CISSP考试练习(习题卷4)

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]以下哪一个是处理事件的基本目标?
A)恢复受影响系统的控制
B)没收嫌疑犯的 电脑
C)起诉 攻击者
D)执行系统的完整备份
答案:A
解析:

2.[单选题]下一个不是使用数据存储能力控制能力的数据？
A)清除
B)、打标
C)处理
D)存储
答案:A
解析: Handling - 如何传输/在什么控制下
Storage - 存储位置和方式
Marking - 如何标记媒体

3.[单选题]两家公司希望在供应商和客户关系中共享电子库存和订单。
什么是对他们最好的安全解决方案?
A)为两家公司编写服务级别协议 (SLA)。
B)建立虚拟专用网络 (VPN) 是两家公司的补间 。
C)在两家公司的周边配置防火墙 。
D)在两家公司之间建立文件传输协议 (FTP) 连接 。
答案:B
解析:

4.[单选题]以下哪项是系统工程生命周期(SELC)的技术过程?
Which of the following are Systems Engineering Life Cycle (SELC)Technical Processes?
A)概念、发展、生产、利用,支持,退役
Concept, Development, Production, Utilization, Support, Retirement
B)利益相关者需求定义、架构设计、实施、验证、运营
Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
C)采集、测量、配置管理、生产、运营、支持
Acquisition, Measurement, Configuration Management, Production, Operation, Support
D)概念、要求、设计、实施、生产、维护、支持、处置
Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal
答案:B
解析:

5.[单选题]以下哪一项规定了执行工作功能所需的最低特权集,并将用户限制在具有所需特权的域?
A)基于规则的访问
B)基于用户角色的访问
C)由系统确定的访问权限

D)基于数据敏感性的访问
答案:B
解析:

6.[单选题]The quality assurance (QA) department is short-staffed and is unable to test all modules before the anticipated release date of an application. What security control is MOST likely to be violated? 质量保证（QA）部门人员不足，无法在应用程序的预期发布日期之前测试所有模块。最有可能违反的安全控制是什么?
A)Separation of environments环境分离
B)Program management计划管理
C)Mobile code controls移动代码控件
D)Change management变更管理
答案:D
解析:

7.[单选题]在DRP计划中， 系统恢复在那个阶段启动
A)评估恢复现场
B)评估灾难损失以后
C)正式宣告灾难以后
D)灾难发生之后
答案:C
解析:略
章节：模拟考试202201

8.[单选题]在与其他组织共享或提供给其他组织时,谁负责保护信息?
A)系统所有者
B)授权官员 (AO)
C)信息 所有者
D)保安人员
答案:C
解析:

9.[单选题]当Jim 进入其组织的数据中心时,他必须使用智能卡和密码进入,先通过第一组门,接着第一组门关闭,然后他必须再次使用他的卡通过第二组门。这是什么类型的控制,它叫什么?
A)物理控制;单向活板门
B)逻辑控制;双刷卡授权
C)指令控制;单向通道走廊
D)预防性访问控制;陷门
答案:D
解析:一个陷门会使用两组门,其中一次只能打开一次。陷门是一种预防性访问控制,尽管是通过物理控制来实现的。
A mantrap uses two sets of doors, only one of which can open at a time. A mantrap is a type of preventive access control, although its implementation is a
Physical control.

10.[单选题]为客户提供了访问控制后,Ben收到一个投诉,有人在他的咖啡馆窃听其他客户的网络流量,包括用户名和密码。这是如何做到的?
A)密码由所有用户共享,使得网络流量易受攻击
B)恶意用户在路由器上安装了木马
C)用户使用ARP欺骗了路由器,使所有流量广播到所有用户
D)开放网络未加密,使得网络流量很容易被嗅探
答案:D

解析:未加密的开放网络以明文方式广播流量,这意味着可使用数据包嗅探器轻松地捕获到未加密的网站会话,FireSheep等工具专门用于捕获知名网站的会话。目前许多网站都默认使用TLS(安全传输层协议),但一些网站仍然直接发送用户的会话信息,而不进行加密处理。共享密码不是导致漏洞的原因,ARP(地址协议)欺骗与无线网络无关,并且木马是伪装成安全软件的恶意程序,它的攻击目标并不是路由器。
Unencrypted open networks broadcast traffic in the clear. This means that unencrypted sessions to websites can be easily captured with a packet sniffer. Some tools like FireSheep have been specifically designed to capture sessions from popular websites.

