CISSP考试练习(习题卷12)

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]以下哪一项是使用自动风险分析工具的最好理由？
A)大部分审查期间收集的数据不能用于随后的分析
B)大多数软件工具具有易于使用，且不需要任何训练的用户界面
C)自动化方法所需的培训和风险知识最少
D)由于大量信息已构建到工具中，信息收集将被最小化，并且加快
答案:D
解析:

2.[单选题]下列选择中，哪一项能在不牺牲安全性的情况下避免这种损失
A)标记场外保持的介质
B)不要在场外存储数据
C)销毁在场外存储的备份
D)使用安全的异地存储设备
答案:D
解析:

3.[单选题]Rivest-Shamir-Adleman (RSA)算法最适合以下哪种操作? The Rivest-Shamir-Adleman (RSA)algorithm is BEST suited for which of the following operations?
A)批量数据加解密
Bulk data encryption and decryption
B)用于用户和消息身份验证的单向安全散列
One-way secure hashing for user and message authentication
C)对称加密的安全密钥交换
Secure key exchange for symmetric cryptography
D)为消息完整性创建数字校验和
Creating digital checksums for message integrity
答案:C
解析:

4.[单选题]A web-based application known to be susceptible to attacks is now under review by a senior developer. The organization would like to ensure this application Is less susceptible to injection attacks specifically, What strategy will work BEST for the organization's situation? 一位高级开发人员正在审查一个已知易受攻击的基于web的应用程序。组织希望确保此应用程序不易受到注入攻击。具体来说，什么策略最适合组织的情况？
A)Do not store sensitive unencrypted data on the back end.不要在后端存储敏感的未加密数据。
B)Whitelist input and encode or escape output before it is processed for rendering.白名单输入和编码或转义输出之前，它是处理呈现。
C)Limit privileged access or hard coding logon credentials.限制特权访问或硬编码登录凭据。
D)Store sensitive data in a buffer that retains data in operating system (OS) cache or memory.将敏感数据存储在将数据保留在操作系统(OS)缓存或内存中的缓冲区中。
答案:B
解析:

5.[单选题]Mandatory Access Controls (MAC) are based on: 强制访问控制 (MAC) 基于：

A)Security classification and security clearance. 安全分类和安全许可。
B)Data segmentation and data classification. 数据分割和数据分类。
C)Data labels and user access permissions. 数据标签和用户访问权限。
D)User roles and data encryption. 用户角色和数据加密。
答案:A
解析:

6.[单选题]In software development, which of the following entities normally signs the code to protect the code integrity? 在软件开发中，以下哪个实体通常签署代码以保护代码完整性？
A)The organization developing the code开发代码的组织
B)The quality control group质量控制小组
C)The data owner数据所有者
D)The developer开发人员
答案:B
解析:

7.[单选题]In which process MUST security be considered during the acquisition of new software? 在购买新软件的过程中，必须考虑哪个过程的安全性？
A)Contract negotiation合同谈判
B)Request for proposal（RFP）招标书（RFP）
C)Implementation实施
D)Vendor selection供应商选择
答案:B
解析:

8.[单选题]以下哪种类型的攻击涉及到IP欺骗，ICMP ECHO 和网站反弹
A)IP欺骗攻击
B)Smurf 攻击
C)SYN攻击
D)Teardrop 攻击
答案:B
解析:

9.[单选题]What is one advantage of deploying Role based access control in large networked applications? 在大型网络化应用中,部署基于角色的访问控制的一个优点是什么?
A)Higher security更高的安全性
B)Higher bandwidth更高的带宽
C)User friendliness用户友好性
D)Lower cost 更低的成本
答案:D
解析:

10.[单选题]虚拟机(VM)环境具有五个来宾操作系统(OS),并提供强隔离,管理员必须审核哪些内容才能审核用户对数据文科的访问权限?
A)一个。主机虚拟机监视器审核日志
B)来宾操作系统访问控制
C)主机虚拟机访问控制
D)来宾操作系统审核日志
答案:A
解析:

11.[单选题]什么法律阻止版权持有人取消对受版权保护作品的保护机制?
A)HIPAA
B)DMCA
C)GLBA
D)ECPA
答案:B
解析:《数字千年版权法案》(DMCA)通过立法方式,对网上作品著作权的保护提供了法律依据,其主要特点体现在以著作权人为中心,加强对权益的保护。The Digital Millennium Copyright Act (DMCA) prohibits attempts to circumvent copyright protection mechanisms placed on a protected work by the copyright holder.

12.[单选题]发现组织在审计期间无法正确确定其 Web 托管解决方案的性能指标。最可能的原因是什么?
A)服务导向型架构(SOA)的不当部署
B)缺少布辛智能(BI)解决方案
C)成本建模不足
D)服务级别协议 不足
答案:D
解析:

13.[单选题]以下哪一项提供了传输身份验证令牌的最佳安全功能?
A)JavaScript 对象表示法 (JSON)
B)终端访问控制器访问控制系统(TACACS)
C)安全断言标记语言 (SAML)
D)远程认证拨入用户服务 (RADIUS)
答案:C
解析:

14.[单选题]A hacker can use a lockout capability to start which of the following attacks? 黑客可以使用锁定功能启动以下哪种攻击?
A)Denial of service (DoS) 拒绝服务 (DoS)
B)Dictionary词典
C)Ping flood客以封包洪流
D)Man-in-the-middle (MITM) 中间人 (MITM)
答案:A
解析:

15.[单选题]SDLC 在什么环境就应该开始考虑安全需求
A)需求分析确认
B)代码编写
C)运行维护
D)结束废弃
答案:A
解析:略
章节：模拟考试202201

16.[单选题]防止无意中披露受限制的信息,以下哪一项是媒体被丢弃之前消除数据的最不有效的流程?
A)多路 过写
B)消磁
C)高级 格式设置
D)物理破坏n
答案:C
解析:

17.[单选题]安全顾问被要求对某机构就保护隐私相关信息的法律义务进行调查,以下哪一类阅读材料与这一项目的关联度最高?
A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?
A)机构目前与隐私相关的安全政策
The organization's current security policies concerning privacy issues
B)由管理机构强制的试用于该机构的相关隐私法规
Privacy-related regulations enforced by governing bodies applicable to the organization
C)由公认的安全标准组织所公布的有关隐私的最佳实践
Privacy best practices published by recognized security standards organizations
D)由机构设计的旨在保护隐私信息的规程
Organizational procedures designed to protect privacy information
答案:B
解析:

18.[单选题]While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government- issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team? 在对新产品进行安全审查时，信息安全专业人员发现，该组织的产品开发团队建议从客户处收集政府发布的标识（ID）号，以用作唯一的客户标识符。应向产品开发团队提出以下哪项建议？
A)Customer identifiers should be a variant of the user's government-issued ID number. 客户标识符应该是用户政府颁发的ID号的变体。
B)Customer identifiers that do not resemble the user's government-issued ID number should be used. 应使用与用户政府颁发的ID号不相似的客户标识符。
C)Customer identifiers should be a cryptographic hash of the user's government-issued ID number. 客户标识符应该是用户政府颁发的ID号的加密哈希。
D)Customer identifiers should be a variant of the user's name, for example, "jdoe" or "john.doe." 客户标识符应该是用户名的变体，例如，“jdoe”或“john.doe”
答案:C
解析:

19.[单选题]信息系统审查的集中是相关定义1T服务级别过程中的控制措施。下列哪个工作人员最适合在审查期间提供信息？
A)程序员
B)业务单元经理
C)法律工作人员
D)系统程序员
答案:B
解析: Understanding the business requirements is key in defining the service levels. While each of the other entities listed may provide some definition, the best choice here is the business unit manager, because of the broad knowledge that this person has over the related requirements of the organization.

20.[单选题]Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities? 漏洞扫描程序允许管理员分配以下哪项，以帮助确定补救活动的优先级？
A)Definitions for each exposure type每种暴露类型的定义
B)Vulnerability attack vectors漏洞攻击向量
C)Asset values for networks网络的资产价值

D)Exploit code metrics利用代码度量
答案:C
解析:

21.[单选题]哪一个是基本的防火墙?
A)包过滤防火墙
B)代理防火墙
C)以上都是
D)以上都不是
答案:A
解析: 包过滤防火墙 - 仅检查基于源 IP (SIP)、目的地
IP (DIP)、源端口和目的地端口的 IP 数据包，用于 UDP 和 TCP，通过服从每个 IP
数据包到访问控制列表。

22.[单选题]弗洛里安收到美国联邦政府机构的传单,宣布一项新的行政法将影响他的业务运营。 他应该去哪里寻找法律文本?
Florian receives a flyer from a U.S. federal government agency announcing that a new administrative law will affect his business operations. Where should he go to find the text of the law?
A)美国法典
United States Code
B)最高法院的裁决
Supreme Court rulings
C)联邦法规
Code of Federal Regulations
D)法律纲要
Compendium of Laws
答案:C
解析:

23.[单选题]在漏洞评估期间,以下哪些活动最有可能被执行?
Which of the following activities is MOST likely to be performed during a vulnerability assessment?
A)建立来访者身份验证程序去验证用户身份
Establish caller authentication procedures to verify the identities of users.
B)通过与相关方进行面谈来分析环境
Analyze the environment by conducting interview sessions with relevant parties.
C)把不合规方式访问的例外情况记录为策略
Document policy exceptions required to access systems in non-compliant areas.
D)审查漏洞评估团队或供应商的专业证书
Review professorial credentials of the vulnerability assessment team or vendor.
答案:D
解析:

24.[单选题]构建防火墙的第一步是
A)分配防火墙管理员的角色和责任 。
B)定义将阅读防火墙策略的预期受众 。
C)确定鼓励遵守政策的机制 。
D)执行 风险分析,以确定需要解决的问题 。
答案:D
解析:

25.[单选题]使用接近卡进入建筑物是哪种类型的安全控制的一个例子?
A)法律
B)逻辑
C)物理的
D)程序
答案:C
解析:

26.[单选题]为实现其目标, Jack 最适合遵循哪种 ISO/IEC 标准?
A)ISO/IEC 27002
B)ISO/IEC 27004
C)ISO/IEC 27005
D)ISO/IEC 27006
答案:C
解析:

27.[单选题]Isabelle希望通过其组织的服务帐户阻止特权提升攻击。以下哪种安全实践最适合这种情况?Isabelle wants to prevent privilege escalation attacks via her organization's service accounts. Which of the following security practices is best suited to this?
A)删除不必要的权限
Remove unnecessary rights.
B)禁用服务帐户的交互式登录
Disable interactive login for service accounts.
C)限制帐号可以登录的时间
Limit when accounts can log in.
D)为服务帐户使用无意义或随机的名字
Use meaningless or randomized names for service accounts.
交互式登录是我们平常登录时最常见的类型,就是用户通过相应的用户账号(User Account)和密码在本机进行登录。有些网友认为“交互式登录”就是“本地登录”,其实这是错误的。“交互式登录”还包括“域账号登录”,而“本地登录”仅限于“本地账号登录”。默认是关闭的,需要进行输入用户名密码,开启后不需要。
答案:A
解析:保护服务帐户安全的最重要的一步是确保它们仅拥有完成其设计任务所需要的绝对权限。 禁用交互式登录也很重要,这将是下一个最佳答案:。限制帐户何时可以登录并使用随机或无意义的帐户名称,在某些情况下可能会有所帮助,但却不那么重要。

28.[单选题]The use of private and public encryption keys is fundamental in the implementation of which of the following? 私有和公共加密密钥的使用是实现以下哪项的基础?
A)Diffie-Hellman algorithm Diffie-Hellman算法
B)Secure Sockets Layer (SSL) 安全套接字层 (SSL)
C)Advanced Encryption Standard (AES) 高级加密标准 (AES)
D)Message Digest 5 (MD5) 消息摘要5 (MD5)
答案:B
解析:

29.[单选题]Charles 正在开发一种对人类安全有直接影响的关键任务应用程序。
时间和成本不如正常运行的软件重要。 鉴于这些要求,他应该选择以下哪种软件开发方法?
A)敏捷
B)开发运营
C)螺旋
D)瀑布
答案:D

解析:尽管许多组织转向敏捷、DevOps 或其他响应更快的开发方法,但当明确的目标和稳定的需求与防止缺陷和高水平的需求相结合时,瀑布仍然是控制开发过程和输出中一个强力的竞争者。

30.[单选题]以下哪项启动灾难恢复计划的系统恢复阶段?
A)激活组织的热站点
B)发布正式灾难声明
C)评估灾难后的破坏程度
D)撤离灾区
答案:B
解析:

31.[单选题]自由裁量访问控制 (DAC)根据
A)数据分类 标签。
B)应用程序中的页面视图 。
C)授予用户的授权 。
D)管理 认证。
答案:C
解析:

32.[单选题](04013) Which of the following rules is less likely to support the concept of least privilege?下面哪个规则最不可能支持了最小特权的概念
A)The number of administrative accounts should be kept to a minimum管理员账户的数量应当保持最少化
B)The number of administrative accounts should be kept to a minimum管理员账户的数量应当保持最少化
C)The number of administrative accounts should be kept to a minimum管理员账户的数量应当保持最少化
D)The number of administrative accounts should be kept to a minimum管理员账户的数量应当保持最少化
答案:C
解析:

33.[单选题]允许数据对象所有者允许其他用户访问该对象的做法通常会提供
A)强制性访问控制 (MAC)。
B)所有者管理 的控制。
C)依赖所有者的访问 控制。
D)可自由裁量权控制 (DAC)。
答案:D
解析:

34.[单选题]检测到一个url http://xxx.xxx.com/product.sap? id=1 or 1=1
A)sql注入
B)XSS
C)CSRF
D)缓存溢出
答案:A
解析:略
章节：模拟考试202201

35.[单选题]什么级别的 RAID 也称为具有奇偶校验的磁盘条带化?
A)RAID0
B)RAID1
C)RAID5
D)RAID10
答案:C

解析:RAID 级别5也被称为具有奇偶性的磁盘条带化。
RAID 0 称为磁盘条带化。RAID 1 称为磁盘镜像。
RAID 10 称为镜像条。
RAID level 5 is also known as disk striping with parity.
RAID 0 is called disk striping. RAID 1 is called disk mirroring. RAID 10 is known as a stripe of mirrors.

36.[单选题]在法庭上，可容许的计算机证据必须是下列哪项?
A)有罪的证据
B)编辑过的
C)解密的
D)相关的
答案:D
解析:

37.[单选题]知识产权主要关注l以下哪一项?
A)一个。所有者实现经济收益的能力
B)所有者维护版权的能力
C)所有者享受其创作的权利
D)所有者控制交付方式的权利
答案:D
解析:

38.[单选题]Which testing method requires very limited or no information about the network infrastructure? 哪种测试方法需要非常有限或没有关于网络基础设施的信息?
A)While box白盒
B)Static静止
C)Black box黑盒
D)Stress强调
答案:C
解析:

39.[单选题]以下哪项是攻击 Internet 协议 (IP) v6 第 3 层和第 4 层的方法?
Which of the following is a method of attacking internet protocol (IP) v6 Layer 3 and Layer 4?
A)Internet 控制消息协议 (ICMP) 泛洪
Internet Control Message Protocol (ICMP) flooding
B)媒体访问控制 (MAC)泛洪
Media Access Control (MAC)flooding
C)域名服务器 (DNS) 缓存中毒
Domain Name Server (DNS) cache poisoning
D)同步序列号(SYN)泛洪
Synchronize sequence numbers (SYN) flooding
答案:D
解析:

40.[单选题]Steven's staff has asked for funding to implement technology that provides Mobile lP. Steven's staff has asked forfunding to implement technology that provides Mobile lP.which of the following would be a reason for employing thistype of technology?史提芬的工作人员已经要求提供资金以实施提供移动IP技术,下列哪项是采用这种技术的原因?
A)Employees can move from one network to another员工可以从一个网络移动到另一个网络
B)Peer-to-peer networks would not be allowed不允许对等网络

C)Security staff could carry out sniffing安全人员可以进行嗅
D)Users would not be allowed to move theirwireless devices and still stay connected to the network用户将不被允许移动他们的无线设备,并仍然保持连接到网络
答案:A
解析:

41.[单选题]BCP业务连续性计划基于?
A)关于灾难恢复要求事项的检测表
B)同行业的BCP 业务连续性计划实践
C)方针和规程手册
D)对业务流程和规范的评审
答案:D
解析:略
章节：模拟考试202201

42.[单选题]with byte-level?RAID的不同级别决定了将在RAID系统中发生的活动类型。下面哪个级别与字节级别相关联?
A)RAID Level 0
B)RAID Level 3
C)RAID Level 5
D)RAID Level 10
答案:B
解析:

43.[单选题]以下哪一项在笔记本电脑被盗时提供最可防止敏感信息数据被盗的保护?
A)设置 BIOS 和操作系统 密码
B)加密可以存储机密文件的虚拟驱动器
C)实施一项强制性政策,其中敏感数据不能存储在笔记本电脑上,而只能存储在公司网络上
D)加密整个磁盘,并在一定次数的访问尝试失败后删除内容
答案:D
解析:

44.[单选题]A security engineer is required to integrate security into a software project that is implemented by small groups test quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process'安全工程师需要将安全性集成到一个软件项目中，该项目由小组实施，快速、连续、独立地开发、测试代码并将其部署到云。工程师最有可能与哪个软件开发过程集成'
A)Service-oriented architecture（SOA）面向服务的体系结构（SOA）
B)Spiral Methodology旋转式
C)Structured Waterfall Programming Development结构化瀑布式编程开发
D)Devops Integrated Product Team（IPT）Devops综合产品团队（IPT）
答案:C
解析:

45.[单选题]在系统开发生命周期中，是安全提供了最大的生命体验吗?
A)系统需求定义阶段。
B)系统设计阶段
C)程序开发阶段。
D)程序测试阶段。
答案:B
解析:

46.[单选题]在保管处理链中对文件进行哈希时,确保以下哪一项?
A)可用性
B)问 责
C)正直
D)非反古迪亚蒂上
答案:C
解析:

47.[单选题]由于市场份额的迅速增加,组织的规模增加了一倍。信息技术(IT)工作人员的规模一直与这一增长保持同步。该组织雇用了几个承包商,他们的现场时间被我限制。IT 部门已突破其构建服务器和推出工作站的限制,并积压了帐户管理请求。
哪份合同最适合从 IT 人员那里卸载任务?
A)平台作为服务 (PaaS)
B)身份作为服务 (IDaaS)
C)桌面服务 (DaaS)
D)软件作为服务 (SaaS)
答案:B
解析:

48.[单选题]使用自动应用程序安全测试工具的主要优势是什么?
A)该应用程序可以在生产环境中得到保护 。
B)大量的代码可以使用更少的资源进行测试 。
C)使用这些工具进行测试时,应用程序的故障会更少 。
D)德泰主导的代码功能测试可以 执行。
答案:B
解析:

49.[单选题]身份管理系统的哪些功能的实施在改进审计和问责制的同时降低了成本和管理费用?
A)双重 身份验证
B)单个登录 (SSO)
C)用户 自助服务
D)元定向
答案:C
解析:

50.[单选题]哪种与捆绑电缆线路相关的射频干扰 (RFI)现象会造成信息泄漏?
Which Radio Frequency Interference (RFI)phenomenon associated with bundled cable runs can create information leakage?
A)隐蔽通道
Covert channel
B)串扰
Cross-talk
C)流血
Bleeding
D)Transference
答案:B
解析:

51.[单选题]An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is应用程序开发