CISSP考试练习(习题卷1)

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]为什么必须很好地保护 Kerberos 服务器免受未经授权的访问?
A)我不包含所有客户的密钥 。
B)它始终以根本 特权运作。
C)它包含所有服务的门票 。
D)它包含所有网络实体的互联网协议 (IP) 地址 。
答案:A
解析:

2.[单选题]Data backup verification efforts should:数据备份验证工作应该:
A)Have the smallest scope possible.尽可能有最小的范围
B)Be based on the threats to the organization.基于组织面临的各种威胁
C)Maximize impact on business.最大化对业务的影响
D)Focus on user data.关注用户数据
答案:B
解析:

3.[单选题]审计期间将收集的数据量主要由
A)审计范围。
B)审计师的经验 水平。
C)数据A的可用性。
D)数据的完整性。
答案:A
解析:

4.[单选题]可能造成的事件或事件的系统或网络造成的损害称为
A)劣势
B)威胁代理
C)威胁
D)漏洞
答案:C
解析: 可能对信息系统或
网络造成危害的事件或活动。

5.[单选题]As a security manger which of the following is the MOST effective practice for providing value to an organization? 作为安全经理，以下哪项是为组织提供价值的最有效实践？
A)Assess business risk and apply security resources accordingly. 评估业务风险并相应地应用安全资源。
B)Coordinate security implementations with internal audit. 协调安全实施与内部审计。
C)Achieve compliance regardless of related technical issues实现法规遵从性，而不考虑相关的技术问题
D)Identify confidential information and protect it. 识别机密信息并加以保护。
答案:D
解析:

6.[单选题]什么类型的恶意软件专门用于利用窃取的计算能力为攻击者谋取经济利益?
What type of malicious software is specifically used to leverage stolen computing power for the

attacker’s financial gain?
A)RAT
B)PUP
C)Cryptomalware
D)Worm
答案:C
解析:尽管任何恶意软件都可能被用来获取经济利益,但取决于其有效负载,加密恶意软件是专门为此目的而设计的。 它窃取计算能力并用它来挖掘加密货币。 远程访问木马 (RAT) 旨在授予攻击者对系统的远程管理访问权限。 潜在有害程序 (PUP) 是任何类型的软件,最初由用户批准,但随后执行了不受欢迎的操作。 蠕虫是恶意代码对象,它们靠自己的力量在系统之间移动。

7.[单选题]文件传输协议 (FTP) 的安全限制是以下哪一个?
A)被动FTP与网络浏览器不兼容。
B)允许匿名访问 。
C)FTP 使用传输 控制协议 (TCP) 端口 20 和 21。
D)身份验证不 加密。
答案:D
解析:

8.[单选题](04004) Which of the following is considered best practice for a forensic investigation?下面哪个被认为是取证调查的最佳实践?
A)Examine a copy of the information collected检查收集的信息的副本
B)Examine a copy of the information collected检查收集的信息的副本
C)Examine a copy of the information collected检查收集的信息的副本
D)Examine a copy of the information collected检查收集的信息的副本
答案:C
解析:

9.[单选题]根据最近关于移动代码和 Web 应用程序风险的文章,您希望调整组织端点设备的安全配置以最大程度地减少风险。 在装有最新版 Microsoft 浏览器且所有其他浏览器均已禁用或阻止的现代 Windows 系统上,以下哪一项最受关注?
A)Java
B)Flash
C)JavaScript
D)ActiveX
答案:C
解析:

10.[单选题]故障容差的主要目标是什么?
A)消除单一故障点
B)使用沙盒进行隔离
C)单点 维修
D)防止传播的遏制
答案:A
解析:

11.[单选题]若当事人没有共享的秘密以及必须传递的大量敏感信息，传送信息的最有效的方法就是使用混合 加密方法。这是什么意思?
A)在收件人私钥的基础上，使用收件人公钥来进行加密和解密。
B)使用硬件加密加速器辅助软件加密。
C)使用公钥加密来保护密钥，以及使用该密钥进行 信息加密。

D)使用椭圆曲线加密。
答案:C
解析: A Public Key is also known as an asymmetric algorithm and the use of a secret key would be a symmetric algorithm.

