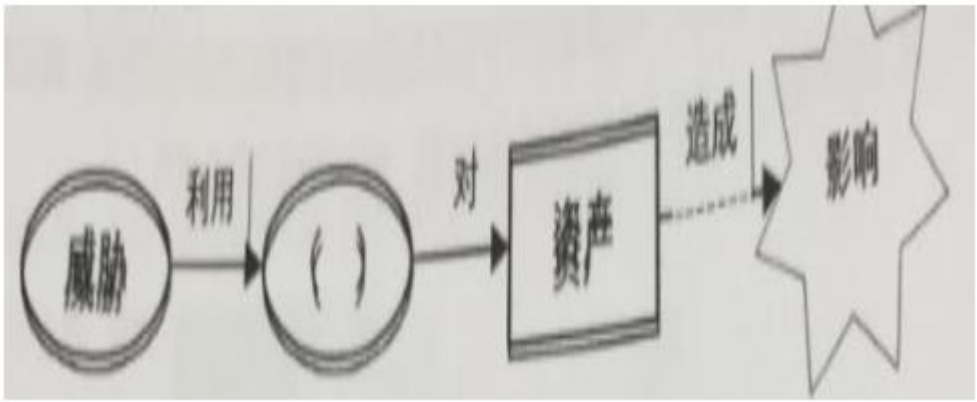
B、该信息系统发生重大安全事件后，工作人员应在 3 小时内完整应急处理工作并恢复对 外运行

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

答案：D

19.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，有五个方面：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，图中空白处应填写？



A. 信息载体　　B.措施

C.脆弱性　　D.风险评估

答案：C

20.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、安全凭证　　B、用户名

C、加密密钥　　D、会话密钥

答案：A

21.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. 在安全区域工作。公共访问、交接区安全

D．人力资源安全

答案：D

22.风险分析师风险评估工作的一个重要内容，GB/T 20984-2007 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，如下图所示，图中括号应填那

个?

		安全事件发生可能性				
		1	2	3	4	5
资产价值	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

答案：D

23.关于信息安全管理体系的作用，下面理解错误的是

A．对内而言，有助于建立起文档化的信息安全管理规范，实现有“法”可依，有据可查

B．对内而言，是一个光花钱不挣钱的事情，需要组织通过其他方法收入来弥补投入

C．对外而言，有助于使各科室相关方对组织充满信心

D．对外而言，规范工作流程要求，帮助界定双方各自信息安全责任

答案：B

24.关于补丁安装时应注意的问题，以下说法正确的是

A． 在补丁安装部署之前不需要进行测试，因为补丁发布之前厂商已经经过了测试

B． 补丁的获取有严格的标准,必须在厂商的官网上获取

C． 信息系统打补丁时需要做好备份和相应的应急措施

D． 补丁安装部署时关闭和重启系统不会产生影响

答案:C

25.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 核员进行审核后该删除操作才能生效，这种设计是遵循了发下哪个原则

A．权限分离原则

B．最小的特权原则

C．保护最薄弱环节的原则

D．纵深防御的原则

答案: A

26.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 法有指令鉴别、令牌鉴别、指纹鉴别等。如图，小王作为合法用

户使用自己的账户进行支 付、转账等操作。这说法属于下列选项中的（）

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

答案：C

27.定量风险分析是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，准确 度量风险的可以性和损失量。小王采用该方法来为单位机房计算火灾风险大小，假设单位 机房的总价值为 200 万元人民币，暴露系数（ExposureFactor,EF）是 x,年度发生率（Annual izod Eato of Occurrence,ARO）为 0.1，而小王计算的年度预期损失（Annual izod Loss Erpectancy,ALE）值为 5 万元人民币，由此，x 值应该是

A．2.5%　　B．25%

C．5%　　D．50%

答案: B

28.关于 Kerberos 认证协议，以下说法错误的是:

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

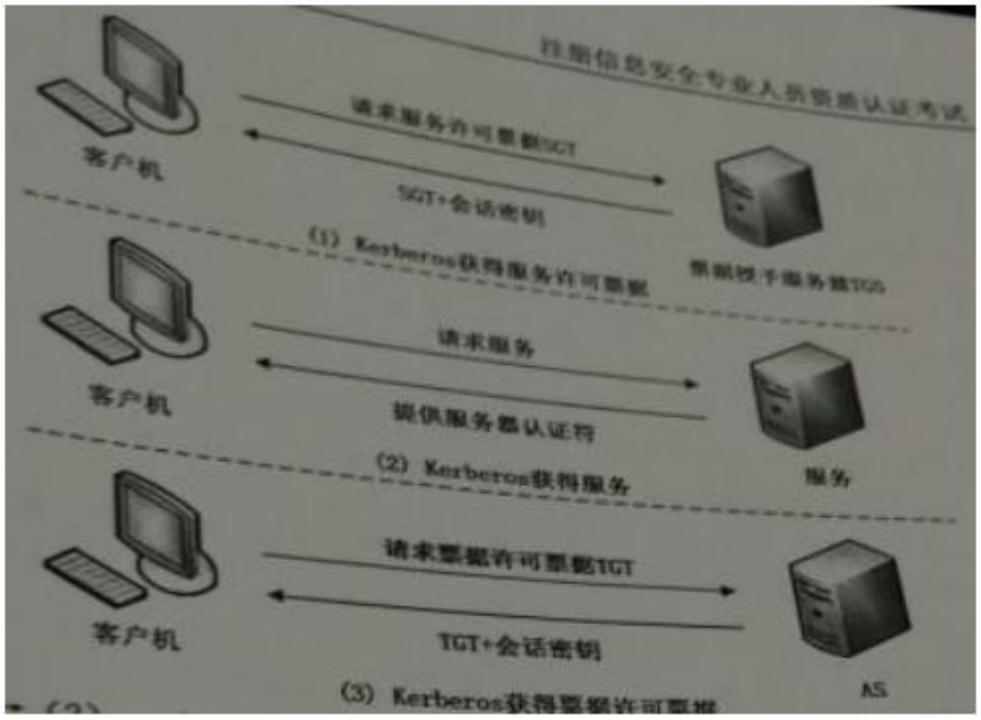
B.认证服务器（AS）和票据授权服务器（TGS）是集中式管理，容易形成瓶颈，系统的性 能和安全也严重依赖于 AS 和 TGS 的性能和安全

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

答案：C

29.kerberos 协议是常用的集中访问控制协议,通过可信第三的认证服务,减轻应用 Kerberos 的运行环境由秘钥分发中心（KDC)、应用服务器和客户端三个部分组成，认证服务器 AS 和票据授权服务器



A.1——2——3　　B.3——2——1

C.2——1——3　　D.3——1——2

答案：D

30.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:

A.强制访问控制　　B.基于角色的访问控制

C.自主访问控制　　D.基于任务的访问控制

答案：C

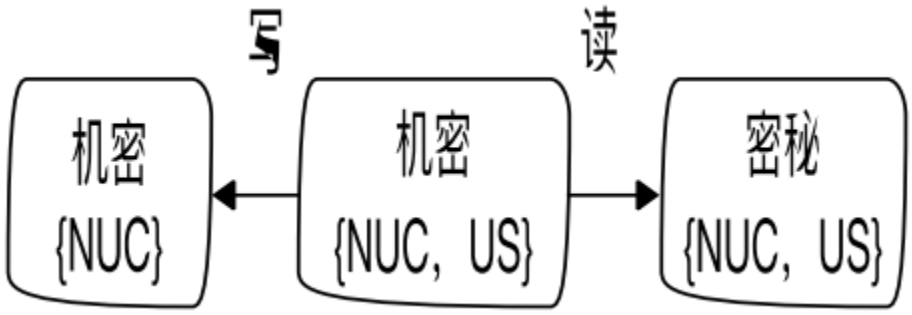
31.由于 Internet 的安全问题日益突出，基于 TCP/IP 协议，相关组织和专家在协议的不同层 次设计了相应的安全通信协议，用来保障网络各层次的安全。其中，属于或依附于传输层的安全协议是（）

A. PP2P　　B. L2TP

C. SSL　　D. IPSec

答案：C

32.根据 Bell-LaPedula 模型安全策略，下图中写和读操作正确的是（ ）



A. 可读可写　　B.可读不可写

C.可写不可读　　D.不可读不可写

答案：B

33.防火墙是网络信息系统建设中常采用的一类产品，它在内外网隔离方面的作用是（）。

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

答案：C

34.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.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 与原来用户 zhang 是同一个用户，因此无权访问

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

答案：B

35.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:

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

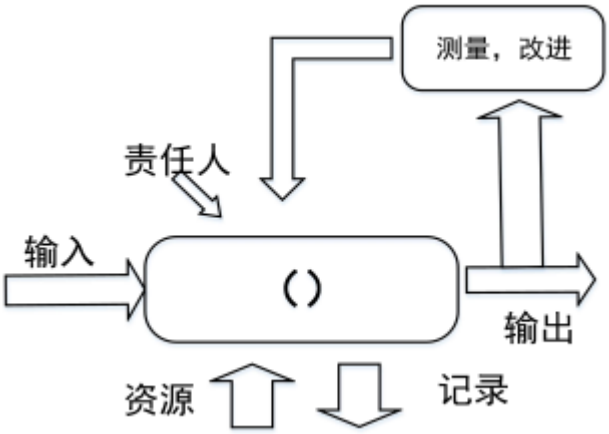
B.存储在注册表中的账号数据只有 administrator 账户才有权访问，具有较高的安全性

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

答案：D

36.ISO9001-2000 标准在制定、实施质量管理体系以及改进其有效性时采用过程方法，通过满足顾客要求增进顾客满意。下图是关于过程方法的示意图，图中括号空白处应填写（）

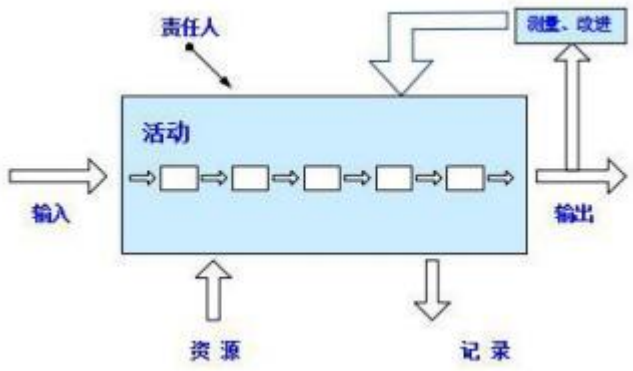


A.策略　　B.管理者

C.组织　　D.活动

答案：D

解释知识点如下：



38.在设计信息系统安全保障方案时，以下哪个做法是错误的：

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

答案：C

39.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:

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

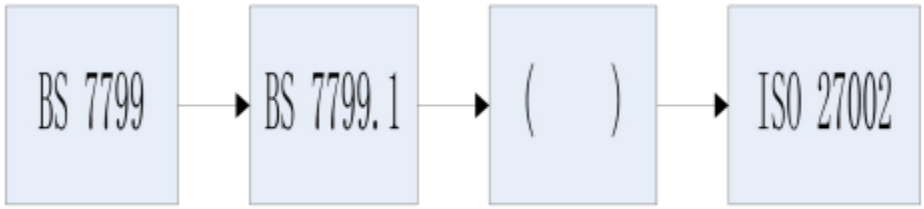
B.由于 Windows 操作系统自身有大量的文件和目录，因此很难对每个文件和目录设置严格 的访问权限，为了使用上的便利，Windows 上的 ACL 存在默认设置安全性不高的问题

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

答案：C

40.ISO27002 （ Information technology-Security techniques0Codeofpratice for inforeation security managcacnt）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，图中括号空白处应填写（）



A.BS 7799.1.3　　B.ISO 17799

C.AS/NZS 4630　　D.NIST SP 800-37

答案：B

41.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（）

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

答案：D

42.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:

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

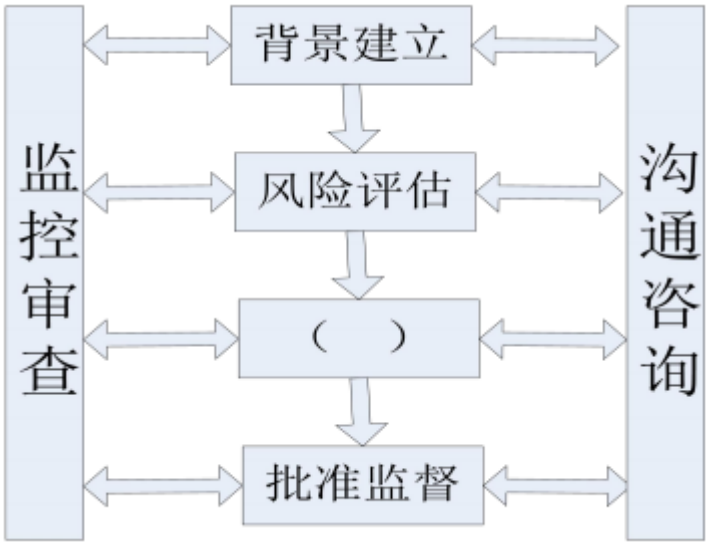
B.最大共享策略，在保证数据库的完整性、保密性和可用性的前提下，最大程度也共享数 据库中的信息

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

答案：B

43.我国标准《信息安全风险管理指南》（GB/Z24364）给出了信息安全风险管理的内容和过 程，可以用下图来表示。图中空白处应该填写（）



A.风险计算　　B.风险评价

C.风险预测　　D.风险处理

答案：D

44.以下哪一项不是信息系统集成项目的特点：

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

答案：B

45.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（）

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

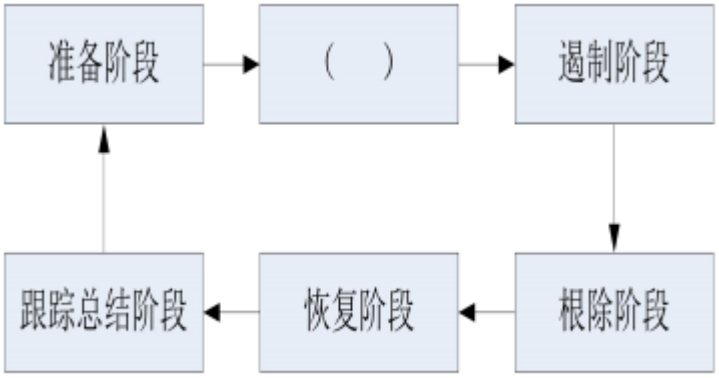
B.检查评估可以由上级管理部门组织，也可以由本级单位发起，其重点是针对存在的问题 进行检查和评测

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

答案：B

46.为了能够合理、有序地处理安全事件，应事件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。PDCERF 方法论是一种防范使用的方法，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

47.关于信息安全管理，下面理解片面的是（）

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，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

答案：C

48.关于风险要素识别阶段工作内容叙述错误的是：

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

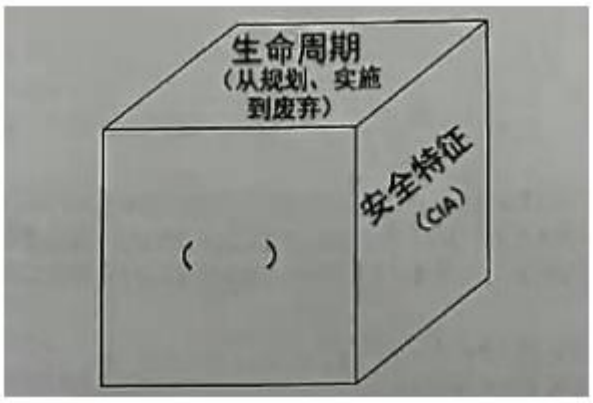
C.脆弱性识别以资产为核心，针对每一项需要保护的资产，识别可能被威胁利

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

答案：D

49.某学员在学习国家标准《信息系统安全保障评估框架第一部分：简介和一般模型》（GB/T 20274.1-2006）后，绘制了一张简化的信息系统安全保障模型图，如下所示。请为图中括 号空白处选择合适的选项（）



A.安全保障（方针和组织）

B.安全防护（技术和管理）

C.深度防御（策略、防护、检测、响应）

D.保障要素（管理、工程、技术、人员）

答案：D

50.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[2004]66 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哟的基本内容、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.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

答案：A

51.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

52.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。文件 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，为文件增加执行权限，并删除

组以外其他用户的写权限，那么以下操作中正确的是（）

A.#chmod u+x, a-w fib.c

B.#chmod ug+x, o-w fib.c

C.#chmod 764 fib.c

D.#chmod 467 fib.c

答案：C

53.关于信息安全事件管理和应急响应，以下说法错误的是：

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）

答案：B

54.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. 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，但 RPO 可以为 0

D. RTO 不可以为 0，RPO 也不可以为 0

答案：A

55.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（）

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

答案：C

56.通过对称密码算法进行安全消息传输的必要条件是:

A．在安全的传输信道上进行通信

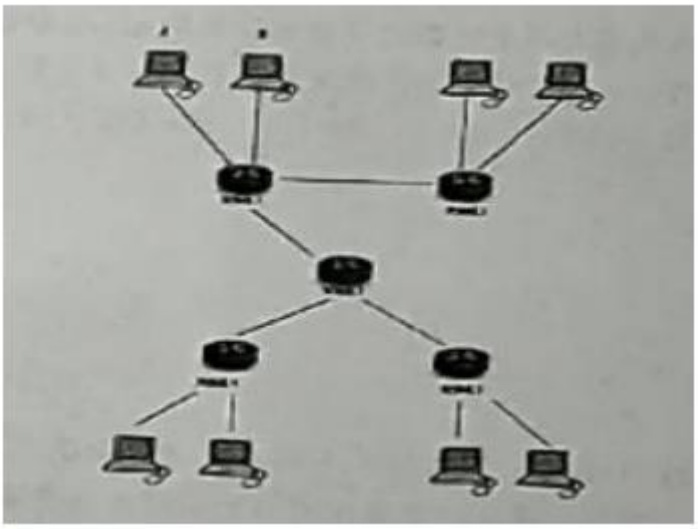
B．通讯双方通过某种方式，安全且秘密地共享密钥

C．通讯双方使用不公开的加密算法

D．通讯双方将传输的信息夹杂在无用信息中传输并提取

答案：B

57.某银行有 5 台交换机连接了大量交易机构的网路（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。没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.VLAN 划分　　B.动态分配地址

C.设立入侵防御系统　　D.为路由交换设备修改默认口令

答案：A

58.Windows 系统下，哪项不是有效进行共享安全的防护措施?

A．使用 netshare\\127.0.0.1\c$/delete 命令，删除系统中的 c$等管理共享，

并重启系统

B．确保所有的共享都有高强度的密码防护

C．禁止通过“空会话”连接以匿名的方式列举用户、群组、系统配置和注册表键值

D．安装软件防火墙阻止外面对共享目录的连接

答案：A

59.以下对 Windows 账号的描述，正确的是：

A．Windows 系统是采用 SID（安全标识符）来标识用户对文件或文件夹的权限

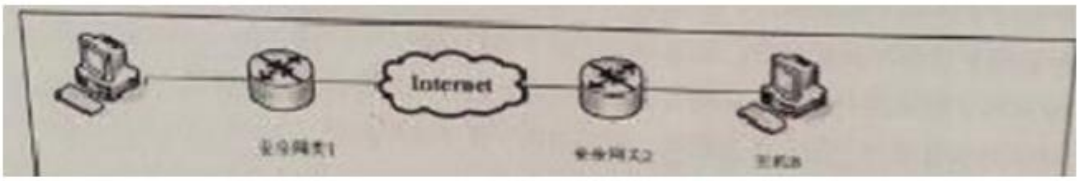
B．Windows 系统是采用用户名来标识用户对文件或文件夹的权限

C．Windows 系统默认会生成 administrator 和 guest 两个账号，两个账号都不允许改名和 删除

D．Windows 系统默认生成 administrator 和 guest 两个账号，两个账号都可以改名和删除

答案：A

60.如图一所示:主机 A 和主机 B 需要通过 IPSec 隧道模式保护二者之间的通信流量,这种情况 下 IPSec 的处理通常发生在哪二个设备中?



A.主机 A 和安全网关 1;

B.主机 B 和安全网关 2;

C.主机 A 和主机 B 中;

D.安全网关 1 和安全网关 2 中;

答案：D

61.以下关于代替密码的说法正确的是:

A．明文根据密钥被不同的密文字母代替

B．明文字母不变，仅仅是位置根据密钥发生改变

C．明文和密钥的每个 bit 异或

D．明文根据密钥作移位

答案：A

62.AES 在抵抗差分密码分析及线性密码分析的能力比 DES 更有效，已经替代 DES 成为新的据 加密标准。其算法的信息块长度和加密密钥是可变的，以下哪一种不是其可能的密钥长度?

A．64bit　　B．128bit

C．192bit　　D．256bit

答案：A

63. 以下对 Windows 系统的服务描述，正确的是:

A．Windows 服务必须是一个独立的可执行程序

B．Windows 服务的运行不需要用户的交互登陆

C．Windows 服务都是随系统启动而启动，无需用户进行干预

D．Windows 服务都需要用户进行登陆后，以登录用户的权限进行启动

答案：B

64.Alice 有一个消息 M 通过密钥 K2 生成一个密文 E（K2，M）然后用 K1 生成一个 MAC 为 C（K1， E（K2，M）），Alice 将密文和 MAC 发送给 Bob，Bob 用密钥 K1 和密文生成一个 MAC 并和 Alice 的 MAC 比较，假如相同再用 K2 解密 Alice 发送的密文，这个过程可以提供什么安 全服务?

