CISSP考试练习(习题卷11)

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]Tactical security plans are BEST used to:战术级安全计划是最适合用来:
A)Establish high-level security policies建立高层次的安全策略
B)Enable enterprise entity-wide security management执行企业/单位范围内安全管理
C)Reduce downtime减少停机时间
D)Deploy new security technology部署新的安全技术
答案:D
解析:

2.[单选题]当基于安全经理对以下哪项理解时，信息安全度量对管理提供了最大的价值?
A)安全漏洞的可能性
B)信息资产价值
C)实施有效控制的成本
D)与定量分析师相关的好处
答案:B
解析:

3.[单选题]下列哪一项不是数据隐藏的例子?
A)防止授权的课题阅读者删除客体
B)防止未经授权的访问者访问数据库
C)限制较低分类级别的主体访问较高分类级别的数据
D)组织应用程序直接访问硬件
答案:A
解析:

4.[单选题]Travis 担心为系统提供服务的 Microsoft 的 BitLocker 的安全性。 如果系统配备了 TPM 并使用全盘加密,那么基于驱动器加密状态的系统何时最安全,不会丢失数据?
A)当它们启动并运行时,因为系统会监视驱动器访问
B)当系统因密钥从内存中删除而关闭时
C)当他们因为 TPM 检查安全启动过程而启动时
D)当它们因驱动器完全加密而关闭时
答案:D
解析:当系统关闭且驱动器已加密且不处于可读状态时,驱动器上的文件最安全。 BitLocker 在使用时根据需要解密文件,
这意味着在系统启动后的任何时间都可以访问文件,尤其是在用户登录并可以访问系统或恶意软件正在运行的情况下。

5.[单选题]以下哪一项对审核员在审查系统配置时的最大帮助?
A)更改管理 流程
B)用户管理 程序
C)操作系统 (OS) 基线
D)系统 m备份 文档
答案:A
解析:

6.[单选题]以下哪项最能描述组织内直接负责数据的角色?

A)数据保管人
B)信息所有者
C)数据库管理员
D)质控
答案:A
解析:

7.[单选题]Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges? 以下哪项提供了执行作业功能所需的最低权限集，并将用户限制到具有所需权限的域？
A)Access based on rules基于规则的访问
B)Access based on user's role基于用户角色的访问
C)Access determined by the system由系统确定的访问权限
D)Access based on data sensitivity基于数据敏感性的访问
答案:B
解析:

8.[单选题]The overall goal of a penetration test is to determine a system's渗透测试的总体目标是确定系统的
A)ability to withstand an attack. 抵御攻击的能力。
B)capacity management. 容量管理。
C)error recovery capabilities. 错误恢复功能。
D)reliability under stress. 压力下的可靠性。
答案:A
解析:

9.[单选题]在传输控制协议/互联网协议 (TCP/IP) 堆栈中,哪个层负责与另一个节点进行谈判和建立连接?
A)运输层
B)应用 层
C)网络层
D)会话层
答案:A
解析:

10.[单选题]下列哪项代表了最好的编程方式
A)低内聚，低耦合
B)高内聚，高耦合
C)高内聚，低耦合
D)低内聚，高耦合
答案:C
解析: The best programming uses the most cohesive modules possible, but because different modules need to pass data and communicate, they usually cannot be totally cohesive. Also, the lower the coupling, the better the software design, because it promotes module independence. The more independent a component is, the less complex the application is and the easier it is to modify and troubleshoot

11.[单选题]The personal laptop of an organization executive is stolen from the office, complete with personnel and project records. Which of the following should be done FIRST to mitigate future occurrences? 一位组织高管的个人笔记本电脑从办公室被盗，里面有完整的人事和项目记录。为了缓解未来的事故，应首先执行以下哪项操作？
A)Encrypt disks on persional laptops. 加密个人笔记本电脑上的磁盘。
B)Issue cable locks for use on personal laptops. 为个人笔记本电脑提供电缆锁。

