CISP练习题四

考试

答题人

97	97
总分100	答对 共100题

答题解析 ⌃

全部题目 错题集

姓名：

考试

一、单项选择题。（每题1分，共100题，合计100分）

1. 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（）。 分值1分

- 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

回答正确 +1分

2. 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（） 分值1分

- 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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

回答错误 +0分

正确答案:

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

3. 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：（） 分值1分

○ 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.x~192.168.20.x

○ B. 总部使用服务器使用10.0.1.1~11、用户终端使用10.0.1.12~212,分支机构IP 地址随意确定即可

● C. 总部服务器使用10.0.1.x、用户终端根据部门划分使用10.0.2.x、每个分支机构分配两 个A 类地址段，一个用做服务器地址段、另外一个做用户终端地址段

○ D. 因为通过互联网连接，访问的是互联网地址，内部地址经NAT映射，因此IP 地址无需特别规划，各机构自行 决定即可

回答正确 +1分

4. 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（）。 分值1分

○ A. A 类和B 类地址中没有私有地址，C 类地址中可以设置私有地址

○ B. A 类地址中没有私有地址，B 类和C 类地址中可以设置私有地址

● C. A 类、B 类和C 类地址中都可以设置私有地址

○ D. A 类、B 类和C 类地址中都没有私有地址

回答正确 +1分

5. 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：（） 分值1分

○ 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

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

6. 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： （） 分值1分

- 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

回答正确 +1分

7. 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（） 分值1分

- 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

回答正确 +1分

8. 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： （） 分值1分

- 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

回答正确 +1分

9. 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 账户锁定阀值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： （） 分值1分

- 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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ 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

回答正确 +1分

10. 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-x 1 testtest
10704Apr 15 2002/home/ test/sh 请问以下描述哪 个是 正确的： （） 分值1分

○ A. 该文件是一个正常文件，是test用户使用的shell，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，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

回答正确 +1分

11. 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（）。 分值1分

○ 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，EFS加密的用户验证过程是在登录Windows 时进行

回答正确 +1分

12. 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： （） 分值1分

○ 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

回答正确 +1分

13. 113、数据在进行传输前，需要由协议栈自上而下对数据进行封装。TCP/IP 协议中，数据封装的顺序是： （） 分值1分

○ 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

回答正确 +1分

14. 114、以下关于SMTP 和POP3 协议的说法那个是错误的：（） 分值1分

○ A. SMTP和POP3协议是一种基于ASCII 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. SMTP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

回答正确 +1分

15. 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（） 分值1分

● A. 使用专用上网购物用计算机，安装好软件后不要对该计算机上的系统软件、应用软件进行升级

○ B. 为计算机安装具有良好声誉的安全防护软件，包括病毒查杀、安全检查和安全加固方面的软件

○ C. 在IE 的配置中，设置只能下载和安装经过签名的、安全的ActiveX 控件

○ D. 在使用网络浏览器时，设置不在计算机中保留网络历史记录和表单数据

回答正确 +1分

16. 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（） 分值1分

○ 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

回答正确 +1分

17. 117、下面对信息安全漏洞的理解中，错误的是（） 分值1分

○ 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

回答正确 +1分

18. 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？ () 分值1分

○ 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

回答正确 +1分

19. 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：() 分值1分

● 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

回答正确 +1分

20. 120、某单位计划在今年开发一套办公自化（0A）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？ () 分值1分

○ 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

回答错误 +0分

正确答案:

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

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

21. 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（） 分值1分

○ 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

回答正确 +1分

22. 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（） 分值1分

○ 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

回答正确 +1分

23. 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露，根据降低攻击面的原则，应采取哪 项处理措施？ （） 分值1分

○ 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

回答正确 +1分

24. 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： （） 分值1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ 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

回答正确 +1分

25. 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？ （） 分值1分

○ 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

回答正确 +1分

26. 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： （） 分值1分

○ 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

回答正确 +1分

27. 127、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（） 分值1分

○ 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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

回答正确 +1分

28. 128、关于信息安全管理，下面理解片面的是（） 分值1分

- 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

回答正确 +1分

29. 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。 （） 分值1分

- A. 信息安全管理体系(ISMS)
- B. 信息安全等级保护
- C. NIST SP800
- D. ISO 270000 系列

回答正确 +1分

30. 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： （） 分值1分

- 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

回答正确 +1分

31. 131、关于风险要素识别阶段工作内容叙述错误的是： （） 分值1分

- 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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● 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

