CISSP考试练习(习题卷9)

第1部分：单项选择题，共100题，每题只有一个正确答案,多选或少选均不得分。

1.[单选题]在业务连续性计划 (BCP) 的设计中编写计划程序的主要目的是什么?
What is the MAIN purpose for writing planned procedures in the design of Business Continuity Plans (BCP)?
A)尽量减少失败的风险。
Minimize the risk of failure
B)消除不必要的决策。
Eliminate unnecessary decision making.
C)建立责任线。
Establish lines of responsibility.
D)加速恢复过程。
Accelerate the recovery process.
答案:A
解析:

2.[单选题]以下哪项是正式信息分类计划的主要优势?
A)一个。它最大限度地减少了系统日志记录要求。
B)它支持风险评估。
C)它减少了资产漏洞。
D)它推动了审计流程。
答案:B
解析:

3.[单选题]Which of the following is MOST critical in a contract in a contract for data disposal on a hard drive with a third party? 在与第三方签订的硬盘数据处理合同中，以下哪项是最关键的?
A)Authorized destruction times授权销毁时间
B)Allowed unallocated disk space允许的未分配磁盘空间
C)Amount of overwrites required所需覆盖量
D)Frequency of recovered media恢复介质的频率
答案:C
解析:

4.[单选题]When performing an investigation with the potential for legal action, what should be the analyst's FIRST consideration? 当进行可能采取法律行动的调查时，分析员应首先考虑什么?
A)Chain-of-custody产销监管链
B)Authorization to collect收款授权书
C)Court admissibility法院受理
D)Data decryption数据解密
答案:A
解析:

5.[单选题]Between which pair of Open System Interconnection（OSI）Reference Model layers are routers used as a communications device? 路由器在哪对开放系统互连（OSI）参考模型层之间用作通信设备?
A)Transport and Session传输层和会话层
B)Data-Link and Transport数据链路层和传输层

C)Network and Session网络层和会话层
D)Physical and Data-Link物理层和数据链路层
答案:B
解析:

6.[单选题]RAID 磁盘名称等级 1 将数据从一个磁盘组到一个磁盘组
A)将数据复制到另一种磁盘或轴承上。
B)将数据移动到其他磁盘或轴承。
C)建立连接到另一种磁盘或轴承。
D)建立双寻址到磁盘或石墨。
答案:A
解析:通过复制过程同时

7.[单选题]Robert 正在审查根据共同标准分配了EAL2评估保证级别的系统。他对系统的最高保证是什么?
A)它已经完成了功能测试
B)它已经完成了结构测试
C)它已经完成了正式的验证、设计和测试
D)它已经半正式地完成了设计和测试
答案:B
解析:EAL2 可以保证系统通过结构测试,这是通用标准下的第二级别到最低级别的保证。
EAL2 assurance applies when the system has been structurally tested. It is the second-to-lowest level of assurance under the Common Criteria.

8.[单选题]在这里所示的图像中,系统B在三次TCP握手的步骤2处向系统A发送什么?
A)SYN
B)ACK
C)FIN/ACK
D)SYN/ACK
答案:D
解析:三次握手分别是SYN、SYN/ACK、ACK,系统B在收到 SYN 之后应该向系统A 发送SYN/ACK。
The three-way handshake is SYN, SYN/ACK, ACK. System B should respond with “Synchronize and Acknowledge" to System A after it receives a SYN.

9.[单选题]数据分类可用在除哪一项之外的所有安全控制中?
A)存储
B)处理
C)分层
D)传输
答案:C
解析:

10.[单选题]为了使审计报告被接受,组织必须考虑以下哪项?
Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?
A)审计评估是由独立评估员进行的
The audit assessment has been conducted by an independent assessor.
B)审计报告已由第三方高级管理人员签署
The audit reports have been signed by the third-party senior management.
C)审计报告是最近六个月出具的
The audit reports have been issued in the last six months.
D)审计评估是由国际审计公司进行的

The audit assessment has been conducted by an international audit firm.
答案:A
解析:

11.[单选题]CaptainCrunch 是一种有名的手机诈骗,使用玩具口哨来模拟电话中继系统用于通信的 2600Hz声音。这种盗用电话线路工具的共有名称叫什么?
A)黑盒
B)红盒
C)蓝盒
D)白盒
答案:C
解析:攻击者使用蓝盒工具来生成中继系统使用的2600Hz 音调。白盒包括双音多频生成器以控制电话系统,黑盒旨在通过操纵线路电压窗取长途服务,红盒模拟掉入投币电话中的硬币的音调。
A blue box was used to generate the 2600 Hz tones that trunking systems required.White boxes included a dual-tone,multifrequency generator to controi phone systems.Black boxes were designed to steal long-distance service by manipulating line voltages,and red boxes simulated the tones of coins being deposited into payphones.

12.[单选题]在 制定灾后恢复计划 (DRP) 时,以下哪一项是最重要的考虑因素?
A)系统的动态重新配置
B)停机成本
C)所有业务流程的恢复策略
D)遏制 战略
答案:C
解析:

13.[单选题]A Chief Information Security Officer (CISO) of a firm which decided to migrate to cloud has been tasked with ensuring an optimal level of security. Which of the following would be the FIRST consideration? 一家决定迁移到云的公司的首席信息安全官 (CISO) 的任务是确保最佳的安全级别。以下哪一项是第一个考虑因素？
A)Define the cloud migration roadmap and set out which applications and data repositories should be moved into the cloud. 定义云迁移路线图，并确定应将哪些应用程序和数据存储库移动到云中。
B)Ensure that the contract between the cloud vendor and the firm clearly defines responsibilities for operating security controls. 确保云供应商和公司之间的合同明确规定了运营安全控制的责任。
C)Analyze the firm's applications and data repositories to determine the relevant control requirements. 分析公司的应用程序和数据存储库，以确定相关的控制要求。
D)Request a security risk assessment of the cloud vendor be completed by an independent third- party. 请独立的第三方完成云供应商的安全风险评估。
答案:A
解析:

14.[单选题]In a data classification scheme, the data is owned by the在数据分类方案中，数据由
A)system security managers系统安全管理器
B)business managers企业管理者
C)Information Technology (IT) managers信息技术 (IT) 经理
D)end users最终用户
答案:B
解析:

15.[单选题]What Is the FIRST step in establishing an information security program? 建立信息安全计划的第一步是什么?

A)Establish an information security policy. 制定信息安全策略。
B)Identify factors affecting information security. 确定影响信息安全的因素。
C)Establish baseline security controls. 建立基线安全控制。
D)Identify critical security infrastructure. 确定关键的安全基础架构。
答案:A
解析:

16.[单选题]重复使用包含敏感数据的媒体时,以下哪一项是最合适的操作?
A)擦 除
B)消毒
C)加密
D)德加乌斯
答案:B
解析:

17.[单选题]那个模型将操作分解成不同的环节并要求由每个单独的环节由不同的用户来执行?
A)Bell-LaPadula 模型
B)非干扰模型
C)CIark-Wilson 模型
D)Biba模型
答案:C
解析: The Clark-Wilson model uses separation of duties, which divides an operation into different parts and requires different users to perform each part. This prevents authorized users from making unauthorized modifications to data, thereby protecting its integrity.

18.[单选题]哪种安全方法最能最大限度地减少数据泄露造成的个人可识别信息 (PII)损失?
A)每个通知过程的强 br
B)个人机密数据收集有限
C)传输数据的端到端数据加密
D)持续监测潜在 漏洞
答案:B
解析:

19.[单选题]下列哪一项限制了个人执行特定过程的所有步骤的能力?
A)工作轮换
B)职责分离
C)最少 的特权
D)强制性 假期
答案:B
解析:

20.[单选题]Proven application security principles include which of the following? 经验证的应用程序安全原则包括以下哪项?
A)Minimizing attack surface area最小化攻击表面积
B)Hardening the network perimeter强化网络周界
C)Accepting infrastructure security controls接受基础架构安全控制
D)Developing independent modules开发独立模块
答案:A
解析:

21.[单选题]Functional security testing is MOST critical during which phase of the system development

life cycle（SDLC）？功能安全测试在系统开发生命周期（SDLC）的哪个阶段最为关键？
A)Operations / Maintenance操作/维护
B)Implementation实施
C)Acquisition / Development收购/开发
D)Initiation起始
答案:B
解析:

22.[单选题]在构建数据分类方案时,主要关注以下哪一个?
A)目的
B)成本 效益
C)可用性
D)真实性
答案:D
解析:

23.[单选题]第三方合同以下哪项应该有最高的优先级？
A)发生灾难后重新谈判的权利
B)灾难恢复处理升级的流程
C)合同到期后争议解决的办法
D)合同涉及赔偿的条款
答案:B
解析:略
章节：模拟考试202201

24.[单选题]事件处理首要的目标是？
A)成功检索所有可用来检举的证据。
B)提高公司应对威胁和灾难的能力。
C)完善公司的灾难恢复计划
D)包含和修复事件所造成的任何损害
答案:D
解析:

25.[单选题]VOIP 在语音通信过程当中， 弱点?
A)没有目标认证
B)没有源认证
C)3 层协议， 没有保障
D)不能保证完整性
答案:B
解析:略
章节：模拟考试202201

26.[单选题]What type of attack sends Internet Control Message Protocol（ICMP）echo requests to the target machine with a larger payload than the target can handle? 哪种类型的攻击将Internet控制消息协议（ICMP）回送请求发送到目标计算机，其有效负载超过目标计算机的处理能力？
A)Man-in-the-Middle（MITM）中间人（MITM）
B)Denial of Service（DoS）拒绝服务（DoS）
C)Domain Name Server（DNS）poisoning域名服务器（DNS）中毒
D)Buffer overflow缓冲区溢出
答案:B
解析:

27.[单选题]数据中心弹簧门在火灾发生时开放。这是一个什么例子？
A)自动防故障
B)自动防故障
C)失效安全
D)防故障
答案:A
解析: Fail-safe mechanisms focuses on failing with a minimum of harm to personnel while fail-secure focuses on failing in a controlled manner to block access while the systems is in an inconsistent state. For example, data center door systems will fail safe to ensure that personnel can escape the area when the electrical power fails. A fail-secure door would prevent personnel from using the door at all, which could put personnel in jeopardy. Fail-open and fail-closed are fail safe mechanisms.

28.[单选题]以下哪一项最能支持在将补丁应用于组织系统时对修补程序兼容性进行有效测试 ？
A)斯坦的配置设备s
B)标准化补丁测试 设备
C)自动系统 修补
D)修补的管理支持
答案:A
解析:

29.[单选题]下列哪个不是一个有效的理由，在使用外部渗透服务公司，而不是公司资源？
A)他们确保更完整的报告
B)他们使用了更高端的黑客人员
C)他们提供无企业偏见
D)他们更划算
答案:C
解析: Two points are important to consider when it comes to ethical hacking: integrity and independence.

30.[单选题](04158) 在追踪事件时发现，只能提供最近30天内的审计日志。这需要关注：
A)数据恢复
B)数据恢复
C)数据恢复
D)数据恢复
答案:A
解析:

31.[单选题]Similarly, Kerberos depends on KDC,SAML. Depends on:类似于Kerberos依赖于KDC,SAML.依赖于;
A)TGS
B)IDP
C)AS
D)PAS
答案:B
解析:

32.[单选题]检测出第一首信息系统的一个行为，对下面第一首信息哪一个？
A)所有消除者访问的方式
B)控件控制
C)确定系统和数据破坏的程度

D)相关与进行分区
答案:B
解析:

33.[单选题]Additional padding may be added to the Encapsulating security protocol (ESP) trailer to provide which of the following? 可以向封装安全协议（ESP）尾部添加额外的填充，以提供以下哪项?
A)Data origin authentication数据源认证
B)Partial traffic flow confidentiality部分流量机密性
C)protection ao>ainst replay attack保护ao>ainst重播攻击
D)Access control访问控制
答案:C
解析:

34.[单选题]What is one feature of the Security Assertion Markup Language (SAML)?
安全断言标记语言(SAMAL)的一项功能是?
A)strategy execution策略执行
B)Redundancy check元余检查
C)Extended validation扩展验证
D)File allocation文件分配
答案:A
解析:

35.[单选题]一家零售公司的雇员已获得人力资源部 (HR) 的延长休假。
此信息已正式传达给访问提供团队。以下哪一项是最好的行动?
A)暂时撤销访问 权限。
B)在六个月后阻止用户访问并删除用户帐户 。
C)立即阻止访问办公室 。
D)蒙伊托帐户使用 时间总是。
答案:D
解析:

36.[单选题]在美国，专利保护的标准期限是多少？
A)自申请之日起14年
B)自专利别授予之日起14年
C)自申请日起20年
D)自专利被授予之日起20年
答案:C
解析:

37.[单选题]你的老板想把大楼的暖通空调系统和照明控制自动化,以降低成本。他建议你保持低成本,使用现成的设备。当您在私人环境中使用loT设备时,降低风险的最佳方法是什么?
A)使用公网IP地址
B)设备不使用时,请切断电源
C)保持设备的最新更新
D)禁止物联网设备接入互联网
答案:C
解析:C.减少这些选项的loT风险的最好方法是保持设备的最新更新。使用公网IP地址将使物联网设备暴露于来自互联网的攻击。
关闭设备电源并不是一个有用的防御措施--loT的好处是,它们总是在运行,随时可以使用,或在触发或计划时采取行动。阻止互联网接入将阻止loT设备自己获取更新,可能会阻止它们通过移动设备应用程序进行控制,并将阻止与任何相关云服务的通信。

38.[单选题]提供关于安全控制措施有效性报告给高级管理层，是谁的责任
A)信息系统审计员
B)数据拥有者
C)信息系统安全专家
D)数据保管者
答案:A
解析: T auditors determine whether systems are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction and other requirements" and "provide top company management with an independent view of the controls that have been designed and their effectiveness."

39.[单选题]以下哪项密码攻击描述了攻击者有明文的副本和相应的密文？
A)强力攻击
B)密文
C)选择明文
D)已知明文
答案:D
解析: The goal to this type of attack is to find the cryptographic key that was used to encrypt the message. Once the key has been found, the attacker would then be able to decrypt all messages that had been encrypted using that key.

40.[单选题]In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs? 在变更控制的环境中，以下哪项最有可能导致对生产程序进行未经授权的变更？
A)Modifying source code without approval未经批准修改源代码
B)Promoting programs to production without approval未经批准将节目推向生产
C)Developers checking out source code without approval开发人员未经批准就签出源代码
D)Developers using Rapid Application Development (RAD) methodologies without approval未经批准使用快速应用程序开发（RAD）方法的开发人员
答案:A
解析:

41.[单选题]建议使用以下哪种报警系统来检测高噪音、占用环境中通过窗户的入侵?
A)声学传感器
B)运动传感器
C)冲击传感器
D)光电 传感器
答案:C
解析:

42.[单选题]以下哪项不属于代码审查?
A)电子邮件传递
B)Overtheshoulder
C)配对编程
D)指定 IDE
答案:D
解析:“Over-the-shoulder”审查要求原始开发者在走查代码的时候向同伴解释他的代码。电子邮件传递代码审查将代码发送给同行进行审查。结对编程需要两个开发人员,只有其中一个编写代码,而另一个人负责与之协作。“指定IDE”不是一种代码审查,IDE 是集成开发环境的简称。
Over-the-shoulder reviews require the original. developer to explain her code to a peer while walking

through it. Email pass-around code reviews are done by sending code for review to peers. Pair programming requires two developers, only one of whom writes code while both collaborate.

43.[单选题](04154) 进行安全认证的主要目的是：
A)识别系统威胁、漏洞和可接受的风险水平
B)识别系统威胁、漏洞和可接受的风险水平
C)识别系统威胁、漏洞和可接受的风险水平
D)识别系统威胁、漏洞和可接受的风险水平
答案:C
解析:

44.[单选题]更新在多个或远程整个数据库，作为一种方法来确保适当的记录和放置位置，被称为：
A)数据镜像
B)影像复制
C)备份
D)文件
答案:B
解析: 数据镜像是一种 RAID 技术，它将所有磁盘写入从一个磁盘复制到另一个磁盘，以创建两个相同的驱动器。数据库阴影是一种在多个位置对更新进行阴影的技术。这就像将整个数据库复制到远程位置。备份将定期进行，并有助于在发生灾难时恢复信息或系统。归档是指存储没有 出于历史目的而持续使用的数据。

45.[单选题]In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill? 在灾难恢复（DR）和业务连续性培训中，哪一项最能描述功能演练？
A)A full-scale simulation of an emergency and the subsequent response functions紧急情况和后续响应功能的全尺寸模拟
B)A specific test by response teams of individual emergency response functions由响应团队对单个应急响应功能进行的特定测试
C)A functional evacuation of personnel人员功能性疏散
D)An activation of the backup site激活备份站点
答案:C
解析:

46.[单选题]以下哪种方法是在多个硬盘驱动器上处置数据的最有效方法?
A)一个。删除每个驱动器上的每个文件。
B)使用命令行销毁每个驱动器的分区表。
C)单独消磁每个驱动器。
D)使用批准的格式化方法在每个驱动器上执行多次传递。
答案:D
解析:

47.[单选题]以下哪一项不是磁带备份的性质或问题？
A)-个大的磁盘使用多个磁盘创建
B)在备份和恢复期间数据传输缓慢
C)服务器磁盘空间利用率扩展
D)可能需要一些数据重新输入。
答案:A
解析: The correct answer is "One large disk created by using several disks". RAID level 0 striping is the process of creating a large disk out of several smaller disks.

48.[单选题]在使用OAuth(开放标准授权)2.0整合第三方身份验证者时,以下哪个问题不能得到解决?
Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to

integrate a third-party identity provider for a service?
A)需要资源服务器使用密码来验证最终用户
Resource Servers are required to use passwords to authenticate end users.
B)撤销第三方的一些用户而不是第三方所有用户的访问权
Revocation of access of some users of the third party instead of all the users from the third party.
C)第三方的漏洞意味着对服务的所有用户的漏洞
Compromise of the third party means compromise of all the users in the service.
D)客人用户(guest users)需要第三方身份提供商进行验证
Guest users need to authenticate with the third party identity provider.
答案:A
解析:

49.[单选题]下列哪项攻击依赖于对次要目标的破坏以达到主要目标?
A)水坑
B)鱼叉式网络钓鱼
C)ARP中毒
D)暴力破解
答案:C
解析:

50.[单选题]每次都完全地备份服务器上每个文件的备份方法是什么?
A)完全备份方法
B)增量备份方法
C)差异备份方法
D)录音方法
答案:A
解析:

51.[单选题]Lauren 希望对她正在处理的应用程序使用软件审查流程。 如果她是一名远程工作者,与团队其他成员的工作时间不同,那么以下哪个流程最有效?
A)Pass around
B)Pair programming
C)Team review
D)Fagan inspection
答案:A
解析:传递审查通常通过电子邮件或使用中央代码审查系统完成,允许开发人员异步审查代码。 结对编程需要两个程序员一起工作,一个编写代码,另一个审查和跟踪进度。
团队审查通常在一个小组中完成,而 Fagan 检查是一个正式的审查过程,开发人员和团队都将使用正式的过程审查代码。

52.[单选题]An Internet software application requires authentication before a user is permitted to utilize the resource. Which testing scenario BEST validates the functionality of the application? 在允许用户使用资源之前, Internet软件应用程序需要身份验证。哪个测试场景最能验证应用程序的功能?
A)Reasonable data testing合理的数据测试
B)Input validation testing输入验证测试
C)Web session testing Web会话测试
D)Allowed data bounds and limits testing允许的数据界限和限制测试
答案:B
解析:

53.[单选题]Asymmetric algorithms are used for which of the following when using Secure Sockets

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/675020140324011110