C)Create policies addressing critical information on personal laptops. 创建解决个人笔记本电脑上关键信息的策略。
D)Monitor personal laptops for critical information. 监控个人笔记本电脑中的关键信息。
答案:A
解析:

12.[单选题]Database software should meet the AClD test requirements. Why should atomic transactions, one of the ACID testrequirements, be performed when using online transaction processing or TP?
数据库软件应当满足ACID测试的要求,在使用联机事务处理OITP时,为什么应当执行ACID测试要求之一的原子性事务?
A)Establish integrity rules as specified in the database security policy
建立数据库安全策略中所规定的完整性规则
B)So that the database performs transactions as a single unit without interruption.
数据库作为一个单元来执行事务,而不会中断
C)To ensure that a rollback does not occur.
来确保回滚不会发生
D)To prevent concurrent processes from interacting with each other.
来防止同时进行的事务进程之间的相互干扰
答案:B
解析:

13.[单选题]As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem? 作为设计原则，以下哪一个参与者负责确定和批准云生态系统中的数据安全需求？
A)Cloud broker云代理
B)Cloud provider云提供商
C)Cloud consumer云消费者
D)Cloud auditor云审计者
答案:C
解析:

14.[单选题]数据库视图用于什么?
A)为了确保引用的完整性
B)为了允许在数据库中更容易访问数据
C)为了在数据库中限制用户访问数据
D)为了提供审计跟踪
答案:C
解析:

15.[单选题]在遵循变更管理计划中定义的流程后,超级用户升级了信息系统中的设备。
将采取什么步骤来确保升级不会影响网络安全态势?
A)进行评估和授权 (A&A)
B)进行安全影响分析
C)查看最近一次漏洞扫描的结果
D)使用基线配置进行差距分析
答案:B
解析:

16.[单选题]ln order for evidence to be legally admissible, it must be true, complete, sufficient and reliable.There is a reasonable relationship between evidence andfindings. Which property is it?为了让证据被合法采纳,证据必须是真实、完整、充分并可靠的。证据与发现的结果有一个合情合理的关系,指的是哪一个特性?
A)Complete完整

B)Reliable可靠
C)Authentic真实
D)Sufficient充分
答案:C
解析:

17.[单选题]如果FAR 和 FRR都 不能提供满足其组织需求所能接受的性能水平,应该怎么做?
A)调整生物识别设备的灵敏度。
B)评估其他生物识别系统以进行比较。
C)移动 CER。
D)在软件中调整 FRR 设置。
答案:B
解析:

18.[单选题]业务连续性计划(BCP)基于
A)一个。政策和程序手册。
B)来自类似组织的现有BCP。
C)审查业务流程和程序。
D)所需项目和目标的标准清单。
答案:C
解析:

19.[单选题]如果员工因违反组织的可接受使用政策(ALP)而被解雇,以下哪项是关键的?
A)适当的文件
B)Internet访问日志
C)代理记录
D)特权中止
答案:A
解析:

20.[单选题]为向所有相关方有效的传递安全战略,组织必须执行以下哪项?
Which of the following MUST an organization do to effectively communicate is security strategy to all affected parties?
A)让每个关键组织领域的代表都参与进来
Involve representatives from each key organizational area.
B)向董事会提供定期更新
Provide regular updates to the board of directors.
C)将战略变更告知员工
Notify staff of changes to the strategy.
D)消除潜在的沟通障碍
Remove potential communication barriers.
答案:C
解析:

21.[单选题]在采购新信息系统期间,确定系统规范中未涉及某些安全要求。以下哪一个是最可能的原因?
A)采购官缺乏技术 知识。
B)在采购过程中,安全要求发生了变化 。
C)供应商的投标团队中没有安全专业人员 。
D)对安全要求的描述 不够充分。
答案:D
解析:

22.[单选题]是一种在XML中实施的声明性访问控制第略语言和处理模型,它描述如何解释安全策略。是一种XML型框架,由OASIS开发,用来在合作组织之间交换用户、资源和服务供应信息。
A)服务供应标记语言(SPMIL),可扩展访问控法际记语言(XAGML)
B)可扩展访问控制标记语言(XACM气L),服务供应标记语言(SPML)
C)可扩展访问控制标记语言(XACML),安金断言标记语言(SAML)
D)安全断言标记语言(SAMML)。服务供应标记语言(SPML)
答案:B
解析:可扩展访问控制标记语言Extensile Access Control Markup Language,XACML)是一种在XML中实施的声明性访问腔M第略语言和处理慷型。描述如何解释安全策略。服务供膛际记语言(Service Provisioning Markup Language,SPMAL)是一种XMAL型框架,由OASIS 开发,用来在合作组织之间交换用广、资源和服务供应信息.

23.[单选题]以下哪一个在开放系统互连 (OSI)模型的网络层中运行?
A)数据包 过滤
B)端口服务 过滤
C)内容 筛选
D)应用程序访问 控制
答案:A
解析:

24.[单选题]A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected? 已对系统进行漏洞扫描，发现其中包含大量未经授权打开的通信端口。该系统可能会受到以下哪种情况的影响？
A)Trojan horse特洛伊木马
B)Denial of Service（DoS）拒绝服务（DoS）
C)Spoofing电子欺骗
D)Man-in-the-Middle（MITM）中间人（MITM）
答案:A
解析:

25.[单选题]敏感开发项目经理的角色：
A)选择好的开发语言
B)尽可能多的交付软件
C)保障项目管理
D)遵循项目开发计划
答案:B
解析:略
章节：模拟考试202201

26.[单选题]要在对称密钥加密法中确保双向通信安全，最少需要使用多少个密码密钥？
A)1个
B)2个
C)3个
D)4个
答案:A
解析:

27.[单选题]两种常见的数据分类方案是什么?
A)政府/军事分类方案和商业/私营部门分类方案
B)个人和政府

C)已私营部门和非限制性部门
D)已分类和未分类
答案:A
解析:军事(或政府)和私营部门(或商业)是两种常见的数据分类方案。

28.[单选题]加密适用于以下所有 OSI/ISO 层，除了：
A)网络层
B)物理层
C)会话层
D)数据链路层
答案:B
解析: The Physical Layer describes the physical properties of the various communications media,
As well as the electrical properties and interpretation of the exchanged signals. Ex: this layer
Defines the size of Ethernet coaxial cable, the type of BNC connector used, and the
Termination method. You cannot encrypt nothing at this layer because it's physical, it is not
Protocol / software based. Network, Data link and transport layer supports encryption

29.[单选题]Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches? 检查电子邮件上的路由信息以确定其格式有效且包含有效信息，这是以下哪种反垃圾邮件方法的一个示例？
A)Simple Mail Transfer Protocol（SMTP）blacklist简单邮件传输协议（SMTP）黑名单
B)Reverse Domain Name System（DNS）lookup反向域名系统（DNS）查找
C)Hashing algorithm哈希算法
D)Header analysis标题分析
答案:D
解析:

30.[单选题]当安全技术被恰当第执行和配置时，以下哪种攻击最可能是成功的？
A)逻辑攻击
B)物理攻击
C)社会工程学攻击
D)特洛伊木马攻击
答案:C
解析:

31.[单选题]以下哪种安全机制提供了限制特权程序执行的最佳方式?
A)基于角色的访问控制 (RBAC)
B)生物识别访问 控制
C)联合身份管理 (IDM)
D)应用 硬化
答案:A
解析:

32.[单选题]为什么异常检测智能检决策支持系统经常会产生大量的误报呢？
A)因为他们只能正确识别它们已知的攻击。
B)因为它们是基于应用程序的，更容易受到攻击。
C)因为他们不能识别异常行为。
D)由于用户和系统的正常行为模式变化很大。
答案:D
解析:

33.[单选题]A large bank deploys hardware tokens to all customers that use their online banking system. The token generates and displays a six digit numeric password every 60.seconds. The customers must log into their bank accounts using this numeric password. This is an example of大型银行向使用其网上银行系统的所有客户部署硬件代币。令牌每60生成并显示一个六位数的数字密码。秒。客户必须使用此数字密码登录其银行帐户。这是
A)asynchronous token. 异步令牌。
B)Single Sign-On（SSO）token. 单点登录（SSO）令牌。
C)single factor authentication token. 单因素身份验证令牌。
D)synchronous token. 同步令牌。
答案:D
解析:

34.[单选题]以下竞争情报攻击最好分类为性质类型的攻击?
A)商业攻击
B)知识攻击
C)财务攻击
D)恶意攻击
答案:A
解析: 既然我们说的是竞争情报攻击，我们可以将其归类为商业攻击，因为它正在扰乱商业活动。情报攻击是最
 最常
用于伤害公司的攻击之一，在其信息中伤害更大。

35.[单选题]When using Security Assertion markup language（SAML）, it is assumed that the principal subject当使用安全断言标记语言（SAML）时，假设主体
A)accepts persistent cookies from the system. 接受来自系统的持久cookie。
B)allows Secure Sockets Layer（SSL）for data exchanges. 允许安全套接字层（SSL）进行数据交换。
C)is on a system that supports remote authorization. 位于支持远程授权的系统上。
D)enrolls with at least one identity provider. 至少向一个身份提供程序注册。
答案:D
解析:

36.[单选题]将电子存储介质退回第三方进行维修时,有效做法是什么?
A)确保媒体不会以任何方式标记组织 名称。
B)拆卸介质并拆卸可能包含敏感 datA 的部件。
C)物理上破坏可能包含敏感数据的媒体部分。
D)与第三方签订关于安全处理 媒体的合同。
答案:D
解析:

37.[单选题]知识产权主要关注以下哪一项?
A)-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]一个谁定义的模型定义了一个约束的数据，完整的验证和?
A)授权模型
B)Biba鼻子模型
C)CIark Wilson 模特

D)Bell-LaPadula 人体模型
答案:C
解析:

39.[单选题]The use of proximity card to gain access to a building is an example of what type of security control? 使用接近卡进入建筑物是什么类型的安全控制的一个例子?
A)Legal合法
B)Logical必然
C)Physical物理的
D)Procedural程序
答案:C
解析:

40.[单选题]Jim 正在为他的组织实施IDaaS 解决方案。他使用了什么类型的技术?
A)身份即服务
B)员工ID作为服务
C)基于云的RADIUS
D)OAuth
答案:A
解析:身份即服务(IDaaS)使用身份管理平台来提供第三方服务。使用IDaas 包含以下这些优点:集成云服务、减少传统的内部身份系统的维护开销。然而,风险同样存在,因为用户身份管理由第三方控制,本地身份验证依赖于异地的基础设施,这些都可能引发安全问题。
Identity as a Service (IDaaS) provides an identity platform as a third-party service.This can provide benefits,indduding integration with ddoud services and removing overhead for maintenance of traditional on-premise identity systems, but can also create risk due to third-party control of identity services and reliance on an offsite identity infrastructure.

41.[单选题]ppp 解决了什么问题?
A)调制解调器的固有问题
B)解决了上网的网速和质量问题
C)解决了IP地址不足
D)解决了上网加密的问题
答案:B
解析:略
章节：模拟考试202201

42.[单选题]对于服务提供商来说,他关注最有效的哪一个程序可以有效解决使用云计算的客户的保密问题?
A)哈希函数
B)数据 隔离
C)文件系统 权限
D)非否定 控制
答案:B
解析:

43.[单选题]开放系统互连 (OSI)模型的哪个层增加了有关发件人和接收方之间逻辑连接的信息?
A)物理的
B)会期
C)运输
D)数据链接
答案:C
解析:

44.[单选题]加密和解密可发生在不同的操作系统、应用程序和网络协议枝的层面上。端到端力口密发生 内。 IPSec 发生在 层。 PPTP 加密发生在 层。链路加密发生在 层和 层。
A)应用程序、传输、数据链路、数据链路、物理
B)应用程序、传输、网络、数据链路、物理
C)应用程序、网络、数据链路、数据链路、物理
D)网络、传输、数据链路、数据链路、物理
答案:C
解析:端对端加密发生在应用程序内。 IPSec 加密发生在网络层。 PPTP 加密发生在数据链路层。链路加密发生在数据链路层和物理层。

45.[单选题]在考虑传输安全性时,以下哪一个考虑的影响最小?
A)网络 可用性
B)节点位置
C)网络 带宽
D)数据 完整性
答案:C
解析:

46.[单选题]什么原则要求只给用户完成工作所必需的权限?
A)聚合特权原则
B)最高特权原则
C)有效特权原则
D)最小特权原则
答案:D
解析:

47.[单选题]在为一个拟建的设施设计安全计划时,你被告知预算减少了30%。然而,他们没有调整或减少安全要求。内部和外部使用的最常见和最便宜的物理访问控制设备是什么?
A)照明
B)保安
C)键锁
D)棚栏
答案:C
解析:

48.[单选题]针对针对移动系统的恶意代码攻击最有效的反面方法是什么?
A)沙盒
B)更改控制
C)内存 管理
D)公钥基础设施 (PKI)
答案:A
解析:

49.[单选题]下列哪个是生物测定学系统的最关键的特征?
A)可接受性
B)准确性
C)吞吐量
D)可靠性
答案:B
解析:<p>We don't agree with the original answer, which was throughput. Granted throughput is vital

but Krutz lists accuracy is most important. In addition to the accuracy of the biometric systems, there are OTHER factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.

50.[单选题]Unused space in a disk cluster is important in media analysis because it may contain which of the following? 磁盘群集中未使用的空间在介质分析中很重要，因为它可能包含以下哪一项？
A)Residual data that has not been overwritten未被覆盖的剩余数据
B)Hidden viruses and Trojan horses隐藏的病毒和特洛伊木马
C)Information about the File Allocation table (FAT) 有关文件分配表 (FAT) 的信息
D)Information about patches and upgrades to the system有关系统修补程序和升级的信息
答案:A
解析:

51.[单选题]一家企业在其无线局域网 (WLAN) 拓扑中实施了符合标准的支付卡行业数据安全标准 (PCI-DSS) 手持式信用卡处理。网络团队将 WLAN 划分为使用防火墙控制设备访问和路由到互联网上的卡处理器的卡处理器的信用 c ard 处理专用段。PCI-DSS 范围内有哪些组件?
A)整个企业网络 基础设施。
B)手持设备、无线接入点和 border 网关。
C)终端设备、无线接入点、WLAN、交换机、管理控制台和 防火墙。
D)终端设备、无线接入点、WLAN、交换机、管理控制台和 互联网
答案:C
解析:

52.[单选题]SDN应用的什么层使用程序通过API来传达对资源的需求?
What layer of an SDN implementation uses programs to communicate needs for resources via APIs?
A)数据平面
The data plane
B)控制平面
The control plane
C)应用平面
The application plane
D)监控平面
The monitoring plane
答案:C
解析:软件定义网络(SDN)的应用平面是应用程序运行的地方,这些应用程序使用应用编程接口 (API)与SDN就所需资源进行通信。控制平面接收指令并将其发送到网络。最后一个公共平面是设备本身。
The application plane of a software-defined network (SDN) is where applications run that use application programming interfaces (APIs) to communicate with the SDN about needed resources. The control plane receives instructions and sends them to the network. The last common plane is the devices themselves.

53.[单选题]编写在Visual Basic应用程序语言(VBA)中的宏病毒是一个主要的问题，因为
A)软盘可以传播这样的病毒
B)这些病毒可以感染许多类型的环境
C)防毒软件可用来删除病毒代码
D)这些病毒几乎只影响到操作系统
答案:D
解析: VBA is typically Windows OS base, so Unlikely many types of environments, but impact the OS(need a real reference source to justify this though).

54.[单选题]Who would be the BEST person to approve an organizations information security policy? 谁是批准组织信息安全策略的最佳人选？