回答正确 +1分

32. 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（） 分值1分

○ 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

回答正确 +1分

33. 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（）。 分值1分

○ 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》

回答正确 +1分

34. 134、关于业务连续性计划（BCP）以下说法最恰当的是： （） 分值1分

○ A. 组织为避免所有业务功能因重大事件而中断，减少业务风险而建立的一个控制过程

● 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

回答正确 +1分

35. 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PDCERF 应急响应方法，这些工作应处于以下哪个阶段（） 分值1分

○ A. 准备阶段

○ B. 检测阶段

○ C. 遏制阶段

● D. 根除阶段

回答正确 +1分

36. 136、关于信息安全事件管理和应急响应，以下说法错误的是：（） 分值1分

○ 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）

回答正确 +1分

37. 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：（） 分值1分

○ 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

回答正确 +1分

38. 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（） 分值1分

● 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

回答正确 +1分

39. 139、以下关于灾难恢复和数据备份的理解，说法正确的是：（） 分值1分

○ 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

回答正确 +1分

40. 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：（） 分值1分

- 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

回答正确 +1分

41. 141、对系统工程(Systems Engineering,SE)的理解，以下错误的是：（） 分值1分

- 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

回答正确 +1分

42. 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：（） 分值1分

- 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

回答正确 +1分

43. 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：（） 分值1分

- A. 系统安全工程能力成熟度模型(SSE-CMM)定义了6 个能力级别。当工程队伍不能执行一 个过程域中的基本实践时，该过程的过程能力是0 级
- B. 达到 SSE-CMM 最高级以后，工程队伍执行同一个过程，每次执行的结果质量必须相同
- C. 系统安全工程能力成熟度模型(SSE-CMM)定义了 3 个风险过程：评价威胁，评价脆弱性，评价影响
- D. SSE-CMM 强调系统安全工程与其他工程学科的区别性和独立性

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

44. 144、以下哪一项不是信息系统集成项目的特点： () 分值1分

- 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

回答正确 +1分

45. 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： () 分值1分

- 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

回答正确 +1分

46. 146、以下关于信息安全工程说法正确的是（） 分值1分

- 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

回答正确 +1分

47. 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： () 分值1分

- 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

回答正确 +1分

48. 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： () 分值1分

- 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

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

49. 149、以下关于信息安全工程说法正确的是（） 分值1分

- 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

回答正确 +1分

50. 150、系统安全工程-能力成熟度模型(Systems SecurityEngineering-Capability maturity model, 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： （） 分值1分

- A. 风险过程
- B. 工程过程
- C. 保证过程
- D. 评估过程

回答正确 +1分

51. 151、以下行为不属于违反国家保密规定的行为： （） 分值1分

- 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

回答正确 +1分

52. 152、具有行政法律责任强制力的安全管理规定和安全制度包括（）1 > 安全事件(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 分值1分

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

回答正确 +1分

53. 153、信息系统建设完成后，( )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。 （） 分值1分

- A. 二级以上
- B. 三级以上

C. 四级以上

D. 五级以上

回答正确 +1分

54. 154、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（） 分值1分

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

回答正确 +1分

55. 155、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？ () 分值1分

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

回答正确 +1分

56. 156、对于数字证书而言，一般采用的是哪个标准？ () 分值1分

A. ISO/IEC15408

B. 802.11

C. GB/T 20984

D. X.509

回答正确 +1分

57. 157、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？ () 分值1分

A. C2

B. C1

C. B2

D. B1

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

58. 158、关于标准，下面哪项理解是错误的（）。 分值1分

○ 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

回答正确 +1分

59. 159、2005年，RFC4301 (Request for Comments4301: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 分值1分

● 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(D)。

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

○ 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 Secctor，ITU-T)

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

回答正确 +1分

60. 160、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。() 分值1分

○ 4

○ 5

○ 6

● 7

回答正确 +1分

61. 161、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： () 分值1分

● 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。

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

回答正确 +1分

62. 162、有关系统工程的特点，以下错误的是： () 分值1分

○ 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

回答正确 +1分

63. 163、以下关于项目的含义，理解错误的是： () 分值1分

○ 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)

回答正确 +1分

64. 164、以下说法正确的是： () 分值1分

○ 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

回答正确 +1分

65. 165、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： () 分值1分

● 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

回答正确 +1分

66. 166、以下系统工程说法错误的是： () 分值1分

● 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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ 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

回答正确 +1分

67. 167．关于密钥管理，下列说法错误的是: （） 分值1分

○ 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

回答正确 +1分

68. 168、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（） 分值1分

○ A. 准备阶段

● B. 遏制阶段

○ C. 根除阶段

○ D. 检测阶段

回答正确 +1分

69. 169、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（） 分值1分

○ 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

回答正确 +1分

70. 170、“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（） 分值1分

● A. UTM

○ B. FW

○ C. IDS

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ D. SOC

回答正确 +1分

71. 171、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（）。 分值1分

○ 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

回答正确 +1分

72. 172、Gary McGraw 博士及其合作者提出软件安全应由三根支柱来支撑，这三个支柱是（）。 分值1分

○ 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

回答正确 +1分

73. 173、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？（） 分值1分

○ 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

回答正确 +1分

74. 174、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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

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： （） 分值1分

- A. 模糊测试
- B. 源代码测试
- C. 渗透测试
- D. 软件功能测试

回答正确 +1分

75. 175、以下哪一项不是常见威胁对应的消减措施： （） 分值1分

- 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

回答正确 +1分

76. 176、以下关于模糊测试过程的说法正确的是： （） 分值1分

- 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

回答正确 +1分

77. 177、有关危害国家秘密安全的行为，包括： （） 分值1分

- 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

回答正确 +1分

78. 178、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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

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（） 分值1分

- A . 统筹规划
- B. 分组建设
- C. 资源共享
- D. 平战结合

回答正确 +1分

79. 179、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（） 分值1分

- 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

回答正确 +1分

80. 180、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（）。 分值1分

- 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

回答正确 +1分

81. 181、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ACL中，小刘在学习了SID 的组成后，为了巩固所学知识，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SID 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（） 分值1分

- 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 NT的SID 的三个子颁发机构是1534169462、1651380828、111620651

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● D. 此 SID 以500 结尾，表示内置guest 账户

回答正确 +1分

82. 182、/etc/passwd 文件是UNIX/Linux 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 （）、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) 分值1分

☐ 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

回答正确 +1分

83. 183、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 root 10704 Apr 2011:55/usr/bin/passwd （） 分值1分

○ 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

回答错误 +0分

正确答案:

D. s 表示SUID 位，文件在执行阶段具有文件所有者的权限

84. 184、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（）
分值1分

● A. 编辑文件/etc/passwd.检查文件中用户ID，禁用所有ID=O 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_tally.so onerr=faildeny=6unlock_time=300

○ D. 编辑文件/etc/profile,设置TMOUT=600

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

85. 185、目前，信息系统面临外部攻击者的恶意攻击威胁，从威胁能力和掌握资源分，这些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（） 分值1分

○ A. 喜欢恶作剧、实现自我挑战的娱乐型黑客

● B. 实施犯罪、获取非法经济利益网络犯罪团伙

○ C. 搜集政治、军事、经济等情报信息的情报机构

○ D. 巩固战略优势，执行军事任务、进行目标破坏的信息作战部队

回答正确 +1分

86. 186、以下哪种风险被认为是合理的风险（） 分值1分

○ 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(选的人居多)

回答正确 +1分

87. 187、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。（） 分值1分

○ 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

回答正确 +1分

88. 188、以下关于互联网协议安全(Internet Protocol Security,IPsec)协议说法错误的是（） 分值1分

○ 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 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(InternetProtocol,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

回答正确 +1分

89. 189、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IP 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IP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IP 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（） 分值1分

- A. 静态分配地址
- B. 动态分配地址
- C. 静态NAT分配地址
- D. 端口NAT分配地址

回答正确 +1分

90. 190、在Linux 系统中，下列哪项内容不包含在/etc/passwd 文件中（） 分值1分

- A. 用户名
- B、 用户口令…
- C. 用户主目录
- D. 用户登录后使用的SHELL

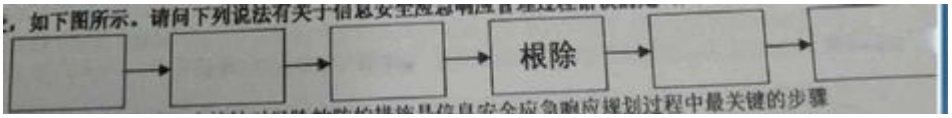
回答正确 +1分

91. 191、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（） 分值1分

- 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

回答正确 +1分

92. 192、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（）



分值1分

- 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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ 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。

回答正确 +1分

93. 193、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（）
分值1分

○ 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

回答正确 +1分

94. 194、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（）。 分值1分

● 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

回答正确 +1分

95. 195、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（） 分值1分

○ 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、软件安全争触点和安全测试

○ 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

回答正确 +1分

96. 196、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（） 分值1分

- 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

回答正确 +1分

97. 197、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（） 分值1分

- 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

回答正确 +1分

98. 198、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（） 分值1分

- 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

回答正确 +1分

99. 199、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。 （） 分值1分

- A、 默认口令
- B、 字典
- C、 暴力
- D、XSS

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

回答正确 +1分

100. 200、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（） 分值1分

- (●) 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

回答正确 +1分

收起答题解析

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

加微信：vic_tom，进cisp考证备考群，请务必备注：备考