CISSP考试练习(习题卷2)

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]实施最小特权原则的最终结果是指?
A)用户可以访问所有系统。
B)用户只能访问他们需要知道的信息。
C)当用户职位改变时，会得到新增的特权
D)授权蠕变
答案:B
解析: The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.

2.[单选题]基于角色的访问控制 (RBAC)的一个重要特征是什么?
A)支持强制访问控制 (MAC)
B)简化访问权限管理
C)依靠杜蒂的旋转
D)需要两个因素 身份验证
答案:B
解析:

3.[单选题]以下哪一选项不是合适用户账户管理的元素？
A)用于跟踪访问权限的流程应予以实施。
B)在敏感职位定期重新筛选人员
C)应该定期审查用户账户
D)用户应该永远不会被转出了其当前职责
答案:D
解析:

4.[单选题]Ed 负责确定一项服务,该项服务可为其雇主提供低延迟、高性能和高可用性的内容托管。他应该采用什么类型的解决方案,以确保雇主的全球客户能够快捷、可靠地访问内容?
A)热站点
B)CDN(内容分发网络)
C)冗余服务器
D)P2P CDN(对等的内容分发网络)
答案:B
解析:内容分发网络(CDN)可提供可靠、低延迟、基于地理位置的内容分发。CDN可以满足本题的要求。企业一般不会选择P2P CDN(例如 BitTorrent)。冗余服务器和热站点可以提供高可用性,但无法满足其他要求。
A Content Distribution Network (CDN) is designed to providereliable, low-latency,geographically distributed content distribution. In this scenario, a CDN is an ideal solution. A P2P CDN like BitTorrent isn't a typical choice for a commercial entity,whereas redundant servers or a hot site can provide high availability but won't provide the remaining requirements.

5.[单选题]IP 数据包可以分为两部分:报头和有效载荷。 IPsec 以传输模式和隧道模式对 IP 数据包进行封装,并通过 AH 和 ESP 对其进行保护。 AH 仅支持真实性,而 ESP 是 IPsec 实现中的强制性要求,支持机密性和真实性。 以下哪个是不正确的? (Wentz QOTD)
A)传输模式下的AH对IP包进行认证

B)隧道模式下的AH对新的IP包进行认证
C)传输模式下的 ESP 对 IP 负载进行加密和认证
D)隧道模式下的ESP对新的IP包进行加密和认证
答案:D
解析:隧道模式下的 ESP 加密和验证新 IP 数据包的 IP 负载,而不是新 IP 数据包本身。 AH 验证“IP 数据包”,而 ESP 加密和验证“IP 负载”。 IPsec 隧道模式,无论是使用 AH 还是 ESP,都会创建一个新的 IP 数据包,因此原始 IP 数据包成为其“有效载荷”。

6.[单选题]业务连续性计划 (BCP) 培训和意识计划的目标是
A)提高创建、维护和执行计划所需的技能 。
B)规定在发生灾害时进行高水平的恢复。
C)向新员工描述恢复组织。
D)为每个恢复团队提供检查表和 程序。
答案:A
解析:

7.[单选题]知识产权保护什么
A)权利 可以自己控制交付形式的权利
B)能力 拥有版权的能力
C)权利 享有创作的权利
D)能力 金钱收入的能力
答案:C
解析:略
章节：模拟考试202201

8.[单选题](04056) During the development of a contingency plan, which of the following processes MUST be performed prior to the design phase?在开发业务连续性计划时，下面哪个流程必须是在设计阶段之前执行的？
A)Maintenance analysis 维护分析
B)Maintenance analysis 维护分析
C)Maintenance analysis 维护分析
D)Maintenance analysis 维护分析
答案:A
解析:

9.[单选题]光盘介质怎么销毁？
A)消磁
B)销毁
C)删除
D)清除
答案:B
解析:略
章节：模拟考试202201

10.[单选题]下列哪一项不是CSMA载波侦听多路访问的属性？
A)工作站连续监测线
B)工作站不允许传输，直到它们被从主要主机获得许可
C)它不具有避免工作站控制对话这一问题的特性
D)工作站传送数据包时，它认为线是免费的
答案:B
解析:<p>The correct answer is "Workstations are not permitted to transmit until they are given permission from the primary host". The polling transmission type uses primary and secondary hosts,

and the secondary must wait for permission from the primary before transmitting.</p>

11.[单选题]通过检查传入的数据包的"状态"和"上下文", 它可以帮助跟踪被认为是”无连接"的协议, 如基于 UDP用户数据报协议的应用程序和远程过程调用 (RPC)。这种类型的防火墙系统用于?
A)第一代防火墙系统。
B)第二代防火墙系统。
C)第三代防火墙系统。
D)第四代防火墙系统
答案:C
解析:

12.[单选题]Susan的组织是一个联合的一部分,该联合允许来自多个组织的用户访问其他联合站点上的资源和服务。当Susan想要在合作伙伴站点使用服务时,使用哪个身份提供者?Susan's organization is part of a federation that allows users from multiple organizations to access resources and services at other federated sites. When Susan wants topartner site, which identity provider is used?
A)Susan所在组织的身份提供者
Susan's home organization's identity provider
B)服务提供商的身份提供者
The service provider's identity provider
C)他们的身份提供者和服务提供商的身份提供者
Both their identity provider and the service provider's identity provider
D)服务提供者创建新身份
The service provider creates a new identity
答案:A
解析:

13.[单选题]安全合规的目的
A)提高安全态势/更少的监管
B)增强安全态势/提高攻击防御
C)满足高层要求
D)提升安全策略/提高攻击防御
答案:B
解析:略
章节：模拟考试202201

14.[单选题]在设计漏洞测试时,以下哪一项可能最清楚地说明当前网络上哪些组件在运行?
A)拓扑 图
B)映射工具
C)资产 登记册
D)平测试
答案:D
解析:

15.[单选题]组织FIRST会审查哪些内容以确保符合隐私要求?
A)一个。最佳实践
B)业务目标
C)法律和监管要求
D)员工对政策和标准的遵守情况
答案:C
解析:

16.[单选题]During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.What is the best approach for the CISO?During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant. What is the best approach for the CISO? 在项目的风险评估阶段，CISO发现该大学的一所学院正在通过内部开发的应用程序收集受保护的健康信息（PHI）数据。收集这些数据的学院完全了解《健康保险可携带性和责任法案》（HIPAA）的规定，并完全遵守。CISO的最佳方法是什么？在项目的风险评估阶段，CISO发现该大学的一所学院正在通过内部开发的应用程序收集受保护的健康信息（PHI）数据。收集这些数据的学院完全了解《健康保险可携带性和责任法案》（HIPAA）的规定，并完全遵守。CISO的最佳方法是什么？
A)Document the system as high risk将系统记录为高风险
B)Perform a vulnerability assessment执行漏洞评估
C)Perform a quantitative threat assessment进行定量威胁评估
D)Notate the information and move on记下信息并继续
答案:B
解析:

17.[单选题](04057) Which of the following is the MAIN security concern of the Platform-as-a-Service (PaaS) public cloud computing model?下面哪项是PaaS公共云计算模型主要的安全关注？
A)Event monitoring 事件监控
B)Event monitoring 事件监控
C)Event monitoring 事件监控
D)Event monitoring 事件监控
答案:B
解析:

18.[单选题]下面哪一个最好地描述了调试程序的目的？
A)为了生成可用于实施前测试程序的随时数据。
B)为了确保程序编码缺陷被检测和翻译。
C)为了在编程阶段有效的变化不被其他变化保护覆盖。
D)为了在代码转到测试环境之前比较源版本。
答案:B
解析: Bug是计算机程序中的编码错误。
在
程序最终用户之前发现错误的过程称为调试。首次编写代码后开始调试，
随着代码与其他编程单元组合形成
软件产品，如操作系统或应用程序，调试将在后续阶段继续进行。调试的主要原因
是为了检测和纠正程序中的错误

19.[单选题](04010) Why do some sites choose not to implement Trivial File Transfer Protocol (TFTP)?为什么一些站点不选择实施TFTP协议？
A)list restrictions 列表限制
B)list restrictions 列表限制
C)list restrictions 列表限制
D)list restrictions 列表限制
答案:C
解析:

20.[单选题]以下哪项不是漏洞评估的结果？

A)定量损失评估
B)确定关键支持领域
C)业务连续性计划的范围和启动文件的正式批准
D)定性风险损失评估
答案:C
解析:

21.[单选题]渗透测试在SDLC的哪个阶段？
A)设计和开发
B)操作和维护阶段
C)编码和实现
D)定义和启动
答案:B
解析:略
章节：模拟考试202201

22.[单选题]以下哪种协议允许组织维护可读取受保护网页的集中用户列表?
A)轻量级目录访问控制 (LDAP)
B)精柔断言标记语言 (SAML)
C)超文本传输协议 (HTTP)
D)克贝罗斯
答案:A
解析:

23.[单选题]In software development, developers should use which type of queries to prevent a Structured Query Language（SQL）injection? 在软件开发中，开发人员应该使用哪种类型的查询来防止结构化查询语言（SQL）注入？
A)Parameterised参数
B)Dynamic动态
C)Static静态
D)Controlled控制
答案:A
解析:

24.[单选题](04140) OSI模型中，在发送方和接收方之间建立逻辑连接的是哪一层？
A)物理层
B)物理层
C)物理层
D)物理层
答案:B
解析:

25.[单选题]在提供 Internet 访问的同时,通过接受客户端请求、更改请求的源地址、将请求映射到客户端以及将修改后的请求发送到目的地,这是什么网络工具?
What network tool can be used to protect the identity of clients while providing Internet access by accepting client requests, altering the source addresses of the requests, mapping requests to clients, and sending the modified requests out to their destination?
A)A switch
B)A proxy
C)A router
D)A firewall

答案:B
解析:

26.[单选题]在重新使用驱动器之前,您可以采取什么措施来防止由于 SSD 设备上的磨损均衡而导致意外数据泄露?
A)重新格式化
B)磁盘加密
C)消磁
D)物理销毁
答案:B
解析:

27.[单选题]在进行风险评估后,您的组织确定了设施和数据中心发生火灾的风险。 您正在考虑安全控制来应对风险。 应首先实施以下哪项? (Wentz QOTD)
A)进行消防演习
B)购买火灾保险
C)建立灭火系统
D)提供消防安全意识和培训
答案:D
解析:

28.[单选题]International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following? 国际机构制定了一项管制计划，规定签署国之间如何交换武器。它还涉及网络武器，包括恶意软件、指挥与控制（C2）软件和互联网监控软件。这是以下哪项的描述？
A)General Data Protection Regulation（GDPR）通用数据保护法规（GDPR）
B)Palermo convention巴勒莫条约
C)Wassenaar arrangement塞纳安排
D)International Traffic in Arms Regulations（ITAR）国际武器贩运条例（ITAR）
答案:C
解析:

29.[单选题]在评估第三方应用程序时,以下哪一项是信息安全的最大责任?
A)代表组织接受风险 。
B)向企业报告调查结果,以确定安全 漏洞。
C)量化产品选择 对业务的风险 。
D)批准最符合安全要求的应用程序 。
答案:C
解析:

30.[单选题]Spyware is BEST described as间谍软件最好描述为
A)data mining for advertising. 广告数据挖掘。
B)a form of cyber-terrorism, 一种网络恐怖主义,
C)an information gathering technique, 信息收集技术,
D)a web-based attack. 基于web的攻击。
答案:B
解析:

31.[单选题]信息系统 (IS) 上的漏洞测试
A)利用IS中的安全弱点 。
B)测量安全控制薄弱的系统上的系统性能 。

C)评估安全控制的有效性 。
D)为灾后恢复 (DR) 规划做好准备。
答案:C
解析:

32.[单选题](04014) Which of the following is not an OSI architecture-defined broad category of security standards?下面哪项不是OSI架构定义的安全标准的广义类别之一？
A)Security techniques standards 安全技术标准
B)Security techniques standards 安全技术标准
C)Security techniques standards 安全技术标准
D)Security techniques standards 安全技术标准
答案:D
解析:

33.[单选题]在尝试了解未知应用程序的目的时,在法医分析中最重要的步骤是什么?
A)禁用所有不必要的 服务
B)确保监管链
C)准备系统的另一个备份
D)将系统与网络分离
答案:D
解析:

34.[单选题]文件和应用程序在哪里？
A)最小特权的概念
B)因为他们不能被操作者访问
C)因为他们可能包含依靠
D)“由于知道其需要”的概念
答案:C
解析:

35.[单选题]A practice that permits the owner of a data object to grant other users access to that object would usually provide允许数据对象所有者授予其他用户访问该对象的权限的做法通常会提供
A)Mandatory Access Control（MAC）. 强制访问控制（MAC）。
B)owner-administered control. 业主管理的控制。
C)owner-dependent access control. 依赖于所有者的访问控制。
D)Discretionary Access Control（DAC）. 自主访问控制（DAC）。
答案:D
解析:

36.[单选题]关于链路加密下列哪一项是正确的？
A)每个实体有和目的地节点享有一个共同的密钥
B)如果沿传输路径的任意节点被攻破则这种模式将不提供保护
C)只有安全节点用于这种类型的传输。
D)已加密的消息只在最后一个节点进行解密
答案:B
解析: In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain. Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re-encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.

37.[单选题]以下哪项是法庭取证员从恶意软件中获取最大量相关信息的最佳方法?

Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information form malicious software?
A)查看代码以识别其来源。
Review the code to identify its origin.
B)分析程序的行为。
Analyze the behavior of the program.
C)检查文件属性和权限。
Examine the file properties and permissions.
D)分析软件生成的日志。
Analyze the logs generated by the software.
答案:B
解析:

38.[单选题]通过使用可信路径,可以防止什么类型的攻击?
A)字典攻击
B)暴力攻击
C)中间人攻击
D)登录欺骗
答案:D
解析:通用标准定义了可信路径,这是一种在用户和安全组件之间保护数据的方式。使用可信路径可以防止登录欺骗攻击。可信信道可以防止中间人攻击,通常使用加密和证书来实现。使用回退算法可以有效防止暴力和字典攻击。

39.[单选题]随着事件响应的进展,团队在哪个阶段进行根本原因分析?
A)响应
B)报告
C)补救
D)经验教训
答案:C
解析:通过根本原因分析可以检查事件以确定是否允许该事件发生,并为修复系统提供关键信息,以便事件不再发生。这是事件响应过程中修复步骤的一个部分,因为根本原因分析的结果对完全修复受影响的系统和过程是必需的。
The root cause analysis examines the incident to determine what allowed it to happen and provides critical information for repairing systems so that the incident does not recur. This is a component of the remediation step of the incident response process because the root cause analysis output is necessary to fully remediate affected systems and processes.

40.[单选题]An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the BEST response to the auditor? 执行合规性审核的审计员请求在系统中加密的密码，以验证密码是否符合策略。以下哪项是对审计师的最佳回应？
A)Provide the encrypted passwords and analysis tools to the auditor for analysis. 向审计员提供加密密码和分析工具进行分析。
B)Analyze the encrypted passwords for the auditor and show them the results. 分析审计员的加密密码，并向他们显示结果。
C)Demonstrate that non-compliant passwords cannot be created in the system. 演示无法在系统中创建不合规密码。
D)Demonstrate that non-compliant passwords cannot be encrypted in the system. 演示无法在系统中加密不合规密码。
答案:C
解析:

41.[单选题]哪个模型通过格式化交易和职责分离以实现数据完整性？

A)CIark-Wilson 模型
B)Biba模型
C)非干扰模型
D)Sutherland 模型
答案:A
解析:

42.[单选题]____指对个人身份信息或可能对他人造成伤害、令他人感到尴尬的信息加以保密。
A)隔绝
B)隐藏
C)隐私
D)关键性
答案:C
解析:隐私

43.[单选题]Tom 启用了由他的云基础设施作为服务提供商提供的应用程序防火墙， 旨在阻止多种类型的应用程序攻击。 从风险管理的角度来看， Tom 试图通过实施此对策来降低什么指标?
A)Impact
影响
B)RPO
RPO
C)MTO
MTO
D)Likelihood
可能性
答案:D
解析:安装能够阻止攻击的设备是通过降低应用程序攻击成功的可能性来降低风险的一种尝试。添加防火墙不会解决风险. 恢复点目标 (RPO) 或最大可容忍中断 (MTO) 的影响。
章节：模拟考试202201

44.[单选题]Copyright provides protection for which of the following? 版权为以下哪项提供保护?
A)Ideas expressed in literary works文学作品中表达的思想
B)A particular expression of an idea思想的特殊表达
C)New and non-obvious inventions新的和不明显的发明
D)Discoverise of natural phenomena自然现象的发现
答案:B
解析:

45.[单选题]An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered? 涵盖安全性的内部服务级别协议 (SLA) 由高级管理人员签署并生效。何时应审查SLA合规性，以确保提供良好的安全态势?
A)As part of the SLA renewal process作为SLA续订过程的一部分
B)Prior to a planned security audit在计划的安全审计之前
C)Immediately after a security breach安全漏洞发生后立即
D)At regularly scheduled meetings在定期安排的会议上
答案:D
解析:

46.[单选题]Ben 需要验证他组织的关键应用程序的最新补丁没有在其他地方引入问题。Ben 需要进行什么类型的测试以确保这一点?

A)单元测试
B)白盒测试
C)回归测试
D)黑盒测试
答案:C
解析:回归测试确保应用程序或系统在更改后具有正确功能。单元测试的重点是测试程序的每个模块,而不关注整体功能是否和以前一样。白盒测试和黑盒测试都描述了测试者对系统或应用程序所掌握的知识量。
Regression testing ensures proper functionality of an application or system after it has been changed. Unit testing focuses on testing each module of a program instead of against its previous functional state.White and black box testing both describe the amount of knowledge about a system or application, rather than a specific type or intent for testing.

47.[单选题]业务连续性计划执行阶段需要包括几团队,哪个团队是负责启动主场所的恢复
A)Damage assessment team 损失评估团队
B)BCP team BCP团队
C)Salvage team 救援团队
D)Restoration team 恢复团队
答案:C
解析:略
章节：模拟考试202201

48.[单选题]主体声称身份的过程被称为什么?
A)登录
B)认证
C)授权
D)令牌呈现
答案:B
解析:主体声明身份的过程被称为认证。授权通过检查密码来验证主体的身份。登录通常包括认证和授权,选项D的令牌呈现也是一种认证。

49.[单选题]选择正确的风险分析方法来满足组织的需求目标是很重要的。以下哪一项最好地描述了何时应该使用风险管理标准 ASINZS 4360?
A)当需要评估组织里直接关系到信息安全的各种条目时
B)当需要评估组织里不仅限于那些信息安全的条目时
C)当需要定性地证明符合各种规章的水平时
D)当需要定性地证明符合各种法律的水平时
答案:B
解析:

50.[单选题]Limiting the processor, memory, and Input/output （I/O）capabilities of mobile code is known as
限制移动代码的处理器、内存和输入/输出（I/O）能力称为
A)code restriction. 代码限制。
B)sandboxing. 沙箱。
C)on-demand compile. 按需编译。
D)compartmentalization. 划分。
答案:B
解析:

51.[单选题]Brian 正在为其组织的灾难恢复计划制定培训计划,并希望确保参与者了解灾难活动何时结束。 以下哪一个事件标志着灾难恢复过程的完成?