A．仅提供数字签名　　B．仅提供保密性

C．仅提供不可否认性　　D．保密性和消息完整性

答案：D

65.以下关于 windowsSAM(安全账号管理器)的说法错误的是:

A、安全账号管理器(SAM)具体表现就是%SystemRoot%\system32\config\sam

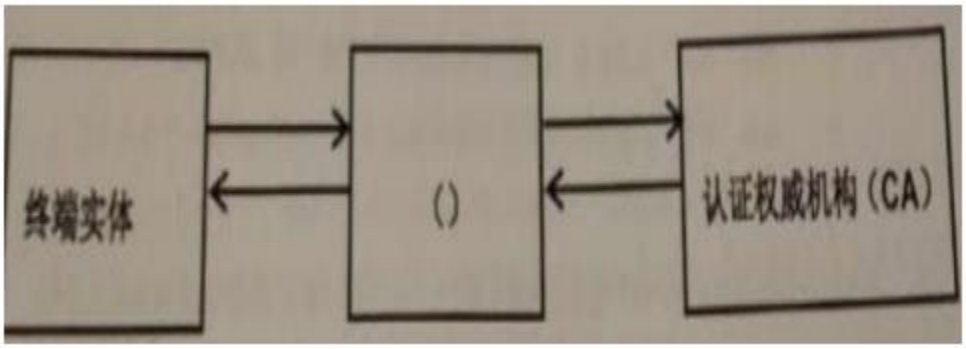
B、安全账号管理器(SAM)存储的账号信息是存储在注册表中

C、安全账号管理器(SAM)存储的账号信息 administrator 和 system 是可读和可写的

D、安全账号管理器(SAM)是 windows 的用户数据库系统进程通过 Security Accounts Manager 服务进行访问和操作

答案：C

66.公钥基础设施，引入数字证书的概念，用来表示用户的身份，下图简要的描述了终端实体 （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（）



A.证书库　　B.RA　　C.OCSP　　D .CRL 库

答案：B

67.常见密码系统包含的元素是：

A.明文，密文，信道，加密算法，解密算法

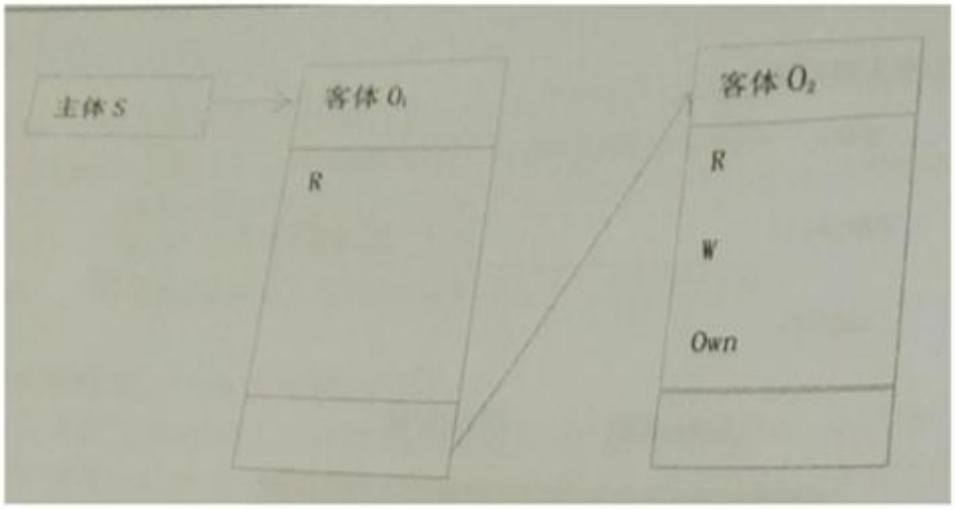
B.明文，摘要，信道，加密算法，解密算法

C.明文，密文，密钥，加密算法，解密算法

D.消息，密文，信道，加密算法，解密算法

答案：C

68.如图所示，主体 S 对客体 01 有读（R）权限，对客体 02 有读（R） 、写（）权限。该 图所示的访问控制实现方法是：



A.访问控制表（ACL）　　B.访问控制矩阵

C.能力表（CL）　　D.前缀表（Profiles）

答案：C

69.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、电子邮件及浏览器。为对抗此类信息收集和分析，公司需要做的是（）

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

答案：A

70.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 ACK/SYN 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 Flood 攻击属于（）

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

答案：A

71.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（）

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

答案：C

72.公钥密码的应用不包括:

A、数字签名　　B、非安全信道的密钥交换

C、消息认证码　　D、身份认证

答案：C

73.hash 算法的碰撞是指:

A、两个不同的消息，得到相同的消息摘要

B、两个相同的消息，得到不同的消息摘要

C、消息摘要和消息的长度相同

D、消息摘要比消息长度更长

答案：A

74.Windows 操作系统的注册表运行命令是:

A.Regsvr32　　B.Regedit

C.Regedit.msc　　D.Regedit.mmc

答案：B

75.视窗操作系统（Windows）从哪个版本开始引入安全中心的概念?

A.WinNT SP6　　B.Win2000 SP4

C.WinXP SP2　　D.Win2003 SP1

答案：C

76.DSA 算法不提供以下哪种服务?

A、数据完整性　　B、加密

C、数字签名　　D、认证

答案：B

77.在 Windows 文件系统中，_____支持文件加密。

A. FAT16　　B.NTFS

C.FAT32　　D.EXT3

答案：B

78.相比 FAT 文件系统，以下那个不是 NTFS 所具有的优势?

A、NTFS 使用事务日志自动记录所有文件和文件夹更新，当出现系统损坏引起操作失败后， 系统能利用日志文件重做或恢复未成功的操作。

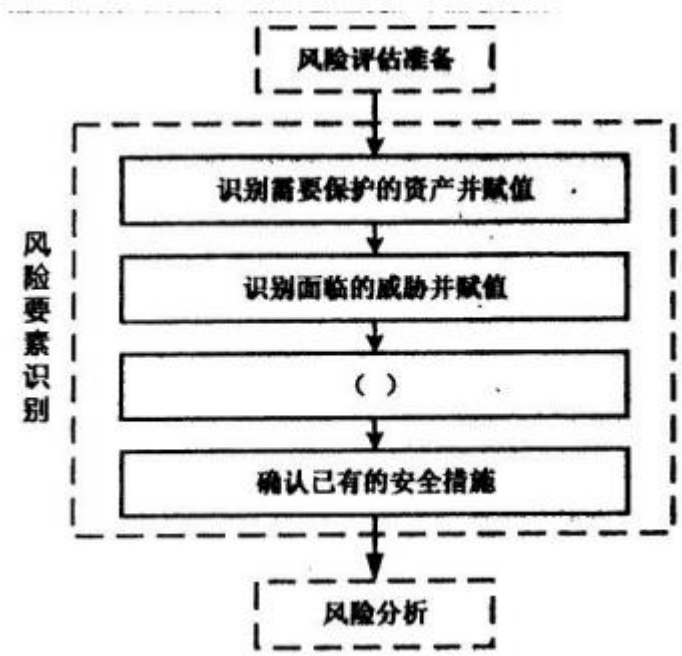
B、NTFS 的分区上，可以为每个文件或文件夹设置单独的许可权限

C、对于大磁盘，NTFS 文件系统比 FAT 有更高的磁盘利用率。

D、相比 FAT 文件系统，NTFS 文件系统能有效的兼容 linux 下的 EXT3 文件格式。

答案：D

79.风险要素识别是风险评估实施过程中的一个重要步骤，小李将风险要素识别的主要过程使 用图形来表示，如下图所示，请为图中空白框处选择一个最合适的选项()。



A．识别面临的风险并赋值

B．识别存在的脆弱性并赋值

C．制定安全措施实施计划

D．检查安全措施有效性

答案：B

80.Windows NT 提供的分布式安全环境又被称为:

A、 域（Domain） B、工作组

C、对等网 D、安全网

答案：A

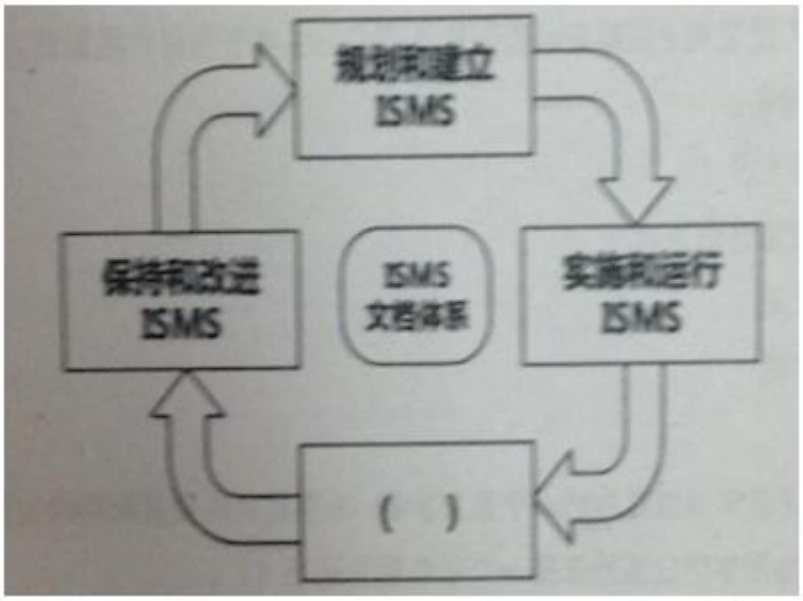
81.在 Windows 系统中，管理权限最高的组是:

A.everyone　　B.administrators

C.powerusers　　D.users

答案：B

82.小李去参加单位组织的信息安全培训后，他把自己对管理信息管理体系 ISMS 的理解画了 一张图，但是他还存在一个空白处未填写，请帮他选择一个合适的选项（）



A．监控和反馈 ISMS

B．批准和监督 ISMS

C．监视和评审 ISMS

D．沟通和咨询 ISMS

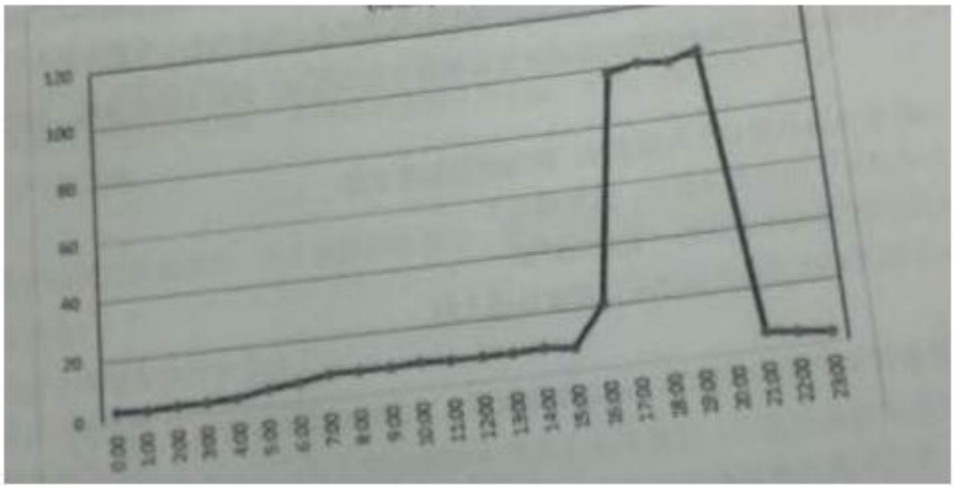
答案：C

83.Windows 系统下，可通过运行_____命令打开 Windows 管理控制台。

A.regedit　　B.cmd　　C.mmc　　D.mfc

答案：C

84.下图是某单位对其主网站一天流量的监测图，如果该网站当天 17：00 到 20：00 之间受到 攻击，则从图中数据分析，这种攻击可能属于下面什么攻击。



A.跨站脚本攻击　　B.TCP 会话劫持

C.IP 欺骗攻击　　D.拒绝服务攻击

答案：D

85.在 window 系统中用于显示本机各网络端口详细情况的命令是:

A． netshow　　B．netstat　　C．ipconfig　　D．Netview

答案：B

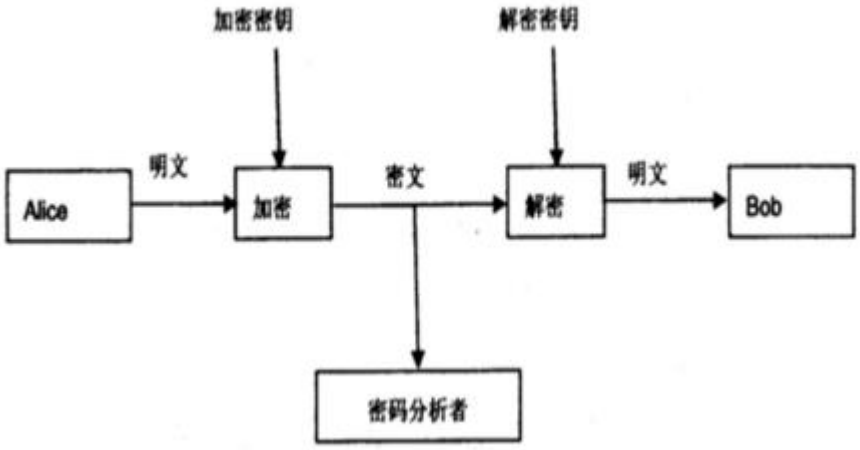
86.以下哪些问题或概念不是公钥密码体制中经常使用到的困难问题?

A、大整数分解　　B、离散对数问题

C、背包问题　　D、伪随机数发生器

答案：D

87.如下图所示，Alice 用 Bob 的密钥加密明文，将密文发送给 Bob，Bob 再用自己的私钥 解密，恢复出明文以下说法正确的是:



A．此密码体制为对称密码体制　　B．此密码体制为私钥密码体制

C．此密码体制为单钥密码体制　　D、此密码体制为公钥密码体制

答案：D

88.以下哪种公钥密码算法既可以用于数据加密又可以用于密钥交换?

A、DSS　　B、Diffie-Hellman

C、RSA　　D、AES

答案：C

89.在密码学的 Kerchhof 假设中，密码系统的安全性仅依赖于_____。

A．明文　　B．密文　　C．密钥　　D．信道

答案：C

90.在 Windows XP 中用事件查看器查看日志文件，可看到的日志包括?

A．用户访问日志、安全性日志、系统日志和 IE 日志

B．应用程序日志、安全性日志、系统日志和 IE 日志

C．网络攻击日志、安全性日志、记账日志和 IE 日志

D．网络链接日志、安全性日志、服务日志和 IE 日志

答案：B

91.操作系统安全的基础是建立在:

A、安全安装　　B、安全配置　　C、安全管理　　D、以上都对

答案：D

92.某用户通过账号，密码和验证码成功登陆某银行的个人网银系统，此过程属于以下哪一类

A.个人网银和用户之间的双向鉴别

B.由可信第三方完成的用户身份鉴别

C.个人网银系统对用户身份的单向鉴别

D.用户对个人网银系统 合法性 单向鉴别

答案：C

93.windows 文件系统权限管理作用访问控制列表（Access Control List.ACL）机制，以下哪 个说法是错误的:

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，为了作用上的便利，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的

用户的权限

答案：C

94.下列关于 kerckhof 准则的说法正确的是：

A、保持算法的秘密性比保持密钥的秘密性要困难的多

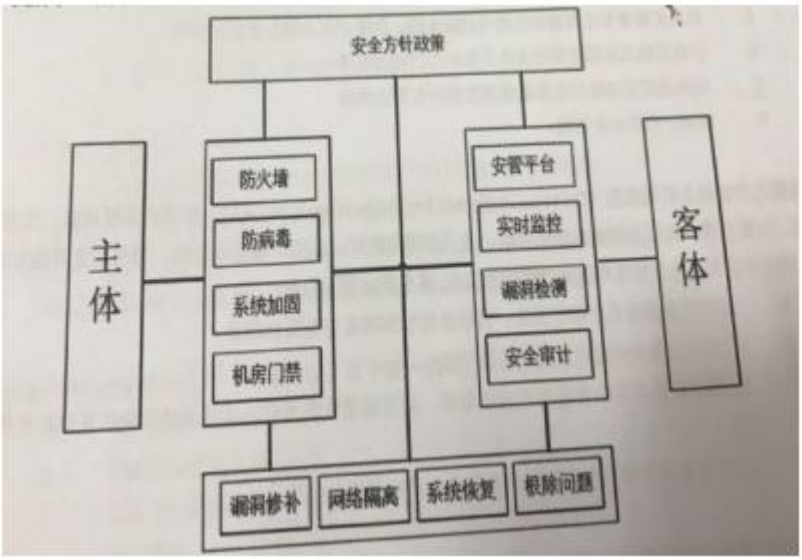
B、密钥一旦泄漏，也可以方便的更换

C、在一个密码系统中，密码算法是可以公开的，密钥应保证安全

D、公开的算法能够经过更严格的安全性分析

答案：C

小李是某公司系统规划师，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（ ）



A.PDR　　B. PPDR　　C. PDCA　　D. IATF

答案：B

95.信息发送者使用_____进行数字签名。

A、己方的私钥 B、己方的公钥 C、对方的私钥 D、对方的公钥

答案：A

96.根据 BEll—lapadula 模型安全策略，下图中写和读操作正确的是：

A.可读可写　　B.可读不可写

C.可写不可读　　D.不可读不可写

答案：D

97.以下列出了 mac 和散列函数的相似性,哪一项说法是错误的?

A、MAC 和散列函数都是用于提供消息认证

B、MAC 的输出值不是固定长度的，而散列函数的输出值是固定长度的

C、MAC 和散列函数都不需要密钥

D、MAC 和散列函数都不属于非对称加密算法

答案：A

解释： 1） MAC：消息验证、完整性校验、抗重放攻击；输出是固定的；

MAC 需密钥；不是非对称。

2） 哈希函数：消息完整性校验；输出是固定的；不需要密钥；不是非对称。

98.下面哪种方法产生的密码是最难记忆的?

A.将用户的生日倒转或是重排

B.将用户的年薪倒转或是重排

C.将用户配偶的名字倒转或是重排

D.用户随机给出的字母

答案：D

99.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?

A．软件在 Linux 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

答案：D

100.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．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闯题，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

答案：A

101.针对软件的拒绝服务攻击是通过消耗系统资源使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:

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

答案：D

102.以下哪个选项不是防火墙提供的安全功能?

A．IP 地址欺骗防护　　B．NAT

C．访问控制　　D．SQL 注入攻击防护

答案：D

103.以下关于可信计算说法错误的是:

A．可信的主要目的是要建立起主动防御的信息安全保障体系

B．可信计算机安全评价标准(TCSEC)中第一次提出了可信计算机和可信计算基的概念

C．可信的整体框架包含终端可信、终端应用可信、操作系统可信、网络互联可信、互联 网交易等应用系统可信

D．可信计算平台出现后会取代传统的安全防护体系和方法

答案：D

104.Linux 系统对文件的权限是以模式位的形式来表示，对于文件名为 test 的

一个文件，属于 admin 组中 user 用户，以下哪个是该文件正确的模式表示?

A. -rwxr-xr-x 3 user admin 1024 Sep 13 11：58 test

B. drwxr-xr-x 3 user admin 1024 Sep 13 11：58 test

C．-rwxr-xr-x 3 admin user 1024 Sep 13 11：58 test

D．drwxrxr-x 3 admin user1024 Sep 13 11：58 test

答案：A

105.Apache Web 服务器的配置文件一般位于/usr / local / apache / conf 目录，其中用来控制 用户访问 Apache 目录的配置文件是:

A. httpd.conf　　B．srL conf　　C．access．conf　　D．lnet.conf

答案：A

106.应用软件的数据存储在数据库中，为了保证数据安全，应设置良好的数据库防护策略，以 下不属于数据库防护策略的是?

A．安装最新的数据库软件安全补丁

B．对存储的敏感数据进行安全加密

C．不使用管理员权限直接连接数据库系统

D．定期对数据库服务器进行重启以确保数据库运行良好

答案：D

107.下列哪项内容描述的是缓冲区溢出漏洞?

A. 通过把 SQL 命令插入到 web 表单递交或输入域名或页面请求的查询字符串，最终达到 欺骗服务器执行恶意的 SQL 命令

B．攻击者在远程 WEB 页面的 HTML 代码中插入具有恶意目的的数据，用户认为该页面是可 信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行。

C．当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量溢出的数据覆盖在合法 数据上

D．信息技术、信息产品、信息系统在设计、实现、配置、运行等过程中，有意或无意产 生的缺陷

答案：C

108.对恶意代码的预防，需要采取增强安全防范策略与意识等措施，关于以下预防措施或意识， 说法错误的是:

A．在使用来自外部的移动介质前，需要进行安全扫描

B．限制用户对管理员权限的使用

C. 开放所有端口和服务，充分使用系统资源

D．不要从不可信来源下载或执行应用程序

答案：C

109.安全专家在对某网站进行安全部署时，调整了 Apache 的运行权限，从 root 权限降低为 nobody 用户，以下操作的主要目的是:

A．为了提高 Apache 软件运行效率

B．为了提高 Apache 软件的可靠性

C. 为了避免攻击者通过 Apache 获得 root 权限

D．为了减少 Apache 上存在的漏洞

答案：C

110.下列关于计算机病毒感染能力的说法不正确的是:

A．能将自身代码注入到引导区

B．能将自身代码注入到扇区中的文件镜像

C．能将自身代码注入文本文件中并执行

D．能将自身代码注入到文档或模板的宏中代码

答案：C

111.以下哪个是恶意代码采用的隐藏技术:

A．文件隐藏　　B．进程隐藏　　C．网络连接隐藏　　D．以上都是

答案：D

112.通过向被攻击者发送大量的 ICMP 回应请求，消耗被攻击者的资源来进行响应，直至被攻 击者再也无法处理有效的网络信息流时，这种攻击称之为:

A．Land 攻击 B．Smurf 攻击 C．Ping of Death 攻击 D. ICMP Flood

答案：D

113.以下哪个拒绝服务攻击方式不是流量型拒绝服务攻击

A．Land　　B．UDP Flood　　C．Smurf　　D.Teardrop

答案：D

114.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?

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

答案：D

115.以下关于 UDP 协议的说法，哪个是错误的?

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，超时重发等机制，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

答案：D

116.有关项目管理，错误的理解是：

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、方法和理论，对项目涉及的全部工作进行有效地管理，不受项目资源的约束

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

答案：B

117.近年来利用 DNS 劫持攻击大型网站恶性攻击事件时有发生，防范这种攻击比较有效的方法是?

A．加强网站源代码的安全性

B．对网络客户端进行安全评估

C. 协调运营商对域名解析服务器进行加固

D．在网站的网络出口部署应用级防火墙

答案：C

118.关于源代码审核，下列说法正确的是：

A．人工审核源代码审校的效率低，但采用多人并行分析可以完全弥补这个缺

点

B．源代码审核通过提供非预期的输入并监视异常结果来发现软件故障，从而定位可能导 致安全弱点的薄弱之处

C．使用工具进行源代码审核，速度快，准确率高，已经取代了传统的人工审核

D. 源代码审核是对源代码检查分析，检测并报告源代码中可能导致安全弱点的薄弱之处

答案：D

119.在戴明环(PDCA)模型中，处置(ACT)环节的信息安全管理活动是:

A．建立环境

B．实施风险处理计划

C．持续的监视与评审风险

D. 持续改进信息安全管理过程

答案：D

120.信息系统的业务特性应该从哪里获取?

A．机构的使命

B．机构的战略背景和战略目标

C. 机构的业务内容和业务流程

D．机构的组织结构和管理制度

答案：C

121.在信息系统设计阶段，“安全产品选择”处于风险管理过程的哪个阶段?

A．背景建立　　B．风险评估　　C．风险处理　　D．批准监督

答案：C

122.以下关于“最小特权”安全管理原则理解正确的是：

A．组织机构内的敏感岗位不能由一个人长期负责

B．对重要的工作进行分解，分配给不同人员完成

C. 一个人有且仅有其执行岗位所足够的许可和权限

D．防止员工由一个岗位变动到另一个岗位，累积越来越多的权限

答案：C

123.以下哪一项不属于常见的风险评估与管理工具：

A．基于信息安全标准的风险评估与管理工具

B．基于知识的风险评估与管理工具

C. 基于模型的风险评估与管理工具

D．基于经验的风险评估与管理工具

答案：D

124.以下说法正确的是：

A．验收测试是由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

答案：C

125.信息系统安全保护等级为 3 级的系统，应当()年进行一次等级测评?

A．0．5　　B.1　　C．2　　D．3

答案：B

126.国家科学技术秘密的密级分为绝密级、机密级、秘密级，以下哪项属于绝密级的描述?

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．能够局部反应国家防御和治安实力的

C．我国独有、不受自然条件因素制约、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

答案：D

127.关于我国加强信息安全保障工作的总体要求，以下说法错误的是:

A．坚持积极防御、综合防范的方针

B．重点保障基础信息网络和重要信息系统安全

C．创建安全健康的网络环境

D．提高个人隐私保护意识

答案：D

128.根据《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》的规定，以下 正确的是:

A．涉密信息系统的风险评估应按照《信息安全等级保护管理办法》等国家有关保密规定 和标准进行

B．非涉密信息系统的风险评估应按照《非涉及国家秘密的信息系统分级保护管理办法》 等要求进行

C．可委托同一专业测评机构完成等级测评和风险评估工作，并形成等级测评报告和风险 评估报告

D．此通知不要求将“信息安全风险评估”作为电子政务项目验收的重要内容

答案：C

129.某单位信息安全岗位员工，利用个人业余时间，在社交网络平台上向业内同不定期发布信 息安全相关知识和前沿动态资讯，这一行为主要符合以下哪一条注册信息安全专业人员 （CISP）职业道德准则:

A．避免任何损害 CISP 声誉形象的行为

B．自觉维护公众信息安全，拒绝并抵制通过计算机网络系统泄露个人隐私的行为

C．帮助和指导信息安全同行提升信息安全保障知识和能力

D．不在公众网络传播反动、暴力、黄色、低俗信息及非法软件

答案：C

130.以下哪一项不是我国信息安全保障的原则:

A．立足国情，以我为主，坚持以技术为主

B．正确处理安全与发展的关系，以安全保发展，在发展中求安全

C．统筹规划，突出重点，强化基础性工作

D．明确国家、企业、个人的责任和义务，充分发挥各方面的积极性，共同构筑国家信息 安全保障体系

答案：A

131.下列选项中，哪个不是我国信息安全保障工作的主要内容:

A．加强信息安全标准化工作，积极采用“等同采用、修改采用、制定”等多种方式，尽 快建立和完善我国信息安全标准体系

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

答案：B

132.关于信息安全管理，说法错误的是:

A．信息安全管理是管理者为实现信息安全目标(信息资产的 CIA 等特性，以及业务运作的 持续)而进行的计划、组织、指挥、协调和控制的一系列活动。

B．信息安全管理是一个多层面、多因素的过程，依赖于建立信息安全组织、明确信息安 全角色及职责、制定信息安全方针策略标准规范、建立有效的监督审计机制等多方面非技 术性的努力。

C．实现信息安全，技术和产品是基础，管理是关键。

D．信息安全管理是人员、技术、操作三者紧密结合的系统工程，是一个静态过程。

答案：D

133.以下哪个选项不是信息安全需求的来源?

A．法律法规与合同条约的要求

B．组织的原则、目标和规定

C．风险评估的结果

D．安全架构和安全厂商发布的病毒、漏洞预警

答案：D

134.下列关于信息系统生命周期中实施阶段所涉及主要安全需求描述错误的是:

A．确保采购定制的设备、软件和其他系统组件满足已定义的安全要求

B．确保整个系统已按照领导要求进行了部署和配置

C．确保系统使用人员已具备使用系统安全功能和安全特性的能力

D．确保信息系统的使用已得到授权

答案：B

135.下列关于信息系统生命周期中安全需求说法不准确的是：

A．明确安全总体方针，确保安全总体方针源自业务期望

B．描述所涉及系统的安全现状，提交明确的安全需求文档

C．向相关组织和领导人宣贯风险评估准则

D．对系统规划中安全实现的可能性进行充分分析和论证

答案：C

136.小张在某单位是负责事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，小张主要负责讲解风险评估工作形式，小张认为：

1．风险评估工作形式包括：自评估和检查评估；

2．自评估是指信息系统拥有、运营或使用单位发起的对本单位信息系统进行风险评估；

3．检查评估是信息系统上级管理部门组织或者国家有关职能部门依法开展的风险评估；

4．对信息系统的风险评估方式只能是“自评估”和“检查评估”中的一个，非此即彼.

请问小张的所述论点中错误的是哪项：

A．第一个观点　　B．第二个观点

C．第三个观点　　D．第四个观点

答案：D

137.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

138.风险评估工具的使用在一定程度上解决了手动评佑的局限性，最主要的是它能够将专家知识进行集中，使专家的经验知识被广泛使用，根据在风险评估过程中的主要任务和作用原理，风险评估工具可以为以下几类，其中错误的是：

A．风险评估与管理工具

B．系统基础平台风险评估工具

C．风险评估辅助工具

D．环境风险评估工具

答案：D

139.为了解风险和控制风险，应当及时进行风险评估活动，我国有关文件指出：风险评估的工 作形式可分为自评估和检查评估两种，关于自评估，下面选项中描述错误的是()。

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．自评估应参照相应标准、依据制定的评估方案和评估准则，结合系统特定的安全要求 实施

C．自评估应当是由发起单位自行组织力量完成，而不应委托社会风险评估服务机构来实施

D．周期性的自评估可以在评估流程上适当简化，如重点针对上次评估后系统变化部分进行

答案：C

140.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(2006)5 号)中，风险评估分为自评估和检查评估两种形式，并对两种工作形式提出了有关工作原则和要求，下面选项中描述正确的是( )。

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．自评估和检查评估是相互排斥的，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

答案：A

141.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值为 200 万元人民币，暴露系数(Exposure Factor，EF)是 25%，年度发生率 (Annualized Rate of Occurrence，ARO)为 0．1，那么小王计算的年度预期损失(Annualized Loss Expectancy，ALE)应该是()。

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

答案：A

142.规范的实施流程和文档管理，是信息安全风险评估结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．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

答案：A

143.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功的重要基础。某单 41 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()

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

答案：B

144.某单位在实施信息安全风险评估后，形成了若干文挡，下面( )中的文挡不应属于风险评 估中“风险评估准备”阶段输出的文档。

A．《风险评估工作计划》，主要包括本次风险评估的目的、意义、范围、目标、组织结构、 角色及职责、经费预算和进度安排等内容

B．《风险评估方法和工具列表》。主要包括拟用的风险评估方法和测试评估工具等内容

C．《已有安全措施列表》，主要包括经检查确认后的已有技术和管理各方面安全措施等内 容

D．《风险评估准则要求》，主要包括风险评估参考标准、采用的风险分析方法、风险计算 方法、资产分类标准、资产分类准则等内容

答案：B

145.文档体系建设是信息安全管理体系(ISMS)建设的直接体现，下列说法不正确的是：

A．组织内的信息安全方针文件、信息安全规章制度文件、信息安全相关操作规范文件等 文 档是组织的工作标准，也是 ISMS 审核的依据

B．组织内的业务系统日志文件、风险评估报告等文档是对上一级文件的执行和记录，对这些记录不需要保护和控制

C.组织在每份文件的首页，加上文件修订跟踪表，以显示每一版本的版本号、发布日期、 编写人、审批人、主要修订等内容

D．层次化的文档是 ISMS 建设的直接体现，文档体系应当依据风险评估的结果建立

答案：B

146.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:

A．在异地建立备份机房时，设计时应与主用机房等级相同

B．由于高端小型机发热量大，因此采用活动地板上送风，下回风的方式

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 级主机房应设置洁净气体灭火系统

答案：B

.147.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。

A．功能性　　B．可用性　　C．保障性　　D．符合

答案：D

148.下系统工程说法错误的是：

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遍意义的科学方法

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

答案：A

149.系统安全工程-能力成熟度模型(Systems Security Engineering Capability maturity model，SSECMM)定义的包含评估影响、评估威胁、评估脆弱性和评估安全风险的基本过程 领域是：

A．风险过程 B．工程过程 C．保证过程 D．评估过程

答案：A

150.组织建立业务连续性计划（BCP)的作用包括：

A.在遭遇灾难事件时，能够最大限度地保护组织数据的实时性，完整性和一致性；

B.提供各种恢复策略选择，尽量减小数据损失和恢复时间，快速恢复操作系统、应用和数据；

C.保证发生各种不可预料的故障、破坏性事故或灾难情况时，能够持续服务，确保业务系 统的不间断运行，降低损失；

D.以上都是。

答案：D

152.业务系统运行中异常错误处理合理的方法是：

A.让系统自己处理异常

B.调试方便，应该让更多的错误更详细的显示出来

C.捕获错误，并抛出前台显示

D.捕获错误，只显示简单的提示信息，或不显示任何信息

答案：D

153.以下哪项不是应急响应准备阶段应该做的？

A.确定重要资产和风险，实施针对风险的防护措施

B.编制和管理应急响应计划

C.建立和训练应急响应组织和准备相关的资源

D.评估事件的影响范围，增强审计功能、备份完整系统

答案：D

154.关于秘钥管理，下列说法错误的是：

A.科克霍夫原则指出算法的安全性不应基于算法的保密，而应基于秘钥的安全性

B.保密通信过程中，通信方使用之前用过的会话秘钥建立会话，不影响通信安全

C.秘钥管理需要考虑秘钥产生、存储、备份、分配、更新、撤销等生命周期过程的每一个 环节

D.在网络通信中。通信双方可利用 Diffie-He11man 协议协商出会话秘钥

答案：B

155.以下属于哪一种认证实现方式：用户登录时，认证服务器（Authentication Server，AS）产生一个随机数发送给用户，用户用某种单向算法将自己的口令、种子秘钥和随机数混合 计算后作为一次性口令，并发送给 AS,AS 用同样的方法计算后，验证比较两个口令即可验 证用户身份。

A.口令序列　　B. 时间同步　　C.挑战/应答　　D.静态口令

答案：C

156.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

157.在对某面向互联网提供服务的某应用服务器的安全检测中发现，服务器上开放了以下几个 应用，除了一个应用外其他应用都存在明文传输信息的安全问题，作为一名检测人员，你需要告诉用户对应用进行安全整改以外解决明文传输数据的问题，以下哪个应用已经解决 了明文传输数据问题:

A．SSH　　B．HTTP　　C．FTP　　D．SMTP

答案：A

158.以下哪个属性不会出现在防火墙的访问控制策略配置中?

A.本局域网内地址　B．百度服务器地址　C．HTTP 协议　D．病毒类型

答案：D

159.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--x 1 test tdst 10704 apr 15 2002/home/test/sh 请问以下描述哪个是 正确的:

A．该文件是一个正常文件，test 用户使用的 shell，但 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 shell,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，由于所有者是 test，因此运行这个文件时文件执行权限为 test

答案：D

160.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录功能，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:

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，导致网站攻击面增大，产生此 安全问题

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，产生此问题

答案：D

161.微软提出了 STRIDE 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

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，

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

答案：C

161.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 发人员决定用户登陆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

C.纵深防御原则　　D.最少共享机制原则

答案：C

162.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，威胁就是漏洞。

答案：D

163.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

164.有关能力成熟度模型（CMM）错误的理解是

A.CMM 的基本思想是，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.CMM 的思想来源于项目管理和质量管理

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

165.提高阿帕奇系统(Apache HTTP Server)系统安全性时，下面哪项措施不属于安全配置内容 ()?

A．不在 Windows 下安装 Apache，只在 Linux 和 Unix 下安装

B．安装 Apache 时，只安装需要的组件模块

C．不使用操作系统管理员用户身份运行 Apache，而是采用权限受限的专用用户账号来运 行

D．积极了解 Apache 的安全通告，并及时下载和更新

答案：A

166.某公司开发了一个游戏网站，但是由于网站软件存在漏洞，在网络中传输大数据包时总是会丢失一些数据，如一次性传输大于 2000 个字节数据时，总是会有 3 到 5 个字节不能传 送到对方，关于此案例，可以推断的是（）

A 该网站软件存在保密性方面安全问题

B 该网站软件存在完整性方面安全问题

C 该网站软件存在可用性方面安全问题

D 该网站软件存在不可否认性方面安全问题

答案：B

167.信息安全保障是网络时代各国维护国家安全和利益的首要任务，以下哪个国家最早将网络 安全上长升为国家安全战略，并制定相关战略计划。

A 中国　　B 俄罗斯　　C 美国　　D 英国

答案：C

168.我国党和政府一直重视信息安全工作，我国信息安全保障工作也取得了明显成效，关于我 国信息安全实践工作，下面说法错误的是（）

A、加强信息安全标准化建设，成立了“全国信息安全标准化技术委员会”制订和发布了 大批信息安全技术，管理等方面的标准。

B、重视信息安全应急处理工作，确定由国家密码管理局牵头成立“国家网络应急中心” 推动了应急处理和信息通报技术合作工作进展

C、推进信息安全等级保护工作，研究制定了多个有关信息安全等级保护的规范和标准， 重点保障了关系国定安全，经济命脉和社会稳定等方面重要信息系统的安全性

D 实施了信息安全风险评估工作，探索了风险评估工作的基本规律和方法，检验并修改完 善了有关标准，培养和锻炼了人才队伍

答案：B

169.为保障信息系统的安全，某经营公众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，并严格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描述 报告，关于此项工作，下面说法错误的是（）

A、信息安全需求是安全方案设计和安全措施实施的依据

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

答案：D

170.对系统工程（Systems Engineering，SE）的理解，以下错误的是：

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

答案：C

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：

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

答案：C

171.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 xp_cmdshell 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:

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

答案：B

172.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. 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。

答案：A

173.以下关于信息安全工程说法正确的是

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

答案：C

174.系统安全工程-能力成熟度模型（Systems Security Engineering-Capability maturity model，SSE-CMM）定义的包含评估影响、评估威胁、评估脆弱性和评估安全风险的基本过 程领域是：

A. 风险过程　　B.工程过程　　C.保证过程　　D.评估过程

答案：A

174.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。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（）。

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》

答案：B

175.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：

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（Base Practices，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

答案：B

176.关于标准，下面哪项理解是错误的（）。

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 使用的一种规范性文件。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

答案：B

177.2005 年，RFC4301（Request for Comments 4301:Security Architecture for the Internet Protocol）发布，用以取代原先的 RFC2401，该标准建议规定了 IPsec 系统基础架构，描 述如何在 IP 层（IPv4/IPv6）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（）。

A.国际标准化组织（International Organization for Standardization，ISO）

B.国际电工委员会（International Electrotechnical Commission，IEC）

C.国际电信联盟远程通信标准化组织（ITU Telecommunication Standardization Secctor， ITU-T）

D. Internet 工程任务组（Internet Engineering Task Force，IETF）

答案：D

.178.GB/T 18336《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 Profile，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（）个递增 的评估保证等级。

A. 4 B. 5 C. 6 D. 7

答案：D

179.有关系统工程的特点，以下错误的是:

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

答案：B

180.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

181.以下说法正确的是:

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

答案：C

182.. 以下系统工程说法错误的是:

A．系统工程的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遍意义的科学方法

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

答案：A

183.应急响应是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（ ）。

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。即包括预防性措施，也包括事件发生后的应对措施

B．应急响应工作有其鲜明的特点：具有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．应急响应是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： 安全事件发生时的正确指挥、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 1988 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置和整体协调的重要性

答案：C

184.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、和/或封锁被攻破的登录账号等（）

A．准备阶段　　B．遏制阶段　　C．根除阶段　　D．检测阶段

答案：B

185.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（ ）

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

答案：C

186.“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

187.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

188.Gary McGraw 博士及其合作者提出软件安全 BSI 模型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

189.以下哪一项不是常见威胁对应的消减措施：

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

答案：C

190.以下关于模糊测试过程的说法正确的是:

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

答案：C

191.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（ ）

A． 统筹规划 B． 分组建设 C. 资源共享 D． 平战结合

答案：B

192 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：A

193.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

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

答案：D

194.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：

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

答案：C

195.依据国家标准/T20274《信息系统安全保障评估框架》，信息系统安全目标(ISST)中，安全保障目的指的是：

A、信息系统安全保障目的

B、环境安全保障目的

C、信息系统安全保障目的和环境安全保障目的

D、信息系统整体安全保障目的、管理安全保障目的、技术安全保障目的和工程安全保障目的

答案：D

196.以下哪一项是数据完整性得到保护的例子?

A．某网站在访问量突然增加时对用户连接数量进行了限制，保证已登录的用

户可以 完成操作

B．在提款过程中 ATM 终端发生故障，银行业务系统及时对该用户的账户余额进行了冲正操作

C．某网管系统具有严格的审计功能，可以确定哪个管理员在何时对核心交换机进行 了什么操作

D．李先生在每天下班前将重要文件锁在档案室的保密柜中，使伪装成清洁工的商业间谍无法查看

答案：B

197 进入 21 世纪以来，信息安全成为世界各国安全战略关注的重点，纷纷制定并颁布网 络空间安全战略，但各国历史、国情和文化不同，网络空间安全战略的内容也各不相同，以下说法不正确的是:

A．与国家安全、社会稳定和民生密切相关的关键基础设施是各国安全保障的重点

B．美国尚未设立中央政府级的专门机构处理网络信息安全问题，信息安全管理职能 由不同政府部门的多个机构共同承担

C．各国普遍重视信息安全事件的应急响应和处理

D．在网络安全战略中，各国均强调加强政府管理力度，充分利用社会资源，发挥政 府与企业之间的合作关系

答案：B

198.与 PDR 模型相比，P2DR 模型多了哪一个环节?

A．防护　　B．检测　　C．反应　　D.策略

答案：D

199.2008 年 1 月 2 日，美目发布第 54 号总统令，建立国家网络安全综合计划 （Comprehensive National Cyber security Initiative，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．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

答案：A

200.下列对于信息安全保障深度防御模型的说法错误的是:

A．信息安全外部环境：信息安全保障是组织机构安全、国家安全的一个重要组成部分，因此对信息安全的讨论必须放在国家政策、法律法规和标准的外部环境制约下。

B．信息安全管理和工程：信息安全保障需要在整个组织机构内建立和完善信息安全 管理体系，将信息安全管理综合至信息系统的整个生命周期，在这个过程中，我 们需要采用信息系统工程的方法来建设信息系统。

C．信息安全人才体系：在组织机构中应建立完善的安全意识，培训体系也是信息安 全保障的重要组成部分。

D．信息安全技术方案："从外而内、自下而上、形成边界到端的防护能力"。

答案：D

201.某用户通过账号、密码和验证码成功登录某银行的个人网银系统，此过程属于以下哪 一类：

A．个人网银系统和用户之间的双向鉴别

B．由可信第三方完成的用户身份鉴别

C. 个人网银系统对用户身份的单向鉴别

D．用户对个人网银系统合法性的单向鉴别

答案：C

202.Alice 用 Bob 的密钥加密明文，将密文发送给 Bob。Bob 再用自己的私钥解密，恢复 出明文。以下说法正确的是：

A．此密码体制为对称密码体制

B．此密码体制为私钥密码体制

C．此密码体制为单钥密码体制

D．此密码体制为公钥密码体制

答案：D

203.下列哪一种方法属于基于实体“所有”鉴别方法：

A．用户通过自己设置的口令登录系统，完成身份鉴别

B．用户使用个人指纹，通过指纹识别系统的身份鉴别

C．用户利用和系统协商的秘密函数，对系统发送的挑战进行正确应答，通过身份鉴 别

D.用户使用集成电路卡(如智能卡)完成身份鉴别

答案：D

204.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 +短信认证”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. 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

答案：A

205.某单位开发了一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性测试，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. 渗透测试以攻击者的思维模拟真实攻击，能发现如配置错误等运行维护期产生的 漏洞

B．渗透测试是用软件代替人工的一种测试方法，因此测试效率更高

C．渗透测试使用人工进行测试，不依赖软件，因此测试更准确

D．渗透测试中必须要查看软件源代码，因此测试中发现的漏洞更多

答案：A

206.软件安全设计和开发中应考虑用户稳私包，以下关于用户隐私保护的说法哪个是错误 的?

A．告诉用户需要收集什么数据及搜集到的数据会如何披使用

B．当用户的数据由于某种原因要被使用时，给用户选择是否允许

C．用户提交的用户名和密码属于稳私数据，其它都不是

D．确保数据的使用符合国家、地方、行业的相关法律法规

答案：C

207.软件安全保障的思想是在软件的全生命周期中贯彻风险管理的思想，在有限资源前提下实现软件安全最优防护，避免防范不足带来的直接损失，也需要关注过度防范造成 的间接损失。在以下软件安全开发策略中，不符合软件安全

保障思想的是:

A.在软件立项时考虑到软件安全相关费用，经费中预留了安全测试、安全评审相关费 用，确保安全经费得到落实

B．在软件安全设计时，邀请软件安全开发专家对软件架构设计进行评审，及时发现 架构设计中存在的安全不足

C．确保对软编码人员进行安全培训，使开发人员了解安全编码基本原则和方法，确 保开发人员编写出安全的代码

D．在软件上线前对软件进行全面安全性测试，包括源代码分析、模糊测试、渗透测 试，未经以上测试的软件不允许上线运行

答案：D

208.以下哪一项不是工作在网络第二层的隧道协议:

A.VTP　　B．L2F　　C．PPTP　　D．L2TP

答案：A

.主体 S 对客体 01 有读(R)权限，对客体 02 有读(R)、写(W)、拥有(Own)权限，该访问 控制实现方法是:

A．访问控制表(ACL)　　B．访问控制矩阵

C. 能力表(CL)　　D．前缀表(Profiles)

答案：C

209.以下场景描述了基于角色的访问控制模型(Role-based Access

Control．RBAC)：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：

A．当用户请求访问某资源时，如果其操作权限不在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

答案：D

210.下面哪一项不是虚拟专用网络(VPN)协议标准：

A．第二层隧道协议(L2TP)

B．Internet 安全性(IPSEC)

C. 终端访问控制器访问控制系统(TACACS+)

D．点对点隧道协议(PPTP)

答案：C

211.下列对网络认证协议(Kerberos)描述正确的是：

A．该协议使用非对称密钥加密机制

B．密钥分发中心由认证服务器、票据授权服务器和客户机三个部分组成

C．该协议完成身份鉴别后将获取用户票据许可票据

D．使用该协议不需要时钟基本同步的环境

答案：C

212.鉴别的基本途径有三种：所知、所有和个人特征，以下哪一项不是基于你所知道的：

A．口令　　B．令牌　　C．知识　　D．密码

答案：B

213.在 ISO 的 OSI 安全体系结构中，以下哪一个安全机制可以提供抗抵赖安全服务?

A．加密　　B.数字签名　　C．访问控制　　D．路由控制

答案：B

某公司已有漏洞扫描和入侵检测系统(Intrusien Detection System，IDS)产品，需要购买防火墙，以下做法应当优先考虑的是：

A．选购当前技术最先进的防火墙即可

B．选购任意一款品牌防火墙

C．任意选购一款价格合适的防火墙产品

D．选购一款同已有安全产品联动的防火墙

答案：D

214.在 OSI 参考模型中有 7 个层次，提供了相应的安全服务来加强信息系统

的安全性，以 下哪一层提供了保密性、身份鉴别、数据完整性服务?

A.网络层　　B．表示层　　C．会话层　　D．物理层

答案：A

215.某单位人员管理系统在人员离职时进行账号删除，需要离职员工所在部门主管经理和 人事部门人员同时进行确认才能在系统上执行，该设计是遵循了软件安全哪项原则

A.最小权限　　B.权限分离　　C．不信任　　D．纵深防御

答案：B

216.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(AuthenticationHead，AH)和 IP 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．在隧道模式中，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

217.某电子商务网站在开发设计时，使用了威胁建模方法来分折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 中欺骗类的威胁，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 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 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

218.以下关于 PGP(Pretty Good Privacy)软件叙述错误的是:

A．PGP 可以实现对邮件的加密、签名和认证

B．PGP 可以实现数据压缩

C．PGP 可以对邮件进行分段和重组

D．PGP 采用 SHA 算法加密邮件

答案：D

219.入侵防御系统(IPS)是继入侵检测系统(IDS)后发展期出来的一项新的安全技术，它与 IDS 有着许多不同点，请指出下列哪一项描述不符合 IPS 的特点?

A．串接到网络线路中

B．对异常的进出流量可以直接进行阻断

C．有可能造成单点故障

D. 不会影响网络性能

答案：D

220.相比文件配置表(FAT)文件系统，以下哪个不是新技术文件系统(NTFS)所具有的优势?

A．NTFS 使用事务日志自动记录所有文件夹和文件更新，当出现系统损坏和电源故障 等闯题 而引起操作失败后，系统能利用日志文件重做或恢复未成功的操作

B．NTFS 的分区上，可以为每个文件或文件夹设置单独的许可权限

C．对于大磁盘，NTFS 文件系统比 FAT 有更高的磁盘利用率

D.相比 FAT 文件系统，NTFS 文件系统能有效的兼容 linux 下 EXT2 文件格式

答案：D

221.某公司系统管理员最近正在部署一台 Web 服务器，使用的操作系统是windows，在进 行日志安全管理设置时，系统管理员拟定四条日志安全策略给领导进行参考，其中能 有效应对攻击者获得系统权限后对日志进行修改的策略是:

A．网络中单独部署 syslog 服务器，将 Web 服务器的日志自动发送并存储到该 syslog 日志服务器中

B.严格设置 Web 日志权限，只有系统权限才能进行读和写等操作

C．对日志属性进行调整，加大日志文件大小、延长日志覆盖时间、设置记录更多信 息等

D．使用独立的分区用于存储日志，并且保留足够大的日志空间

答案：A

222 关于 linux 下的用户和组，以下描述不正确的是 。

A．在 linux 中，每一个文件和程序都归属于一个特定的“用户”

B．系统中的每一个用户都必须至少属于一个用户组

C. 用户和组的关系可以是多对一，一个组可以有多个用户，一个用户不能属于多个 组

D．root 是系统的超级用户，无论是否是文件和程序的所有者都具有访问权限

答案：C

223.安全的运行环境是软件安全的基础，操作系统安全配置是确保运行环境安全必不可少 的工作，某管理员对即将上线的 Windows 操作系统进行了以下四项安全部署工作，其 中哪项设置不利于提高运行环境安全?

A．操作系统安装完成后安装最新的安全补丁，确保操作系统不存在可被利用的安全 漏洞

B.为了方便进行数据备份，安装 Windows 操作系统时只使用一个分区 C，所有数据和 操作系统都存放在 C 盘

C．操作系统上部署防病毒软件，以对抗病毒的威胁

D．将默认的管理员账号 Administrator 改名，降低口令暴力破解攻击的发生可能

答案：B

224.在数据库安全性控制中，授权的数据对象，授权子系统就越灵活?

A. 粒度越小　　B．约束越细致　　C．范围越大　　D．约束范围大

答案：A

225.下列哪一些对信息安全漏洞的描述是错误的?

A．漏洞是存在于信息系统的某种缺陷。

B．漏洞存在于一定的环境中，寄生在一定的客体上(如 TOE 中、过程中等)。

C．具有可利用性和违规性，它本身的存在虽不会造成破坏，但是可以被攻击者利用， 从而给信息系统安全带来威胁和损失。

D．漏洞都是人为故意引入的一种信息系统的弱点

答案：D

226.账号锁定策略中对超过一定次数的错误登录账号进行锁定是为了对抗以下哪种攻击?

A．分布式拒绝服务攻击(DDoS)

B．病毒传染

C. 口令暴力破解

D．缓冲区溢出攻击

答案：C

227.以下哪个不是导致地址解析协议(ARP)欺骗的根源之一?

A．ARP 协议是一个无状态的协议

B．为提高效率，ARP 信息在系统中会缓存

C．ARP 缓存是动态的，可被改写

D. ARP 协议是用于寻址的一个重要协议

答案：D

228.张三将微信个人头像换成微信群中某好友头像，并将昵称改为该好友的昵称，然后向 该好友的其他好友发送一些欺骗消息。该攻击行为属于以下哪类攻击? A．口令攻击　　B．暴力破解

B. 拒绝服务攻击　　D. 社会工程学攻击

答案：D

229 关于软件安全开发生命周期(SDL)，下面说法错误的是:

A．在软件开发的各个周期都要考虑安全因素

B．软件安全开发生命周期要综合采用技术、管理和工程等手段

C．测试阶段是发现并改正软件安全漏洞的最佳环节，过早或过晚检测修改漏洞都将 增大软件开发成本

D．在设计阶段就尽可能发现并改正安全隐患，将极大减少整个软件开发成本

答案：C

230.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：

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

答案：D

231.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：

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-CMM)是在原有能力成熟度模型(CMM)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。

答案：C

232.以下哪一种判断信息系统是否安全的方式是最合理的?

A．是否已经通过部署安全控制措施消灭了风险

B．是否可以抵抗大部分风险

C．是否建立了具有自适应能力的信息安全模型

D. 是否已经将风险控制在可接受的范围内

答案：D

234.以下关于信息安全法治建设的意义，说法错误的是：

A．信息安全法律环境是信息安全保障体系中的必要环节

B．明确违反信息安全的行为，并对该行为进行相应的处罚，以打击信息安全犯罪活动

C．信息安全主要是技术问题，技术漏洞是信息犯罪的根源

D．信息安全产业的逐渐形成，需要成熟的技术标准和完善的技术体系

答案：C

235 小张是信息安全风险管理方面的专家，被某单位邀请过去对其核心机房经受某种灾害 的风险进行评估，已知：核心机房的总价价值一百万，灾害将导致资产总价值损失二 成四(24%)，历史数据统计告知该灾害发生的可能性为八年发生三次，请问小张最后 得到的年度预期损失为多少：

A．24 万　　B．0．09 万　　C．37．5 万　　D.9 万

答案：D

236.2005 年 4 月 1 日正式施行的《电子签名法》，被称为“中国首部真正意义

上的信息化 法律”，自此电子签名与传统手写签名和盖章具有同等的法律效力。以下关于电子签 名说法错误的是：

A.电子签名——是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签 名人认可其中内容的数据

B．电子签名适用于民事活动中的合同或者其他文件、单证等文书

C．电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务

D．电子签名制作数据用于电子签名时，属于电子签名人和电子认证服务提供者共有

答案：D

237.风险管理的监控与审查不包含：

A．过程质量管理

B．成本效益管理

C．跟踪系统自身或所处环境的变化

D．协调内外部组织机构风险管理活动

答案：D

238.信息安全等级保护分级要求，第三级适用正确的是：

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损害

答案：A

239.下面哪一项安全控制措施不是用来检测未经授权的信息处理活动的:

A．设置网络连接时限

B．记录并分析系统错误日志

C．记录并分析用户和管理员操作日志

D．启用时钟同步

答案：A

240.有关危害国家秘密安全的行为的法律责任，正确的是:

A．严重违反保密规定行为只要发生，无论产生泄密实际后果，都要依法追究责任

B．非法获取国家秘密，不会构成刑事犯罪，不需承担刑事责任

C．过失泄露国家秘密，不会构成刑事犯罪，不需承担刑事责任

D．承担了刑事责任，无需再承担行政责任或其他处分

答案：A

241.以下对于信息安全事件理解错误的是：

A．信息安全事件，是指由于自然或者人为以及软硬件本身缺陷或故障的原因，对信 息系统造成危害，或在信息系统内发生对社会造成负面影响的事件

B．对信息安全事件进行有效管理和响应，最小化事件所造成的损失和负面影响，是 组织信息安全战略的一部分

C．应急响应是信息安全事件管理的重要内容

D. 通过部署信息安全策略并配合部署防护措施，能够对信息及信息系统提供保护， 杜绝信息安全事件的发生

答案：D

242.假设一个系统已经包含了充分的预防控制措施，那么安装监测控制设备：

A．是多余的，因为它们完成了同样的功能，但要求更多的开销

B．是必须的，可以为预防控制的功效提供检测

C．是可选的，可以实现深度防御

D．在一个人工系统中是需要的，但在一个计算机系统中则是不需要的，因为预防控 制功能已经足够

答案：C

243.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：

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

答案：D

244 以下哪一项不是信息安全管理工作必须遵循的原则?

A．风险管理在系统开发之初就应该予以充分考虑，并要贯穿于整个系统开发过程之 中

B．风险管理活动应成为系统开发、运行、维护、直至废弃的整个生命周期内的持续 性工作

C．由于在系统投入使用后部署和应用风险控制措施针对性会更强，实施成本会相对较低

D．在系统正式运行后，应注重残余风险的管理，以提高快速反应能力

答案：C

245.《信息安全技术信息安全风险评估规范 GB / T 20984-2007》中关于信息系统生命周期 各阶段的风险评估描述不正确的是:

A.规划阶段风险评估的目的是识别系统的业务战略，以支撑系统安全需求及安全战略等

B.设计阶段的风险评估需要根据规划阶段所明确的系统运行环境、资产重要性，提出 安全功能需求

C.实施阶段风险评估的目的是根据系统安全需求和运行环境对系统开发、实施过程进 行风险识别，并对系统建成后的安全功能进行验证

D.运行维护阶段风险评估的目的是了解和控制运行过程中的安全风险，是一种全面的风险评估。评估内容包括对真实运行的信息系统、资产、脆弱性等各方面

答案：D

246.对信息安全风险评估要素理解正确的是:

A. 资产识别的粒度随着评估范围、评估目的的不同而不同，既可以是硬件设备，也 可以是业务系统，也可以是组织机构

B．应针对构成信息系统的每个资产做风险评价

C．脆弱性识别是将信息系统安全现状与国家或行业的安全要求做符合性比对而找出 的差距项

D．信息系统面临的安全威胁仅包括人为故意威胁、人为非故意威胁

答案：A

247.以下哪些是需要在信息安全策略中进行描述的:

A．组织信息系统安全架构

B. 信息安全工作的基本原则

C．组织信息安全技术参数

D．组织信息安全实施手段

答案：B

248.根据《关于开展信息安全风险评估工作的意见》的规定，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．信息安全风险评估工作要按照“严密组织、规范操作、讲求科学、注重实效”的 原则开展

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．开展信息安全风险评估工作应加强信息安全风险评估工作的组织领导

答案：A

249.下面的角色对应的信息安全职责不合理的是：

A．高级管理层——最终责任

B. 信息安全部门主管——提供各种信息安全工作必须的资源

C．系统的普通使用者——遵守日常操作规范

D．审计人员——检查安全策略是否被遵从

答案：B

250.自 2004 年 1 月起，国内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意见，协调一致后由该组织申报。

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(CCSA)

D．网络与信息安全技术工作委员会

答案：B

251.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(T，V)， F(Ia，Va))以下关于上式各项说明错误的是：

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 表示威胁利资产脆弱性导致安全事件的可能性

C．F 表示安全事件发生后造成的损失

D．Ia，Va 分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

答案：D

252.以下哪一项在防止数据介质被滥用时是不推荐使用的方法：

A．禁用主机的 CD 驱动、USB 接口等 I／O 设备

B．对不再使用的硬盘进行严格的数据清除

C．将不再使用的纸质文件用碎纸机粉碎

D. 用快速格式化删除存储介质中的保密文件

答案：D

253.在进行应用系统的测试时，应尽可能避免使用包含个人稳私和其它敏感信息的实际生产系统中的数据，如果需要使用时，以下哪一项不是必须做的：

A．测试系统应使用不低于生产系统的访问控制措施

B．为测试系统中的数据部署完善的备份与恢复措施

C．在测试完成后立即清除测试系统中的所有敏感数据

D．部署审计措施，记录生产数据的拷贝和使用

答案：B

254.为了保证系统日志可靠有效，以下哪一项不是日志必需具备的特征。

A．统一而精确地的时间

B．全面覆盖系统资产

C．包括访问源、访问目标和访问活动等重要信息

D. 可以让系统的所有用户方便的读取

答案：D

255.以下哪一项不属于信息安全工程监理模型的组成部分：

A．监理咨询支撑要素　　B.控制和管理手段

C．监理咨询阶段过程　　D.监理组织安全实施

答案：D

256.以下关于灾难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

答案：C

257.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:

A．项目计划书　　B．质量控制计划

C．评审报告　　D. 需求说明书

答案：D

258.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．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

答案：A

259.以下关于直接附加存储(Direct Attached Storage，DAS)说法错误的是:

A．DAS 能够在服务器物理位置比较分散的情况下实现大容量存储．是一种常用的数 据存储方法

B．DAS 实现了操作系统与数据的分离，存取性能较高并且实施简单

C．DAS 的缺点在于对服务器依赖性强，当服务器发生故障时，连接在服务器上的存储设备中的数据不能被存取

D．较网络附加存储(Network Attached Storage，NAS)，DAS 节省硬盘空间，

数据非常集中，便于对数据进行管理和备份

答案：D

260.某公司在执行灾难恢复测试时．信息安全专业人员注意到灾难恢复站点的服务器的运 行速度缓慢，为了找到根本愿因，他应该首先检查:

A．灾难恢复站点的错误事件报告

B．灾难恢复测试计划

C．灾难恢复计划(DRP)

D．主站点和灾难恢复站点的配置文件

答案：A

261.以下对异地备份中心的理解最准确的是:

A．与生产中心不在同一城市

B．与生产中心距离 100 公里以上

C．与生产中心距离 200 公里以上

D．与生产中心面临相同区域性风险的机率很小

答案：D

261.作为业务持续性计划的一部分，在进行业务影响分析(BIA)时的步骤是:

1．标识关键的业务过程; 2．开发恢复优先级; 3．标识关键的 IT 资源; 4．表示中断影响和允许的中断时间

A．1-3-4-2　　B．1-3-2-4

C．1－2－3－4　　D．1－4－3－2

答案：A

262.有关系统安全工程-能力成熟度模型(SSE-CMM)，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．基手 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

263.下面关于信息系统安全保障的说法不正确的是：

A．信息系统安全保障与信息系统的规划组织、开发采购、实施交付、运行维护和废 弃等生命周期密切相关

B. 信息系统安全保障要素包括信息的完整性、可用性和保密性

C．信息系统安全需要从技术、工程、管理和人员四个领域进行综合保障

D．信息系统安全保障需要将信息系统面临的风险降低到可接受的程度，从而实现其 业务使命

答案：B

264.在使用系统安全工程-能力成熟度模型(SSECMM)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:

A．测量单位是基本实施(Base Practices，BP)

B．测量单位是通用实践(Generic Practices，GP)

C．测量单位是过程区域(Process Areas，PA)

D．测量单位是公共特征(Common Features，CF)

答案：D

265.下面关于信息系统安全保障模型的说法不正确的是:

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

答案：D

266.信息系统安全工程(ISSE)的一个重要目标就是在 IT 项目的各个阶段充分考虑安全因 素，在 IT 项目的立项阶段，以下哪一项不是必须进行的工作:

A．明确业务对信息安全的要求

B．识别来自法律法规的安全要求

C．论证安全要求是否正确完整

D. 通过测试证明系统的功能和性能可以满足安全要求

答案：D

267.关于信息安全保障技术框架(IATF)，以下说法不正确的是：

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

答案：D

268.某单位开发一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性测试，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，以下哪条是渗透性的优势？

A.渗透测试使用人工进行测试，不依赖软件，因此测试更准确

B.渗透测试是用软件代替人工的一种测试方法。因此测试效率更高

C.渗透测试以攻击者的思维模拟真实攻击，能发现如配置错误等运行维护期产生的漏 洞

D.渗透测试中必须要查看软件源代码，因此测试中发现的漏洞更多

答案：C

269.以下关于软件安全测试说法正确的是（）

A.软件安全测试就是黑盒测试

B.FUZZ 测试是经常采用的安全测试方法之一

C.软件安全测试关注的是软件的功能

D.软件安全测试可以发现软件中产生的所有安全问题

答案：B

270 信息安全工程作为信息安全保障的重要组成部门，主要是为了解决:

A.信息系统的技术架构安全问题

B.信息系统组成部门的组件安全问题

C.信息系统生命周期的过程安全问题

D.信息系统运行维护的安全管理问题

答案：C

271.有关系统安全工程-能力成熟度模型（SSE-CMM)中基本实施（Base Practice）正确的 理解是 ：

A.BP 不限定于特定的方法工具，不同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，实施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

答案：A

272.层次化的文档是信息安全管理体系《information Security Management System.ISMS》 建设的直接体系，也 ISMS 建设的成果之一，通常将 ISMS 的文档结构规划为 4 层金字塔结构，那么，以下选项（）应放入到一级文件中.

A.《风险评估报告》 B.《人力资源安全管理规定》

C.《ISMS 内部审核计划》 D.《单位信息安全方针》

答案：D

273.信息安全管理体系（information Security Management System.简称 ISMS）的实施 和运行 ISMS 阶段，是 ISMS 过程模型的实施阶段（Do），下面给出了一些备①制定风 险处理计划②实施风险处理计划③开发有效性测量程序④实施培训和意识教育计划 ⑤管理 ISMS 的运行⑥管理 ISMS 的资源⑦执行检测事态和响应事件的程序⑧实施内部 审核⑨实施风险再评估选的活动，选项（）描述了在此阶段组织应进行的活动。

A.①②③④⑤⑥

B.①②③④⑤⑥⑦

C.①②③④⑤⑥⑦⑧

D.①②③④⑤⑥⑦⑧⑨

答案：B

274.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（）

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

答案：C

275.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（）

A.软件安全开发生命周期较长，而其中最重要的是要在软件的编码安全措施，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（SDL)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，考试到程序员的专业性，如果该开发人员已经对软件进 行了安全性测试，就没有必要再组织第三方进行安全性测试。

答案：B

276.某网站在设计对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拟问题，一下那种测试方式是最佳的测试方法。

A.模糊测试　　B.源代码测试　　C.渗透测试　　D.软件功能测试

答案：C

277，下面哪项属于软件开发安全方面的问题（）

A.软件部署时所需选用服务性能不高，导致软件执行效率低。

B.应用软件来考虑多线程技术，在对用户服务时按序排队提供服务

C.应用软件存在 SQL 注入漏洞，若被黑客利用能窃取数据库所用数据

D.软件受许可证（license）限制，不能在多台电脑上安装。

答案：C

278.为增强 Web 应用程序的安全性，某软件开发经理决定加强 Web 软件安全开发培训，下 面哪项内容不在考虑范围内（）

A.关于网站身份签别技术方面安全知识的培训

B.针对 OpenSSL 心脏出血漏洞方面安全知识的培训

C.针对 SQL 注入漏洞的安全编程培训

D.关于 ARM 系统漏洞挖掘方面安全知识的培训

答案：D

279.以下关于 https 协议 http 协议相比的优势说明，那个是正确的：

A.Https 协议对传输的数据进行加密，可以避免嗅探等攻击行为

B.Https 使用的端口 http 不同，让攻击者不容易找到端口，具有较高的安全性

C.Https 协议是 http 协议的补充，不能独立运行，因此需要更高的系统性能

D.Https 协议使用了挑战机制，在会话过程中不传输用户名和密码，因此具有较高的

答案：A

280.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（）。

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缺失量

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

答案：B

282.为推动和规范我国信息安全等级保护工作，我国制定和发布了信息安全等级保护工作 所需要的一系列标准，这些标准可以按照等级保护工作的工作阶段

大致分类。下面四 个标准中，（）规定了等级保护定级阶段的依据、对象、流程、方法及等级变更等内 容。

A.GB / T 20271-2006《信息系统通用安全技术要求》

B.GB / T 22240-2008《信息系统安全保护等级定级指南》

C.GB / T 25070-2010《信息系统等级保护安全设计技术要求》

D.GB / T 20269-2006《信息系统安全管理要求》

答案：B

283.某移动智能终端支持通过指纹识别解锁系统的功能，与传统的基于口令的鉴别技术相 比，关于此种鉴别技术说法不正确的是：

A.所选择的特征（指纹）便于收集、测量和比较

B.每个人所拥有的指纹都是独一无二的

C.指纹信息是每个人独有的，指纹识别系统不存在安全威胁问题

D.此类系统一般由用户指纹信息采集和指纹信息识别两部分组成

答案：C

284.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

285.在以下标准中，属于推荐性国家标准的是?

A.GB/T XXXX.X-200X　　B.GB XXXX-200X

C.DBXX/T XXX-200X　　D.GB/Z XXX-XXX-200X

答案：A

286.微软 SDL 将软件开发生命周期制分为七个阶段，并列出了十七项重要的安全活动。其 中“弃用不安全的函数”属于（）的安全活动

A.要求阶段　　B.设计阶段　　C.实施阶段　　D.验证阶段

答案：C

287.由于频繁出现计算机运行时被黑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开发知识培训

B.要求增加软件源代码审核环节，加强对软件代码的安全性审查

C.要求统一采用 Windows10 系统进行开发，不能采用之前的 Windows 版本

D.要求邀请专业队伍进行第三方安全性测试，尽量从多角度发现软件安全问题

答案：C

288.关于源代码审核，描述正确的是（）

A.源代码审核过程遵循信息安全保障技术框架模型(IATF)，在执行时应一步一步严格 执行

B.源代码审核有利于发现软件编码中存在的安全问题，相关的审核工具既有商业开源 工具

C.源代码审核如果想要有效率高，则主要依赖人工审核而不是工具审核，因为人工智 能的，需要人的脑袋来判断

D.源代码审核能起到很好的安全保证作用，如果执行了源代码审核，则不需要安全测试

答案：B

289.微软提出了 STRIDE 模型，其中 R 是 Repudiation(抵赖)的缩写，关于此项错误的 事是（）

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 R 威胁

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”威胁也属于 R 威胁。

C.对于 R 威胁，可以选择使用如强认证、数字签名、安全审计等技术

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

答案：D