12.[单选题]When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production? 在开发面向外部的基于web的系统时，在实施和生产之前，以下哪项是安全评估的主要重点？
A)Assessing the Uniform Resource Locator（URL）评估统一资源定位器（URL）
B)Ensuring Secure Sockets Layer（SSL）certificates are signed by a certificate authority确保安全套接字层（SSL）证书由证书颁发机构签名
C)Ensuring that input validation is enforced确保实施输入验证
D)Ensuring Secure Sockets Layer（SSL）certificates are internally signed确保对安全套接字层（SSL）证书进行内部签名
答案:B
解析:

13.[单选题]在考虑业务连续性 (BC)和灾难恢复 (DR) 培训计划的有效性时,最重要的元素是什么?
A)管理 支持
B)考虑组织 需要
C)用于交付的技术
D)目标 受众
答案:B
解析:

14.[单选题]As per the Orange Book, what are two types of system assurance?
根据橙皮书,系统保证的两种类型是?
A)Design Assurance and Implementation Assurance.设计保证和实施保证
B)Architectural Assurance and Implementation Assurance.架构保证和实施保证
C)Operational Assurance and Life-Cycle Assurance.操作保证和生命周期保证
D)Operational Assurance and Architectural Assurance.操作保证和架构保证
答案:C
解析:

15.[单选题]以下 哪一 个是针对加密硬件模块的最有效攻击?
A)明文
B)蛮 力
C)电源分析
D)中间人 (MITM)
答案:C
解析:

16.[单选题]following is the best description of the virtual directory? Bran被要求在公司的新的身份管理系统的虚拟目录下工作;下面哪个是关于虚拟目录的最佳的描述?
A)Meta directory元目录
B)User attribute information stored in an HR database.存储在HR数据库中的用户属性信息
C)Virtual container for data from multiple sources.装载多个来源的数据的虚拟容器
D)Allow administrators to configure and manage how to conduct identity management services.允许管理员配置和管理如何进行身份管理
答案:C
解析:

17.[单选题]以下哪种方法是验证软件修补程序完整性的最佳方法?
A)加密 检查
B)版本 编号
C)自动 更新
D)供应商保证
答案:A
解析:

18.[单选题]哪种技术是在联合身份解决方案中填充基于云的目录的先决条件?
Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?
A)通知工具
Notification tool
B)安全令牌工具
Security token tool
C)同步工具
Synchronization tool
D)消息队列工具
Message queuing tool
答案:B
解析:

19.[单选题]封装安全载荷ESP 能提供?
A)可用性与完整性
B)完整性与机密性
C)授权利完整行
D)授权和机密性
答案:B
解析:略
章节：模拟考试202201

20.[单选题]以下哪一种灭火系统的意外风险最天,有可能会损坏数据中心的设备?
A)闭式系统
B)于燥管道
C)喷水
D)预处理系统
答案:A
解析:干燥管道,喷水和预处理系统使用的管道在正常情况下是空的,一旦检测到火灾迹象,管道才死满水。闭式系统使用的管道-直充满水,如果管道损坏。可能会极坏设备。

21.[单选题]A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.Why did the network architect likely design the VoIP system with gratuitous ARP disabled? 实施后审查发现，互联网语音协议（VoIP）系统设计为禁用免费地址解析协议（ARP）。为什么网络架构师可能会设计禁用免费ARP的VoIP系统?
A)Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1. 免费ARP要求使用虚拟局域网（VLAN）1。
B)Gratuitous ARP requires the use of insecure layer 3.protocols. 免费ARP要求使用不安全的第3层。协议。
C)Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone. 免费ARP要求在手机上成功进行暴力攻击的可能性。

D)Gratuitous ARP requires the risk of a Man-in-the-Middle（MITM）attack. 无偿ARP要求有中间人（MITM）攻击的风险。
答案:D
解析:

22.[单选题]您网络中的某些用户在使用 Kerberos 服务器进行身份验证时遇到问题。在对问题进行故障排除时,您确认可以登录到您的常规工作计算机。 但是,您无法使用您的凭据登录到用户的计算机。 以下哪项最有可能解决这个问题?
A)高级加密标准 (AES)
B)网络访问控制 (NAC)
C)安全断言标记语言 (SAML)
D)网络时间协议 (NTP)
答案:D
解析:

23.[单选题]What is its called when a system has apparent flaws that were deliberately available for penetration and exploitation?当一个系统有明显的漏洞,故意用来被渗透和利用,这叫什么?
A)investigation调查
B)Entice诱惑
C)Data manipulation数据操纵
D)Trapping诱捕
答案:B
解析:

24.[单选题]Alexis的组织最近转向了软件开发的CI/CD方法,他们打算加快支持其网站的代码部署。使用这种方法,他们期望达到的最合理频率是多少?
Alexis' organization recently moved to a CI/CD approach for software development where they intend to speed up the deployment of code supporting their website. What is the most reasonable frequency that they can expect to achieve using this type of approach?
A)每月部署
Monthly deployments
B)每周部署
Weekly deployments
C)每日部署
Daily deployments
D)数百次每日部署
Hundreds of daily deployments
答案:D
解析:当组织采用持续集成/持续交付(CI/CD)方法进行软件开发时,他们可能会非常快速地部署代码。事实上,一些组织每天使用这种方法将新代码部署到生产环境中数百甚至数千次。
When organizations adopt a continuous integration/continuous delivery (CI/CD) approach to software development, they may deploy code extremely rapidly. In fact, some organizations deploy new code to production hundreds or even thousands of times per day using this approach.

25.[单选题]下列哪些角色有义务确保第三方提供商能够以认真的方式处理和处理数据,并符合组织制定的标准?
A)数据保管人
B)数据所有者
C)数据创建者
D)数据用户
答案:B
解析:

26.[单选题]Which item below is a federated identity standard? 以下哪项是联邦身份标准？
A)802.11i
B)Kerberos
C)Lightweight Directory Access Protocol（LDAP）轻型目录访问协议（LDAP）
D)Security Assertion Markup Language（SAML）安全断言标记语言（SAML）
答案:D
解析:

27.[单选题](04055) During a budgeting meeting an organization's management decides to prioritize security risks Which of the following International Organization for Standardization (ISO) standards would provide the BEST guidance?在组织管理层的预算会议上决定对安全风险进行优先级评级。下面哪项 ISO 标准可以提供最好的指南？
A)ISO 27001
B)ISO 27001
C)ISO 27001
D)ISO 27001
答案:D
解析:

28.[单选题]Following a penetration test, what should an organization do FIRST? 渗透测试之后，组织首先应该做什么？
A)Review all security policies and procedures. 审查所有安全政策和程序。
B)Ensure staff is trained in security. 确保员工接受过安全培训。
C)Determine if you need to conduct a full security assessment. 确定是否需要进行全面的安全评估。
D)Evaluate the problems identified in the test result. 评估测试结果中发现的问题。
答案:D
解析:

29.[单选题]磁盘集群中的未使用空间在媒体分析中很重要,因为它可能包含以下哪一个空间?
A)剩余数据尚未被 覆盖
B)隐藏的病毒和特洛伊 木马
C)有关文件分配表 (FAT) 的信息
D)有关系统修补程序和升级的信息
答案:A
解析:

30.[单选题]What Hypertext Transfer Protocol（HTTP）response header can be used to disable the execution of inline JavaScript and the execution of eval（）-type functions? 什么超文本传输协议（HTTP）响应头可用于禁用内联JavaScript的执行和eval（）类型函数的执行？
A)Strict-Transport-Security严格的运输安全
B)X-XSS-Protection X-XSS-保护
C)X-Frame-Options X帧选项
D)Content-Security-Policy内容安全策略
答案:D
解析:

31.[单选题]以下哪项必须成为支持电子发现存储在云环境中的数据的合同的一部分？
A)与组织目录服务集成以进行身份验证
B)数据的标记
C)混合部署模式
D)识别数据位置

答案:D
解析:略
章节：模拟考试202201

32.[单选题]由于市场份额的快速增长,组织的规模扩大了一倍。信息技术(IT)员工的规模与这种增长保持同步。该组织雇用了几个承包商,他们的现场时间有限。T部门已经突破了构建服务器和推出工作站的限制。并且积压了大量帐户管理请求。哪种合同最适合从IT人员那里卸载任务?
A)一个。平台即服务(PaaS)
B)身份即服务(IDaas)
C)桌面即服务(Daas)
D)软件即服务(SaaS)
答案:B
解析:

33.[单选题]在业务连续性规划 (BCP) 中,记录业务流程的重要性是什么?
A)为高级管理层提供决策 工具
B)建立并采用持续的测试和维护 策略
C)定义谁将在灾难或紧急情况下执行哪些功能。
D)提供对组织相互依存关系的理解
答案:D
解析:

34.[单选题]在生产环境中实施新的漏洞扫描工具时,最重要的是执行以下哪一项以最小化潜在影响?
A)在非高峰时间启用扫描
B)与信息技术(IT)运营团队协商进度
C)建立信息技术(IT)管理的访问权限
D)将漏洞摘要报告记录到安全服务器
答案:B
解析:

35.[单选题]以下有关虚拟专用网VPN协议标准的声明，哪个是错误的?
A)L2第二层隧道协议是PPTP点对点隧道协议和L2F第二层隧道协议的组合。
B)L2第二层隧道协议和PPTP点对点隧道协议是单一点对点客户端到服务器的通信和设计的。
C)L2TP第二层隧道协议在网络层工作。
D)PPTP 点对点隧道协议使用本机 PPP 点对点协议的认证和加密服务。
答案:C
解析:

36.[单选题]关系数据库可以通过查看关系提供安全保障。 查看执行哪一种信息安全原理?
A)最小特权
B)、推理
C)聚合
D)职责分离
答案:A
解析:

37.[单选题](04112) With RBAC, each user can be assigned: 根据RBAC，每个用户可以被分配：
A)One or more roles 一个或多个角色
B)One or more roles 一个或多个角色
C)One or more roles 一个或多个角色
D)One or more roles 一个或多个角色

答案:C
解析:

38.[单选题]Company A is evaluating new software to replace an in-house developed application. During the acquisition process. Company A specified the security retirement, as well as the functional requirements. Company B responded to the acquisition request with their flagship product that runs on an Operating System (OS) that Company A has never used nor evaluated. The flagship product meets all security -and functional requirements as defined by Company A Based upon Company B's response, what step should Company A take? A公司正在评估新软件，以取代内部开发的应用程序。在收购过程中。A公司规定了安全退役以及功能要求。B公司以其旗舰产品回应了收购请求，该产品运行在A公司从未使用或评估过的操作系统（OS）上。旗舰产品符合A公司定义的所有安全和功能要求。根据B公司的回应，A公司应采取什么措施?
A)Move ahead with the acpjisition process, and purchase the flagship software推进acpjisition流程，购买旗舰软件
B)Conduct a security review of the OS对操作系统进行安全审查
C)Perform functionality testing执行功能测试
D)Enter into contract negotiations ensuring Service Level Agreements (SLA) are established to include security patching参与合同谈判，确保建立服务级别协议（SLA），包括安全修补
答案:B
解析:

39.[单选题]灾难恢复 (DR) 包中应包含以下哪一项文档?
Which one of the following documentation should be included in a Disaster Recovery (DR) package?
A)源代码、编译代码、固件更新、操作日志和手册
Source code, compiled code, firmware updates, operational log book and manuals
B)原始格式加密的数据，可审计的交易数据，以及为未来按需提取量身定制的恢复指令
Data encrypted in original format, auditable transaction data, and recovery instructions tailored for future extraction on demand
C)硬件配置说明、硬件配置软件、操作系统映像、数据恢复选项、媒体检索说明和联系信息
Hardware configuration instructions, hardware configuration software, an operating system image, a data restoration option, media retrieval instructions, and contact information
D)系统配置包括硬件、软件硬件接口、软件应用程序编程接口（API）配置、数据结构和上一时期的交易数据
System configuration including hardware, software hardware interfaces, software Application Programming Interface (API)configuration, data structure, and transaction data from the previous period
答案:C
解析:

40.[单选题]您的公司为全球大品牌生产运动鞋,并启动业务持续计划(Business Continuity Program)以支持产品和服务的持续交付。接下来哪项应该先做?(Wentz QOTD)
Your company manufactures sports shoes for a worldwide big label and initiates a business continuity program to support the continuous delivery of products and services. Which of the following should be done first?
A)找出关键活动及其最大可能停止时间
Identify critical activities and their maximum tolerable downtime
B)识别、分析和评估与业务连续性相关的风险
Identify, analyze, and evaluate risk relevant to business continuity
C)确定要受保护以防止中断的产品和服务列表
Determine the list of products and services to be protected from disruption
D)可根据业务需求为关键 IT 服务定义 RTO 和 RPO
Define RTO and RPO for critical IT services subject to business requirements
答案:C
解析:

41.[单选题]以下哪一项通常不是电子发现(e-Discovery) 的一个元素?
A)识别
B)保存
C)产生
D)残留
答案:D
解析:

42.[单选题]物理访问控制类型的示例包括以下所有，除了？
A)徽章
B)锁
C)警卫
D)密码
答案:D
解析: A password is not a physical thing,it’s a logical one.You can control physical access with
Armed guards,by locking doors and using badges to open doors,but you can’t relate
Password to a physical environment.Just to remember,Passwords are used to verify that the
User of an ID is the owner of the ID.The ID-password combination is unique to each user
And therefore provides a means of holding users accountable for their activity on the
System.They are related to software,not to hardware.

43.[单选题]以下哪项防止一个进程访问其他进程的数据？
A)引用监视器
B)内存分割
C)进程隔离
D)数据隐藏
答案:C
解析:

44.[单选题]Including a Trusted Platform Module（TPM）in the design of a computer system is an example of a technique to what? 在计算机系统的设计中包含可信平台模块（TPM）是一种什么技术的示例？
A)Interface with the Public Key Infrastructure（PKI）与公钥基础设施（PKI）的接口
B)Improve the quality of security software提高安全软件的质量
C)Prevent Denial of Service（DoS）attacks防止拒绝服务（DoS）攻击
D)Establish a secure initial state建立安全的初始状态
答案:D
解析:

45.[单选题]What operations role is responsible for protecting the enterprise from corrupt or contaminated media? 什么运营角色负责保护企业免受腐败或污染介质的侵害？
A)Information security practitioner信息安全从业人员
B)Information librarian信息馆员
C)Computer operator电脑操作员
D)Network administrator网络管理员
答案:B
解析:

46.[单选题](04159) 识别数据泄漏的最大挑战是：

A)对相关疑问的理解依赖于法律执行
B)对相关疑问的理解依赖于法律执行
C)对相关疑问的理解依赖于法律执行
D)对相关疑问的理解依赖于法律执行
答案:D
解析:

47.[单选题]临时关键诚信协议 (TKIP) 支持以下哪一项?
A)多广播和广播 消息
B)IEEE 802.11协议的协调
C)有线等效隐私 (WEP) 系统
D)多个设备的同步
答案:C
解析:

48.[单选题]Tareck的组织使用了大量的COTS软件。他最近在对他的业务至关重要的COTS软件包代码中发现了一个严重的缓冲区溢出漏洞。Tareck最有可能纠正这个问题的方法是什么?
Tareck's organization makes use of a significant amount of COTS software. He recently discovered a significant buffer overflow vulnerability in the code of a COTS software package that is crucial to his business. What is the most likely way that Tareck can get this corrected?
A)与他的软件开发团队一起修改代码
Work with his software development team to modify the code.
B)通知供应商并请求补丁
Notify the vendor and request a patch.
C)部署入侵防御系统
Deploy an intrusion prevention system.
D)更新防火墙规则
Update firewall rules.
答案:B
解析:使用商用现货(COTS)软件时,客户通常无法访问源代码,必须依赖供应商发布可纠正漏洞的安全补丁。其他控制措施,例如入侵防御系统和防火墙,可能有助于缓解问题,具体取决于缺陷的性质,但它们无法纠正它。
When using commercial off-the-shelf (COTS) software, customers do not generally have access to the source code and must depend upon the vendor to release security patches that correct vulnerabilities. Other controls, such as intrusion prevention systems and firewalls, may be able to help mitigate the issue, depending upon the nature of the flaw, but they will not correct it.

49.[单选题]关于基于状态的分析作为一种功能软件测试技术,以下哪种说法是正确的?
A)它对于测试通信协议和图形用户界面非常有用
B)通过只考虑分区中的一个代表值,可以覆盖整个分区
C)测试输入来自给定功能规范的导出边界
D)它的特征是在函数中实现的进程的无状态行为
答案:A
解析:

50.[单选题]组织允许ping流量进出其网络。攻击者在网络上安装了一个程序,该程序使用ping数据包的有效负载部分将数据移入和移出网络。组织经历了什么类型的攻击?
A)一个。数据泄露
B)未过滤的通道
C)数据发出
D)隐蔽通道
答案:D