11.[单选题]在以下哪项程序中包含安全过程数据的收集是最重要的?
A)季度访问审查
B)安全持续监控
C)业务连续性测试
D)年度安全培训
答案:B
解析:

12.[单选题]什么类型的信息用于形成专家系统决策过程的基础?
A)一系列加权分层计算
B)来自多个人类专家的综合输入,根据过去的表现加权
C)知识库中编码的一系列“如果/那么”规则
D)模拟人类思维推理过程的生物决策过程
答案:C
解析:

13.[单选题]Digital certificates used in Transport Layer Security (TLS) support which of the following?
传输层安全（TLS）中使用的数字证书支持以下哪项?
A)Information input validation信息输入验证
B)Non-repudiation controls and data encryption不可否认性控制和数据加密
C)Multi-Factor Authentication（MFA）多因素身份验证（MFA）
D)Server identity and data confidentially服务器标识和数据保密
答案:D
解析:

14.[单选题]什么攻击技术经常被高级持续威胁组织利用,但其他攻击者(例如脚本小子和黑客行动主义者)不常用?
A)零日漏洞利用
B)社会工程学
C)特洛伊木马
D)SQL注入
答案:A
解析:尽管高级持续威胁 (APT) 可能会利用这些攻击中的任何一种,但由于发现或购买它们所需的研究成本和复杂性,它们与零日攻击最密切相关。 许多不同类型的攻击者经常尝试社会工程、特洛伊木马(和其他恶意软件)和 SQL 注入攻击。

15.[单选题]CA 证书管理的第二个阶段是?
A)创建
B)分发
C)使用
D)注销
答案:B
解析:略
章节：模拟考试202201

16.[单选题]Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages? 哪种算法的安全性来自于在有限域中计算离散对数的困难，并用于分发密钥，但不能用于加密或解密消息？
A)Diffie-Hellman密钥交换
B)Digital Signature Algorithm（DSA）数字签名算法（DSA）
C)Rivest-Shamir-Adleman（RSA）
D)Kerbero协议
答案:C
解析:

17.[单选题]以下关于软件测试方法的有什么是正确的？
A)自底向上方法错误可以较早地检测到接口
B)自顶方法可以较早地检测到关键模块中的错误
C)测试计划和结果应作为系统的永久文档的一部分被保留下来
D)黑盒测试是程序细节的严格检查为基础的
答案:C
解析:

18.[单选题]评估账户管理实践时应如何产生样本?
A)他们应该由管理员生成
B)账户应该在过去180内被验证
C)抽样应随机进行
D)抽样的做法是无效的,应该审计所有账户
答案:C
解析:抽样应随机进行,以避免人为偏差。选项B的做法可能会遗漏历史问题或仅考虑当前管理者的行为。如果对一个大样本进行真正的随机抽样,那么抽样得出的小样本将很具有代表性,能较好地覆盖用户群体。Sampling should be done randomly to avoid human bias. Choosing a timeframe may miss historic issues or only account for the current administrator' s processes.Sampling is an effective process if it is done on a truly random sample of sufficient size to provide
Effective coverage of the userbase.

19.[单选题]The three PRIMARY requirements for a penetration test are渗透测试的三个主要要求是
A)A defined goal, limited time period, and approval of management明确的目标、有限的时间段和管理层的批准
B)A general objective, unlimited time, and approval of the network administrator一般目标、无限时间和网络管理员的批准
C)An objective statement, disclosed methodology, and fixed cost客观陈述、披露的方法和固定成本
D)A stated objective, liability waiver, and disclosed methodology声明的目标、责任免除和披露的方法
答案:A
解析:

20.[单选题](04038) Which of the following describes the relationship between tolerance to interruption of a business process and the expression of value or cost in risk analysis? 下列哪项描述了业务流程中断的容忍度和风险分析中表达的价值或成本之间的关系？
A)A high tolerance is directly related to the high cost of the hardware and software.对中断的高容忍度与软硬件的高成本直接相关
B)A high tolerance is directly related to the high cost of the hardware and software.对中断的高容忍度与软硬件的高成本直接相关
C)A high tolerance is directly related to the high cost of the hardware and software.对中断的高容忍度与软硬件的高成本直接相关
D)A high tolerance is directly related to the high cost of the hardware and software.对中断的高容忍度与

软硬件的高成本直接相关
答案:C
解析:

21.[单选题]which of the following is a benefit of audit trails?下面哪个是审计轨迹的好处?
A)Accountability可问责性
B)Confidentiality机密性
C)Non-repudiation抗抵赖性
D)Integrity 完整性
答案:A
解析:

22.[单选题]什么可以定义为一个枚举数据证书的数据结构，在到期之前就被发行者吊销并向CA进行申报？
A)不受信证书列表
B)机构吊销列表
C)证书吊销树
D)证书吊销列表
答案:B
解析:

23.[单选题]两个存储设备之间通信防止攻击的方式是：
A)链路加密
B)防火墙
C)IPS
D)IDS
答案:A
解析:

24.[单选题]Greg希望控制对整个组织中用作销售点终端的iPad的访问。 他应该使用以下哪种方法来允许对共享环境中的设备进行逻辑访问控制?
Greg wants to control access to iPads used throughout his organization as point-of-sale terminals. Which of the following methods should he use to allow logical access control for the devices in a shared environment?
A)为所有销售点终端使用共享PIN以使其更易于使用
Use a shared PIN for all point-of-sale terminals to make them easier to use.
B)使用OAuth允许每个用户进行云登录
Use OAuth to allow cloud logins for each user.
C)为每个用户分配的iPad配置一个唯一的PIN
Issue a unique PIN to each user for the iPad they are issued.
D)使用Active Directory,同时用户帐户使用AD用户ID和密码登录iPad。
Use Active Directory and user accounts for logins to the iPads using the AD userID and password.
答案:D
解析:使用类似Active Directory的企业身份验证系统要求个人使用其凭据登录,这样可以在出现问题时确定谁已登录,并且还能让Greg快速轻松地删除终止或切换角色的用户。使用共享PIN 不提供任何责任,而为每个专门iPad的每个用户分配唯一PIN就意味着其他人将无法登录。 OAuth本身并不能提供Greg需要的服务和功能--它是一种授权服务,而不是一种身份验证服务。

25.[单选题]The BEST method to mitigate the risk of a dictionary attack on a system is to减轻系统字典攻击风险的最佳方法是
A)Use a hardware token. 使用硬件令牌。
B)Use complex passphrases. 使用复杂的密码短语。

C)Implement password history. 实现密码历史记录。
D)Encrypt the access control list（ACL）加密访问控制列表（ACL）
答案:A
解析:

26.[单选题]Susan想整合她的网站,以允许用户使用Google等网站的账户。她应该采用什么技术?
A)Kerberos
B)LDAP
C)OpenlD
D)SESAME
答案:C
解析:OpenID 是一个广泛支持的标准,允许用户使用单个账户登录多个网站,Google 账户经常与 OpenID一起使用。
OpenID is a widely supported standard that allows a user to use a single account to log into multiple sites, and Google accounts are frequently used with OpenlD.

27.[单选题]In a High Availability（HA）environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network? 在高可用性（HA）环境中，将虚拟路由器地址用作网络网关的主要目标是什么?
A)The second of two routers can periodically check in to make sure that the first router is operational. 两个路由器中的第二个可以定期检入，以确保第一个路由器可以运行。
B)The second of two routers can better absorb a Denial of Service（DoS）attack knowing the first router is present. 在知道第一个路由器存在的情况下，两个路由器中的第二个可以更好地吸收拒绝服务（DoS）攻击。
C)The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly. 两台路由器中的第一台出现故障并重新安装，而第二台则能完美地处理流量。
D)The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly. 两个路由器中的第一个可以更好地处理特定流量，而第二个可以无缝地处理其余流量。
答案:C
解析:

28.[单选题]哪一项不是DSL的标准类型?
A)HDSL
B)FDSL
C)ADSL
D)VDSL
答案:B
解析: The correct answer is FDSL FDSL does not exist.

29.[单选题](04170) 渗透测试中，攻击人不清楚信息，管理员知道信息的，属于:
A)针对性测试
B)针对性测试
C)针对性测试
D)针对性测试
答案:B
解析:

30.[单选题]是否必须向监管部门报告所有数据违规?
A)组织的道德规范不一定要求必须报告
B)只有产生重要影响的违规才需要报告
C)评估不同的司法管辖有不同的要求
D)如果数据是加密的,就不需要报告
答案:C

解析:略
章节：模拟考试202201

31.[单选题]安全从业者的任务是保护组织的无线接入点 (WAP)。其中哪一种是将此环境限制在授权用户的最有效方法?
A)启用无线接入点上的 Wi-Fi 受保护访问 2 (WPA2) 加密
B)禁用服务集标识符 (SSID)名称的广播
C)将服务集标识符 (SSID)的名称更改为与组织无关的随机值
D)基于媒体访问控制 (MAC)地址创建访问控制列表 (ACL)
答案:D
解析:

32.[单选题]与个人医疗保健在过去、现在或将来的付款有关的数据是每个HIPAA的什么类型的数据?
A)PCI
B)个人计费数据
C)PHI
D)个人身份信息(PII)
答案:C
解析:个人健康信息(PHI)由HIPAA 定义,包括个人医疗账单的信息。PCI是支付卡行业的安全标准,但仅适用于信用卡。PII 是个人可识别信息的广义术语,个人计费数据不是广泛使用的专业术语。
Personal Health Information (PHI) is specifically defined by HIPAA to include information about an individual's medical bills. PCI could refer to the payment card industry's security standard but would only apply in relation to credit cards. PII ís a broadly defined term for personally identifiable information, and personal billing data isn't a broadly used industry term.

33.[单选题]An advantage of link encryption in a communications network is that it
A)improves the efficiency of the transmission.
B)encrypts all information, including headers and routing information.
C)makes key management and distribution easier.
D)protects data from start to finish through the entire network.
答案:B
解析:

34.[单选题]以下哪项最贴合Sean的团队成员关于防火墙配置问题的描述?
A)清理规则,隐形规则
B)隐形规则,沉默规则
C)沉默规则,否定规则
D)隐形规则,否定规则
答案:C
解析:C。下面描述了不同类型的防火墙规则:沉默规则不记录“噪杂"流量便放弃它。不对不重要的数据包作出响应,减小了日志规模隐形规则不允许未经授权的系统访问防火墙软件。清理规则规则库中的最后一条规则,放弃并且记录任何不符合前述规则的流量。否定规则用来代替广泛允许的"任何规则”。否定规则规定什么系统能够被访问和如何访问,对权限控制较紧。

35.[单选题]Mike 正在构建容错服务器并希望实施RAID1,实施此方案需要多少个物理磁盘?
A)1
B)2
C)3
D)5
答案:B
解析:RAID 1 称为磁盘镜像,需要两个物理磁盘,其中一个物理磁盘是另一个的副本。
RAID 1,disk mirroring,requires two physical disks that will contain copies of the same data.

36.[单选题]对于考虑安全网络访问的双重身份验证的组织,以下哪一项最安全?
A)挑战响应和私 钥
B)数字证书和 单一登录 (SSO)
C)令牌和 密码
D)S市场卡和生物计
答案:D
解析:

37.[单选题]Why is authentication by ownership stronger than authentication by knowledge? 为什么所有权认证比知识认证更强大?
A)It is easler to change. 更容易改变。
B)It can be kept on the user’s person. 它可以保存在用户的个人身上。
C)It is more difficult to duplicate. 这更难复制。
D)It is simpler to control. 它更易于控制。
答案:B
解析:

38.[单选题]What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability? 什么样的过程有助于平衡保护措施的运营和经济成本与任务能力的提高?
A)Risk assessment风险评估
B)Performance testing性能测试
C)Security audit安全审计
D)Risk management风险管理
答案:D
解析:

39.[单选题]以下哪一项是用于限制不同执行域内给定主体可用的对象范围的主要机制?
Which of the following is the PRIMARY mechanism used to limit the range of objects availableto a given subject within different execution domains?
A)使用离散分层和应用程序编程接口 (API)
Use of discrete layering and Application Programming Interfaces (API)
B)数据隐藏和抽象
Data hiding and abstraction
C)进程隔离
Process isolation
D)虚拟专用网 (VPN)
Virtual Private Network(VPN)、
答案:A
解析:

40.[单选题]组织的应急响应指南应包括以下哪个组成部分?
A)第一反应者的备选反应程序
B)长期业务连续性协议
C)组织冷站点的活动程序
D)订购设备的联系信息
答案:A
解析:应急响应指南应包括一个组织应对紧急情况应采取的立即步骤。这些包括立即响应程序、紧急事件需通知的人员名单和这些人员的后续行动流程。应急响应指南不包括长期操作,例如激活业务连续性协议、订购设备或激活灾难恢复站点。
The emergency response guidelines should include the immediate steps an organization should follow in

response to an emergency situation. These include immediate response procedures, a list of individuals Who should be notified of the emergency, and secondary response procedures for first responders.

41.[单选题]Valerie需要控制对部署在BYOD环境中的移动设备上的应用程序的访问。哪种类型的解决方案最能让她控制应用程序,同时确保它们不会在最终用户使用的设备上留下残余数据?
Valerie needs to control access to applications that are deployed to mobile devices in a BYOD environment. What type of solution will best allow her to exercise control over the applications while ensuring that they do not leave remnant data on the devices used by her end users?
A)将应用程序部署到BYOD设备,并要求每个设备上都有唯一的PIN
Deploy the applications to the BYOD devices and require unique PINs on every device.
B)将应用程序部署到桌面系统,并要求用户使用远程桌面通过企业身份验证进行访问
Deploy the application to desktop systems and require users to use remote desktop to access them using enterprise authentication.
C)使用应用程序容器将应用程序部署到BYOD设备,并要求每个设备上都有唯一的PIN
Deploy the applications to the BYOD devices using application containers and require unique PINs on every device.
D)使用需要用企业凭据进行身份验证的虚拟托管应用程序环境
Use a virtual hosted application environment that requires authentication using enterprise credentials.
答案:D
解析:当需要非常高级别的控制或端点设备不可信时,使用具有远程连接和企业身份验证的集中式环境可以提供适当的安全性。

42.[单选题]在软件开发生命周期的哪一阶段通常设计安全和访问控制?
A)编码阶段
B)产品设计阶段
C)软件部署和要求阶段
D)详细设计阶段
答案:D
解析:

43.[单选题]下一项哪被用于数据库信息以隐藏信息安全?
A)继承
B)多实例
C)多性态
D)很
答案:B
解析: 多实例化表示一种环境，其特征是信息存储在
比数据库中的一个位置多于一个位置。这允许具有多级
查看和授权的安全模型。多实例化当前的问题是确保数据库中信息的完整性
。如果没有有效的方法来同时
更新所有出现的相同数据元素 - 无法保证完整性

44.[单选题]A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is一个全球性组织希望实现硬件令牌，作为远程访问多因素身份验证解决方案的一部分。此实现的主要优点是
A)the scalability of token enrollment. 令牌注册的可扩展性。
B)increased accountability of end users. 加强最终用户的问责制。
C)it protects against unauthorized access. 它可以防止未经授权的访问。
D)it simplifies user access administration. 它简化了用户访问管理。
答案:C
解析:

45.[单选题]What is a common mistake in records retention? 记录保留中的常见错误是什么?
A)Having the organization legal department create a retention policy让组织法律部门创建保留策略
B)Adopting a retention policy based on applicable organization requirements根据适用的组织要求采用保留策略
C)Having the Human Resource (HR) department create a retention policy让人力资源（HR）部门制定保留政策
D)Adopting a retention policy with the longest requirement period采用要求期限最长的保留策略
答案:C
解析:

46.[单选题]为实现组织的国际化,Jim正在确定组织的审计标准,以下哪项不是他们应该使用的IT 标准?
Jim is helping his organization decide on audit standards for use throughout their international organization. Which of the following is not an IT standard that Jim's organization is likely to use as part of its audits?
A)COBIT
COBIT
B)SSAE-18
SSAE-18
C)ITIL
ITIL
D)ISO27001
ISO 27001
答案:C
解析:ITIL最初代表了IT基础设施库,是一套用于IT服务管理的方法,通常不用于审计。COBIT(信息系统和技术控制目标)、ISO 27001和SSAE-18(鉴证业务准则公告第18号)都用于审计。

47.[单选题]Kathleen 工作的公司已将大多数员工转移到远程工作， 并希望确保他们用于语音. 视频和基于文本的协作的多媒体协作平台是安全的。 以下哪些安全选项将提供最佳用户体验， 同时为通信提供适当的安全性？
A)Require software-based VPN to the corporate network for all use of the Collaboration platform.
需要基于软件的 VPN 连接到企业网络， 以便协作平台的所有使用。
B)Require the use of SIPS and SRTP for all communications.
要求对所有通信使用 SIPS 和 SRTP。
C)Use TLS for all traffic for the collaboration platform.
对协作平台的所有流量使用 TLS。
D)Deploy secure VPN endpoints to each remote location and use a point-to-point VPN for communications.
将安全 VPN 端点部署到每个远程位置， 并使用点对点 VPN 进行通信。
答案:C
解析:略
章节：模拟考试202201

48.[单选题]Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution? 在使用虚拟专用网络（VPN）解决方案时，下列哪项活动会给组织带来重大的安全风险？
A)VPN bandwidth VPN带宽
B)Simultaneous connection to other networks同时连接到其他网络
C)Users with Internet Protocol (IP) addressing conflicts具有Internet协议（IP）寻址冲突的用户
D)Remote users with administrative rights具有管理权限的远程用户
答案:B
解析: