CISSP考试练习(习题卷8)

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]以下所有项目都应包含在业务影响分析中,即 (BIA)调查问卷,以排除问题
A)确定发生业务中断的风险
B)确定业务流程的技术依赖性
C)识别业务中断的运营影响
D)识别业务中断的财务影响
答案:B
解析:

2.[单选题](04143) 在变更生产系统的数据库模式时，应该执行以下哪些活动?
A)在开发环境构建变更，进行用户验收测试，制定回退策略，在生产环境实施变更
B)在开发环境构建变更，进行用户验收测试，制定回退策略，在生产环境实施变更
C)在开发环境构建变更，进行用户验收测试，制定回退策略，在生产环境实施变更
D)在开发环境构建变更，进行用户验收测试，制定回退策略，在生产环境实施变更
答案:C
解析:

3.[单选题]Which of the following vulnerabilities can be BEST detected using automated analysis? 使用自动分析可以最好地检测以下哪种漏洞?
A)Valid cross-site request forgery（CSRF）vulnerabilities有效的跨站点请求伪造（CSRF）漏洞
B)Multi-step process attack vulnerabilities多步骤进程攻击漏洞
C)Business logic flaw vulnerabilities业务逻辑缺陷漏洞
D)Typical source code vulnerabilities典型的源代码漏洞
答案:D
解析:

4.[单选题]测试自定义应用程序代码的最有效方法是什么?
A)阴性 测试
B)白盒 测试
C)笔配对 测试
D)黑匣子 测试
答案:B
解析:

5.[单选题]This statement is the formal requirement for:橙皮书指出,"硬件和软件功能应提供可以用于定期验证[可信计算基]TCB的现场硬件和固件元素的正确操作"。这种说法是对以下哪项的正式要求?
A)Security Testing.安全测试
B)System Architecture Specification.系统架构规范
C)System integrity.系统完整性
D)Design Verification设计验证.
答案:C
解析:

6.[单选题]Gary 正在分析一个安全事故， 在他的调查期间， 他发现有一个用户否认他曾做的事。根据 STRIDE 模型， 此时发生了什么类型的威胁?

A)否认
B)信息泄露
C)篡改
D)特权提升
答案:A
解析:略
章节：模拟考试202201

7.[单选题]Fran 是一个网络开发人员,为一家在线零售商工作。老板要求她采用一种方式,使得客户可以轻松地和Fran公司的网站整合起来。他们需要能够实时检查库存、下订单以及以编程方式检查订单状态,而不必访问网页。Fran可通过什么方式来直接实现这种互动?
A)API
B)WebScraper
C)数据字典
D)呼叫中心
答案:A
解析:应用程序接口(API)允许外部用户直接调用 Fran的程序。用户可以在脚本和其他程序中嵌入API 调用,可自动与Fran的公司进行交互。Web Scraper
或呼叫中心可以促进相同的任务,但是它们不是以集成方式来实现的。数据字典可能提供有用的信息,但它们也不允许直接集成。
An application programming interface (API) allows external users to directly call routines within Fran's code. They can embed API calls within scripts and other programs to automate interactions with Fran's company. A web scraper or call center might facilitate the same tasks, but they do not do so in a direct integration.

8.[单选题]生产系统中对数据库模式进行更改时,应执行以下哪些操作?
A)在开发中测试、确定日期、通知用户并在生产中实施
B)将变化应用于生产,并行运行,最终确定生产变化,并制定 后退战略
C)在生产中执行用户接受测试,让用户签名,并最终完成 更改
D)改变开发,执行用户接受测试,制定退让策略,实施变革
答案:D
解析:

9.[单选题]A Business Continuity Plan (BCP) is based on
业务连续性计划 (BCP) 基于
A)the policy and procedures manual. 政策和程序手册。
B)an existing BCP from a similar organization. 来自类似组织的现有业务连续性计划。
C)a review of the business processes and procedures. 对业务流程和程序的审查。
D)a standard checklist of required items and objectives. 所需项目和目标的标准清单。
答案:C
解析:

10.[单选题](04128) 应急计划演练的目的是?
A)验证服务级别协议
B)验证服务级别协议
C)验证服务级别协议
D)验证服务级别协议
答案:D
解析:

11.[单选题]如果操作系统允许共享资源，如依次被多个用户或应用程序使用的内存，或没有对象/存储区域的刷新的主

体，最有可能存在的安全问题是？
A)残余数据的泄露
B)未经授权而获得的特权执行状态
C)通过秘密渠道的数据泄露
D)通过死锁拒绝服务
答案:C
解析: Allowing objects to be used sequentially by multiple users without a refresh of the objects can lead to disclosure of residual data. It is important that steps be taken to eliminate the chance for the disclosure of residual data.

12.[单选题](04141) 临时密钥完整性协议(TKIP) 用于解决以下哪一项的不足？
A)WEP有线等效保密
B)WEP有线等效保密
C)WEP有线等效保密
D)WEP有线等效保密
答案:D
解析:

13.[单选题]以下哪一项是安全培训和意识计划的关键绩效指标 (KPI)？
A)执行的安全审计次数
B)安全培训活动的参加人数
C)创建的安全培训材料的数量
D)实施的安全控制数量
答案:B
解析:

14.[单选题]A company hired an external vendor to perform a penetration test ofa new payroll system. The company's internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues? 一家公司雇佣了一家外部供应商对一个新的工资系统进行渗透测试。该公司的内部测试团队已经对该系统进行了深入的应用和安全测试，并确定其符合安全要求。然而，外部供应商发现了重大的安全漏洞，即未加密的敏感个人数据被发送到税务处理系统。安全问题最可能的原因是什么？
A)Failure to perform interface testing未能执行接口测试
B)Failure to perform negative testing未能执行阴性测试
C)Inadequate performance testing性能测试不足
D)Inadequate application level testing应用程序级别测试不足
答案:A
解析:

15.[单选题]What would a significant benefit be from conducting an unannounced penetration test? 从哪里进行突然的渗透测试会有很大的益处?
A)Network security would be In a "best stale" posture网络安全被认为在最佳状态的情况下
B)The security analyst could not provide an honest analysis安全分析师未提供一个诚实的分析
C)The analyst could provide an honest. unprepared assessment of the target network.分析师可能会经供一个诚实的,毫无准盔的评估对目标网络
D)lt is best to catch critical infrastructure unpatched;最好在关纳是础设施未打应用补丁时
答案:C
解析:如果经理有理由相信他的IT或安全人员没有保持良好的安全状态,那么就有理由聘请外部分析师来执行评估。其想法是,如果员工有时间在备外部评估,他们将加强安全,并确保一切都准备好接受测试,这不显对他们的网络安全状况的准

确评估。

16.[单选题]Of the following, which BEST provides non- repudiation with regards to access to a server room? 以下哪项最能提供服务器机房访问的不可否认性？
A)Fob and Personal Identification Number (PIN) Fob和个人识别号 (PIN)
B)Locked and secured cages锁定和固定的笼子
C)Biometric readers生物识别读卡器
D)Proximity readers接近读卡器
答案:C
解析:

17.[单选题]以下列出的步骤中，哪一个不属于实施业务影响分析的步骤？
A)为了数据收集选择个人进行约谈
B)备用站点选择
C)创建数据收集技术
D)D. 确定公司的关键业务功能
答案:B
解析: Selecting and Alternate Site would not be done within the initial BIA. It would be done at a later stage of the BCP and DRP recovery effort. All of the other choices were steps that would be conducted during the BIA. See below the list of steps that would be done during the BIA.

18.[单选题]下列哪种攻击类型取决于精确的时间?
A)TOC/TOU
B)SQL 注入
C)传递散列值
D)跨站点脚本
答案:A
解析:

19.[单选题]During a Disaster Recovery (DR) simulation, it is discovered that the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans simultaneously. What would be impacted by this fact if left unchanged? 在灾难恢复 (DR) 模拟过程中，发现共享恢复站点缺乏足够的数据恢复能力，无法支持同时实施多个计划。如果保持不变，这一事实会对什么产生影响？
A)Recovery Point Objective (RPO) 恢复点目标 (RPO)
B)Recovery Time Objective (RTO) 恢复时间目标 (RTO)
C)Business Impact Analysis (BIA) 业务影响分析 (BIA)
D)Return on Investment (ROI) 投资回报率 (ROI)
答案:A
解析:是衡量灾难发生后会丢失多少生产数据的指标。可简单的描述为设施能容忍的最大数据丢失量。

20.[单选题]在RAID5磁盘阵列级别5中，替代故障驱动器的备用驱动器通常是热插拔的，这意味着何时可以更换服务器上的磁盘？
A)系统启动和运行时
B)系统停机和运行时
C)系统在两者之间和运行时
D)系统在中心和运行时
答案:A
解析:

21.[单选题](04012) A hardware feature is built into a Central Processing Unit (CPU) so that all memory locations used by a process can be marked with a non-executable attribute unless the location explicitly

contains executable codeWhich of the following attacks can this feature help prevent?一项硬件功能被内置到一个中央处理单元(CPU)，使一个进程使用的所有内存位置可以打上不可执行属性，除非该位置明确包含可执行代码。此功能可以帮助防止下列哪种攻击？
A)Brute force 暴力破解
B)Brute force 暴力破解
C)Brute force 暴力破解
D)Brute force 暴力破解
答案:A
解析:

22.[单选题]Acme Widgets 公司正在为其会计部门实施新的控制措施。 管理层担心流氓会计师可能会创建一个新的虚假供应商， 然后向该供应商开具支票作为从未提供的服务的付款。 什么安全控制可以最好地帮助防止这种情况？
A)Mandatory vacation
强制休假
B)Separation of duties
职责分离
C)Defense in depth
纵深防御
D)Job rotation
轮岗
答案:B
解析:在遵循职责分离原则时， 组织将关键任务划分为离散的组件， 并确保没有人有能力同时执行这两项任务行动。这可以防止单个流氓个人以未经授权的方式执行该任务。 强制休假和工作轮换旨在检测欺诈， 而不是防止它。 纵深防御不是这里的相关原则， 因为答案是寻求初始控制。 我们可能会选择在以后添加额外的控制， 但这里的主要目标是实现职责分离。
章节：模拟考试202201

23.[单选题]什么样的分布式计算环境组件提供一种机制来确保只有正确指定方才能使用服务？
A)目录服务
B)远程过程调用服务
C)分布式文件服务
D)身份验证和控制服务
答案:A
解析: A directory service has a hierarchical database of users, computers, printers, resources, and
Attributes of each. The directory is mainly used for lookup operations, which enable users to
Track down resources and other users...The administrator can then develop access control,
Security, and auditing policies that dictate who can access these objects, how the objects
Can be accessed, and audit each of these actions.

24.[单选题]根据最佳实践,在生产环境中实施第三方软件的最佳做法是？
A)将第三方软件托管
B)和供应商签订关于补丁的合同
C)扫描第三方的应用软件以发现漏洞
D)协商最终用户使用应用的培训
答案:C
解析:略
章节：模拟考试202201

25.[单选题]Hannah has been assigned the task of installing Web access management (WAM) software. What is

the best description for what WAM is commonly used for?汉娜已经被分配安装Web访问管理(WAM))软件的任务,WAM常用的最好描述是?
A)Control external entities requesting access through ×.500 databases控制外部实体通过请求访问X.500数据库
B)Control external entities requesting access to internal objects控制外部实体请求访问内部对象
C)Control internal entities requesting access through X.500 databases控制内部实体通过请求访问X.500数据库
D)Control internal entities requesting access to external objects控制内部实体请求访问外部对象
答案:B
解析:

26.[单选题]When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test? 在评估web漏洞时，如何导航黑暗的web为渗透测试增加价值？
A)The actual origin and tools used for the test can be hidden. 可以隐藏用于测试的实际原点和工具。
B)Information may be found on related breaches and hacking. 可能会发现有关违规和黑客行为的信息。
C)Vulnerabilities can be tested without impact on the tested environment. 可以在不影响测试环境的情况下测试漏洞。
D)Information may be found on hidden vendor patches. 可以在隐藏的供应商补丁上找到信息。
答案:D
解析:

27.[单选题]下列哪项对确保静态数据的机密性提供最佳保障?
Which of the following provides the best protection to ensure the confidentiality of data at rest?
A)破坏
Destruction
B)加密
Encryption
C)净化
Sanitization
D)标记
Marking
答案:B
解析:

28.[单选题]下列哪一项可能引起对凭据管理系统的拒绝服务(DoS)攻击?
A)延迟撤销或销毁凭据
B)修改证书吊销列表
C)未经授权的续期或补发
D)停止使用后的令牌使用
答案:B
解析:

29.[单选题]A user downloads a file from the Internet, then applies the Secure Hash Algorithm 3 (SHA-3) ? 用户从Internet下载文件，然后应用安全哈希算法3（SHA-3）？
A)It verifies the integrity of the file. 它验证文件的完整性。
B)It checks the file for malware. 它检查文件中是否有恶意软件。
C)It ensures the entire file downloaded. 它确保下载整个文件。
D)It encrypts the entire file. 它对整个文件进行加密。
答案:A
解析:

30.[单选题]一个犯罪组织正计划对政府网络进行攻击。 以下哪一项是对网络可用性最严重的攻击？

A criminal organization is planning an attack on a government network. Which of the following is the MOST severe attack to the network availability?
A)攻击者在网络拓扑上收集敏感信息
Sensitive information is gathered on the network topology by attacker
B)网络管理通信被攻击者中断
Network management communications is disrupted by attacker
C)网络充斥着攻击者的通信流量
Network is flooded with communication traffic by attacker
D)运营商对攻击者失去了对网络设备的控制
Operator loses control of network devices to attacker
答案:D
解析:

31.[单选题]In systems security engineering, what does the security principle of modularity provide? 在系统安全工程中，模块化的安全原则提供了什么？
A)Documentation of functions职能文件
B)Isolated functions and data隔离的功能和数据
C)Secure distribution of programs and data程序和数据的安全分发
D)Minimal access to perform a function执行功能的最小访问权限
答案:A
解析:

32.[单选题]When planning a penetration test, the tester will be MOST interested in which information? 在计划渗透测试时，测试人员最感兴趣的是哪些信息？
A)Places to install back doors安装后门的位置
B)The main network access points主要网络接入点
C)Job application handouts and tours工作申请讲义和参观
D)Exploits that can attack weaknesses可以攻击弱点的漏洞
答案:D
解析:

33.[单选题]维护活动负责定义、实施和测试更新应用系统?
A)程序更改 控制
B)回归 测试
C)出口例外 控制
D)用户接受 测试
答案:A
解析:

34.[单选题]Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege? 哪种身份和访问管理（IAM）流程可用于维护最小权限原则？
A)identity provisioning身份准备
B)access recovery访问恢复
C)multi-factor authentication (MFA) 多因素身份验证（MFA）
D)user access review用户访问审查
答案:A
解析:

35.[单选题]一个组织采用了新的防火墙加固标准。安全专业人员如何验证技术人员正确实施了新标准?
An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

A)执行合规性审查
Perform a compliance review
B)执行渗透测试
Perform a penetration test
C)培训技术人员
Train the technical staff
D)调查技术人员
Survey the technical staff
答案:A
解析:合规是检查实施的结果

36.[单选题]在向高级管理层汇报信息安全控制的结果时,下面哪个是安全理应采用的最好的方法?
A)Number of attacks avoided and stopped 规避和停止的攻击数量
B)Business processes affected and improved 受影响和已改进的业务流程
C)Date loss reduction figures 损失数据减少图表
D)IT budget reduction figures IT 预算降低图表
答案:B
解析:略
章节：模拟考试202201

37.[单选题]如果 SYN 洪水攻击中的攻击者使用其他人的有效主机地址作为源地址,则受攻击的系统将向
A)默认 网关。
B)攻击者的 地址。
C)本地接口受到 攻击。
D)指定的源 地址。
答案:D
解析:

38.[单选题]Wanda正在与其组织的欧盟业务合作伙伴之一进行合作,为了促进客户信息的交换。Wanda的组织位于美国。Wanda用来确保GDPR合规性的最佳方法是什么?
Wanda is working with one of her organization's European Union business partners to facilitate the exchange of customer information. Wanda's organization is located in the United States. What would be the best method for Wanda to use to ensure GDPR compliance?
A)约束性公司规则
Binding corporate rules
B)隐私保护
Privacy Shield
C)标准合同条款
Standard contractual clauses
D)安全港
Safe harbor
答案:C
解析:欧盟提供可用于促进数据传输的标准合同条款。在两家不同公司共享数据的情况下,这将是最佳选择。如果数据在公司内部共享,约束性公司规则也是一种选择。欧盟/美国隐私保护是一项安全港协议,这个协议过去允许转送但现在不再有效。

39.[单选题]以下哪项是缓解活动用户工作站数据被盗的最有效方法?
A)一个。实施全磁盘加密
B)启用多重身份验证
C)部署文件完整性检查器
D)禁用便携式设备

答案:D
解析:

40.[单选题]使用下列哪个公式计算测试覆盖率?
A)测试的用例数量/用例总数
B)测试代码行数/代码行总数
C)测试的功能数量/功能总数
D)测试的条件分支数/可测试分支的总数
答案:A
解析:测试覆盖率的计算方法是:测试覆盖率=测试的用例数/用例总数。代码覆盖率其他公式计算得出,包括函数、条件和总代码覆盖率。
Test coverage is computed using the formula test coverage = number of use cases tested/total number of use cases. Code coverage is assessed by the other formulas, including function, conditional, and total code coverage.

41.[单选题]When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined? 当根据国际标准化组织（ISO）27001和27002制定的标准评估组织的安全政策时，何时可以定义管理责任?
A)Only when assets are clearly defined只有在明确定义资产时
B)Only when standards are defined仅当定义了标准时
C)Only when controls are put in place仅当控制装置就位时
D)Only procedures are defined仅定义了程序
答案:A
解析:

42.[单选题]Matthew希望在他的网络上测试系统的SQL注入漏洞。下面哪个工具最适合这个任务?
A)端口扫描
B)网络漏洞扫描器
C)网络发现扫描器
D)Web漏洞扫描器
答案:D
解析:SQL注入攻击是web漏洞,而web漏洞扫描器将是Matthew的最佳服务。网络漏洞扫描器也可能发现这个漏洞,但web漏洞扫描器是专门为这项任务设计的,更有可能成功。

43.[单选题]Aaron工作的银行希望允许客户使用他们正在合作的第三方合作伙伴提供的新附加应用程序。由于并不是每个客户都想要或需要一个帐户,Aaron建议银行使用基于SAML的工作流程,在用户下载应用程序并尝试登录时创建一个帐户。他建议使用哪种类型的供应系统?
A)JIT
JIT
B)OpenID
OpenID
C)OAuth
OAuth
D)Kerberos
Kerberos
答案:A
解析:JIT(即时供应机制)会在需要时创建账户,而不是提前创建账户。这是一种限制所维护账户数量的有效方法,如果用户账号是许可协议的一部分,则该方法非常有用。问题中未提及 OAuth、OpenID和Kerberos。

44.[单选题]受试者可以与对象进行授权交互的类型是

A)控制。
B)许可。
C)程序。
D)协议。
答案:B
解析:

45.[单选题]安全管理员定期监视威胁源并使用该信息检查网络内的系统。 他们的目标是发现现有工具未检测到的任何感染或攻击。 以上描述了哪种技术?
Security administrators are regularly monitoring threat feeds and using that information to check systems within the network. Their goal is to discover any infections or attacks that haven’t been detected by existing tools. What does this describe?
A)威胁搜寻
Threat hunting
B)威胁情报
Threat intelligence
C)实施杀伤链
Implementing the kill chain
D)使用人工智能
Using artificail intelligence
答案:A
解析:威胁搜寻是在网络内主动搜索感染或攻击的过程。
威胁情报是指在分析传入数据(例如威胁源)后创建的可操作情报。 威胁猎手使用威胁情报来搜索特定威胁。 此外,他们可能会使用杀伤链模型来缓解这些威胁。
人工智能 (AI) 是指机器的操作,但场景表明管理员正在执行工作。

46.[单选题]Richard 在其组织的网络上遇到网络服务质量问题。 主要症状是数据包从源到目的地传输的时间总是太长。 哪个术语描述了理查德面临的问题?
A)抖动
B)丢包
C)干扰
D)延迟
答案:D
解析:延迟是数据包从源到目的地的传输延迟。 抖动是不同数据包延迟的变化。 数据包丢失是传输过程中需要重新传输的数据包的消失。 干扰是电噪声或其他破坏数据包内容的中断。

47.[单选题]安全最基本的原则是什么?
A)问责性、保密性和完整性
B)完整性、可用性和问责性
C)保密性、完整性和可用性
D)可用性、问责性和保密性
答案:C
解析:

48.[单选题](04146) 使用安全验证和日志能够提供?
A)职责分离
B)职责分离
C)职责分离
D)职责分离
答案:D
解析: