CISSP考试练习(习题卷5)

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]one purpose of a security awareness program is to modify ?
安全意识计划的目的之一是要提升?
A)Corporate attitudes about safeguarding data.
企业保护数据的态度
B)The attitude and behavior of employees towards enterprise security posture.
员工对企业安全态势的态度与行为
C)Employees' attitudes to sensitive data.
员工对敏感数据的态度
D)The management method of enterprise security situation.
对企业安全态势的管理方法
答案:B
解析:

2.[单选题]对于已分类的数据,下列哪一项是最低的军事数据分类级别?
A)敏感
B)机密
C)专有
D)私有
答案:B
解析:在列出的选项中,机密是军事数据分类中最低的。请记住,标为"机密" "秘密"和"绝密"的项目统称为"密级",而"机密"在列表中的"秘密"以下。

3.[单选题]组织应如何确定在进行漏洞评估后其补救工作的优先事项?
A)使用基于影响 的方法。
B)使用基于风险 的方法。
C)使用基于批判性 的方法。
D)使用基于威胁 的方法。
答案:B
解析:

4.[单选题]Darren 正在对他的组织使用的 Kerberized 应用程序的身份验证问题进行故障排除。 他认为问题在于会话密钥的生成。 他应该首先调查什么 Kerberos 服务?
A)KDC
B)TGT
C)AS
D)TGS
答案:D
解析:TGS 或票证授予服务(通常与 KDC 位于同一服务器上)从客户端接收 TGT。 它验证 TGT 和用户访问服务的权限他们要求使用。 然后 TGS 向客户端发出票证和会话密钥。 AS作为认证服务器,将用户名转发给KDC。 值得注意的是,客户端不直接与 KDC 通信。 相反,它将与 TGT 和 AS 通信,这意味着 KDC 在这里不是合适的答案

5.[单选题]Renee 正在与她的董事会讨论他们审查网络安全控制的责任。 什么规则要求高级管理人员对信息安全事务承担个人责任?
Renee is speaking to her board of directors about their responsibilities to review cybersecurity

controls. What rule requires that senior executives take personal responsibility for information security matters?
A)尽职调查规则
Due diligence rule
B)个人责任规则
Personal liability rule
C)审慎人治
Prudent man rule
D)正当程序规则
Due process rule
答案:C
解析:

6.[单选题]以下哪种类型的控件没有描述 mantrap?
A)威慑
B)预防
C)补偿
D)物理
答案:C
解析:

7.[单选题]At a MINIMUM, audits of permissions to individual or group accounts should be scheduled至少应安排对个人或集团帐户权限的审核
A)annually一年一次地
B)to correspond with staff promotions与员工晋升相对应
C)to correspond with terminations与终端相对应
D)continually不断地
答案:A
解析:

8.[单选题]以下哪项描述了一个信任域共享一个单独的安全策略和单独的管理？
A)安全内核
B)安全边界
C)引用监视器
D)安全域
答案:D
解析: A security domain is a domain of trust that shares a single security policy and single management. The term security domain just builds upon the definition of domain by adding the fact that resources within this logical structure (domain) are working under the same security policy and managed by the same group.

9.[单选题]Jeff 想采用行业标准方法来评估其组织用来管理风险的流程。 哪种成熟度模型最适合他的使用?
Jeff would like to adopt an industry-standard approach for assessing the processes his organization uses to manage risk. What maturity model would be most appropriate for his use?
A)CMM
B)SW-CMM
C)Risk Maturity Model
D)COBIT
答案:C
解析:

10.[单选题]对数据进行分类时,通常不考虑下列哪一项特征?
A)价值
B)客体的大小
C)可用的生命周期
D)对国家安全的影响
答案:B
解析:大小不是建立数据分类的标准。在对目标进行分类时,应该考虑价值、生命周期和安全。

11.[单选题](04138) 在审核系统管理时，审计师发现系统管理员没有经过必要的培训，为了确保系统的完整性，需要立即采取哪项行动?
A)安排有经验的管理员对所有系统进行评审
B)安排有经验的管理员对所有系统进行评审
C)安排有经验的管理员对所有系统进行评审
D)安排有经验的管理员对所有系统进行评审
答案:B
解析:

12.[单选题]Adam 正在处理对最终用户的访问请求。在授予访问权限之前,他还应该验证哪两项?
A)分离和需知
B)许可和认可
C)许可和需知
D)第二因素和许可
答案:C
解析:在授予任何用户访问信息之前,Adam 应验证用户是否有适当的安全许可,用户是否需要了解相关信息。
Before granting any user access to information,Adam should verify that the user has an appropriate security dearance as well as a business need to know the information in question.

13.[单选题](04120) 一个大型组织使用唯一的身份标识，并要求他们在每次系统会话的开始时使用。应用程序访问是基于工作职责的分类。该组织定期对访问控制和违规进行独立的审核。该组织使用了有线和无线网络，以及远程访问。该组织还使用了到分支机构的安全连接，以及针对某些选择的信息和流程实施安全的备份和恢复策略。访问控制日志除了身份标识外还必须包含什么内容?
A)Time of the access 访问的时间
B)Time of the access 访问的时间
C)Time of the access 访问的时间
D)Time of the access 访问的时间
答案:A
解析:

14.[单选题]以下哪一项是用来计算ALE的公式?
A)ALE=AV*EF*ARO
B)ALE=ARO*EF
C)ALE=AV*ARO
D)ALE=EF*ARO
答案:A
解析:年度损失期望(ALE)是资产价值(AV)乘以暴露因子(EF)后再乘以年度发生率(ARO)的积。ALE=AV*EF*ARO

15.[单选题]关于安全内核的状态描述下述哪项是不正确的?
A)安全内核是一个访问控制的概念，和实际物理组件无关
B)安全内核组成的机制属于TCB,用于执行和强制引用监视器概念.
C)安全内核必须为提供隔离进行参考监视器概念的过程，他们必须具有防篡改性
D)安全内核必须足够小以便可以以完整和全面的方式进行检测和证明

答案:A
解析: The reference monitor, not the security kernel is an access control concept. The security kernel is made up of software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems.

16.[单选题]关于VPN隧道，下列哪一陈述是不正确的？
A)它可以通过实现节点身份验证系统来创建。
B)它只能通过实现IPSec设备来创建。
C)它可以通过实现密钥和证书交换系统来创建。
D)它可以通过在客户端或网络上安装软件或硬件代理来创建。
答案:B
解析: IPSec-compatible and non-IPSec compatible devices are used to create VPNs. The other three answers are all ways in which VPNs can be created.

17.[单选题]业务影响分析 (BIA)的目标是确定以下哪一个?
A)业务恢复的成本效益
B)安装软件安全修补程序的成本效益
C)恢复和最大可容忍停机时间(MTD)的资源优先级
D)应执行哪些安全措施
答案:C
解析:

18.[单选题]下列哪个问题是可能产生的物理和环境的情况？
A)输入代码是定期更改的吗？
B)有安装和燃烧火焰的燃烧设备吗？
C)确保未经授权的个人无法、复制、修改或阅读各种印刷品或电子信息的吗？
D)有控制物理访问数据传输线路吗？
答案:C
解析:

19.[单选题]保留系统日志六个月或更长时间对于哪些活动可能很有价值?
A)灾后恢复和业务 连续性
B)法医和事件 反应
C)身份和授权 管理
D)物理和逻辑访问 控制
答案:B
解析:

20.[单选题]CHAP质询握手身份验证协议的最好描述是？
A)密码都以明文形式发送
B)密码不会以明文形式发送
C)没有用密码，发送数字签名
D)它是不合于密码认证协议PAP的
答案:B
解析: Passwords are not sent in clear text. The server performing the authentication sends a challenge value and the user types in the password. The password is used to encrypt the challenge value then is sent back to the authentication server.

21.[单选题]If a content management system (CSM) is implemented, which one of the following would occur?

如果实施了内容管理系统（CSM），会出现以下哪种情况?
A)The test and production systems would be riming the same software测试和生产系统将使用相同的软件
B)The applications placed into production would be secure投入生产的应用程序将是安全的
C)Developers would no longer have access to production systems开发人员将无法再访问生产系统
D)Patching the systems would be completed mere quickly修补这些系统将很快完成
答案:A
解析:

22.[单选题]根据最佳实践,在生产环境中实施第三方软件时需要以下哪一项?
A)扫描漏洞的应用程序
B)合同供应商进行 修补
C)协商最终用户应用程序 培训
D)托管软件副本
答案:A
解析:

23.[单选题]Sally 在传输模式下使用 IPSec的ESP组件。她应该了解哪些关于传输模式的重要信息?
A)传输模式提供整个IP数据包的完全加密
B)传输模式添加一个新的未加密报头,以确数据包到达其目的地
C)传输模式不加密数据包的头
D)传输模式不提供加密,只有隧道模式提供加密
答案:C
解析:ESP 的传输模式加密 IP 分组数据,但不加密数据包头部。隧道模式加密整个数据包,并添加一个新的报头以支持通过隧道的传输。
ESP's Transport mode encrypts IP packet data but leaves the packet header unencrypted.Tunnel mode encrypts the entire packet and adds a new header to support transmission through the tunnel.

24.[单选题]了解最初生成加密消息的语言可能有助于cryptanalyst执行?
A)明文攻击。
B)已知密码攻击。
C)频率分析。
D)随机评估
答案:C
解析:

25.[单选题]以下哪组控制配对注重支持访问控制目标的“软”机制?
A)预防性/物理性配对
B)检测性/行政管理性配对
C)预防性/行政管理性配对
D)预防性/技术性配对
答案:C
解析: In this pairing, emphasis is placed on "soft" mechanisms that support the access control objectives. Soft Control is another way of referring to Administrative control. Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.

26.[单选题]SSL是一个事实上的协议,用来实现在不可信的网络上安全传输。 下面哪项最好的描述了在SSL 连接建立流程上发生的情况?
A)The server creates a session key and encrypts it with a public key.
服务器创建会话密钥,并用公钥进行加密
B)The server creates a session key and encrypts it with a private key.
服务器创建会话密钥,并用私钥进行加密

C)The client creates a session key and encrypts it with a private key
客户端创建会话密钥,并用私钥进行加密
D)客户端创建会话密钥,并用公钥进行加密
答案:D
解析:略
章节：模拟考试202201

27.[单选题]一个组织已决定与基于云的服务提供商签订合同,以利用其作为服务产品的身份。他们将使用开放身份验证(OAuth) 2.0 来 验证 外部用户对组织服务的认证。
作为 authen抽搐过程的一部分,最终用户必须提供以下哪一个?
A)访问 令牌
B)用户名和 密码
C)用户名
D)密码
答案:A
解析:

28.[单选题]What type of firewall architecture employs two network cards and a single screening router?什么类型的防火墙架构采用了两块网卡和单场次路由器?
A)A dual-homed host firewall双穴主机防火墙
B)An application-level proxy server一个应用级代理服务器
C)Ascreened-subnet firewall一个屏蔽子网防火墙
D)A screened-host firewall一个屏蔽主机防火墙
答案:D
解析:与双宿主主机一样,受屏蔽主机防火墙使用两个网卡连接到可信和不可信网络,但在主机和不可信网络之间添加了一个筛选路由器。*双主主机有两个网卡,但不一定有一个筛选路由器。*screen -subnet防火墙也使用两个网卡,但有两个筛选路由器与主机Exhibit:作为代理服务器在自己的网段。一个筛选路由器控制本地网络的流量,而第二个监控和控制输入和输出的Internet流量,应用程序级代理,与这个问题无关。

29.[单选题]Refer to the information below to answer the question.A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.The organization should ensure that the third party's physical security controls are in place so that they请参阅以下信息以回答问题。一家大型跨国组织决定将其信息技术（IT）组织的一部分外包给第三方提供商的设施。该提供商将负责设计、开发、测试和支持组织使用的几个关键的、基于客户的应用程序。组织应确保第三方的物理安全控制措施到位，以便
A)are more rigorous than the original controls. 比原来的控制更严格。
B)are able to limit access to sensitive information. 能够限制对敏感信息的访问。
C)allow access by the organization staff at any time. 允许组织员工随时访问。
D)cannot be accessed by subcontractors of the third party. 第三方分包商无法访问。
答案:B
解析:

30.[单选题]对于已分类的数据，下列哪一项是最低的军事数据分类级别?
A)敏感
B)机密
C)专有
D)私有
答案:B
解析:机密，秘密，绝密

31.[单选题](04161) 点阵(lattice)模型的主要特征是：
A)最小上界和下界
B)最小上界和下界
C)最小上界和下界
D)最小上界和下界
答案:C
解析:

32.[单选题]在实施安全断言标记语言 (SAML) 时,在本地环境和外部身份提供商服务之间实现身份集成时,常见的挑战是什么?
A)某些用户未被配置到 service 中。
B)SAML 令牌由本地身份 提供商提供。
C)单个用户不能从服务中撤销 。
D)SAML令牌包含用户 信息。
答案:A
解析:

33.[单选题]哪个安全访问策略包含系统用于确定用户访问文件或对象的固定安全属性?
A)强制性访问控制 (MAC)
B)访问控制列表 (ACL)
C)自由访问控制 (DAC)
D)授权用户 控制
答案:A
解析:

34.[单选题]身份识别是指：
A)用户给系统提供共享的密钥。
B)用户对系统自称的身份。
C)用户给系统提供密码。
D)用户通过系统身份验证。
答案:B
解析:

35.[单选题]TCP猜测序列号是什么攻击?
A)窃听
B)中间人
C)DOS
D)社工
答案:B
解析:略
章节：模拟考试202201

36.[单选题]what is the main purpose of Corporate Security Policy?企业安全政策的主要目的是什么?
A)To provide a common framework for all development activities.
为所有的开发活动提供一个通用框架
B)To provide detailed steps for performing specific actions.提供执行特定操作的详细步骤
C)To communicate management's intentions in regards to information security.传达管理层关于信息安全的态度
D)To transfer the responsibility for the information security to all users of the organization.将信息安全的责任转移给组织的所有用户
答案:C
解析:

37.[单选题]第 2 层隧道协议 (L2TP) 的主要用途是隧道数据
A)通过Session层的防火墙
Through a firewall at the Session layer
B)通过传输层的防火墙
Through a firewall at the Transport layer
C)在点对点协议(PPP)中
In the Point-to-Point Protocol (PPP)
D)在有效载荷压缩协议(PCP)中
In the Payload Compression Protocol (PCP)
答案:C
解析:

38.[单选题]Most operating systems and applications allow for administrators to configure the data that will be captured in audit logs for security purposes.Which of the following is the least important item to be captured in audit logs?大多数操作系统和应用程序允许管理员配置那些为安全目的将在审计日志中捕获的数据,下列哪一项是在审计日志中被捕获的最不重要的项目?
A)System performance output data系统性能输出数据
B)Last user who accessed the device访问该设备的最后的用户
C)Number of unsuccessful access attempts不成功的访问次数
D)Number of successful access attempts成功访问次数
答案:A
解析:系统的设计方式可以保数翻的机密性、完整胜和呵可用性。阿格中包含的研究工作站来自内部用户,最大限度地降低了分发数据风险。然而,分布式计算客户端中的隔离破坏可能是灾难性的,会使得破坏了控制器的人能控制组织中每个设备。

39.[单选题]Alyssa的团队最近实施了一个新系统,该系统从各种不同的日志源收集信息,分析这些信息,然后触发自动脚本响应安全事件。什么术语最能描述这项技术?
Alyssa's team recently implemented a new system that gathers information from a variety of different log sources, analyzes that information, and then triggers automated playbooks in response to security events. What term best describes this technology?
A)SIEM
SIEM
B)日常存储库
Log repositories
C)IPS
IPS
D)SOAR
SOAR
答案:D
解析:安全信息和事件管理(SIEM)系统确实将来自多个来源的信息关联起来并执行分析,但它们无法提供自动脚本响应。这就是安全编排、自动化和响应(SOAR)平台的领域。入侵防御平台的范围更有限,允许根据IPS本身执行的分析阻止流量。日志存储库只收集日志信息,不执行分析。

40.[单选题]The ability to send malicious code, generally in the form of a client side script, to a different end user is categorized as which type of vulnerability? 向不同的最终用户发送恶意代码（通常以客户端脚本的形式）的能力被归类为哪种类型的漏洞?
A)Session hijacking会话劫持
B)Cross-site request forgery（CSRF）跨站点请求伪造（CSRF）
C)Cross-Site Scripting（XSS）跨站点脚本（XSS）
D)Command injection命令注入

答案:C
解析:

41.[单选题]A new Chief Information Officer (CIO) created a group to write a data retention policy based on applicable laws. Which of the following is the PRIMARY motivation for the policy? 新上任的首席信息官（CIO）成立了一个小组，负责根据适用法律编写数据保留策略。以下哪项是该政策的主要动机？
A)To back up data that is used on a daily basis备份每天使用的数据
B)To dispose of data in order to limit liability处置数据以限制责任
C)To reduce costs by reducing the amount of retained data通过减少保留的数据量来降低成本
D)To classify data according to what it contains根据数据包含的内容对数据进行分类
答案:B
解析:

42.[单选题]哪个联邦机构有责任确保不用于处理敏感和/或机密信息的政府计算机系统的安全？
A)美国国家安全局
B)美国联邦调查局
C)美国国家标准与技术研究员
D)美国特工处
答案:C
解析:美国国家标准与技术研究员 NIST

43.[单选题]网卡设置了混合模式,但只收到自己的网络信息?
A)防火墙禁止嗅探
B)网络使用交换机连接模式
C)网络使用集线器
D)当前没有通讯数据
答案:B
解析:略
章节：模拟考试202201

44.[单选题]Ben 所在的组织有一个传统的现场 ActiveDirectory环境,该公司有350名员工,每增加一名员工都需要进行手动配置。随着公司采用新技术,他们越来越多地使用软件即服务应用程序来替换其内部开发的软件堆栈。
Ben 的任务是设计一个身份管理系统,该系统允许公司使用云服务,同时应该支持现有的系统。使用给出的逻辑图,回答关于以下问题。
当 Ben 的组织向他们的电子商务云合作伙伴提供验证和授权时,可能会涉及哪些技术?
A)ActiveDirectory
B)SAML
C)RADIUS
D)SPML
答案:B
解析:安全声明标记语言(SAML)经常用于集成云服务,并允许进行身份验证和授权声明。Active Directory的集成是可能的,但云服务提供者很少提供该项服务,并且 RADIUS(远程用户拨号身份验证系统)并非专门用于这样的集成。服务配置标记语言(SPML)用于配置用户、资源和服务,而不用于身份验证和授权。
Security Assertion Markup Language (SAML) is frequently used to integrate cloud services and provides the ability to make authentication and authorization assertions. Active Directory integrations are possible but are less common for cloud service providers, and RADIUS is not typically used for integrations like this.

45.[单选题]来自威胁的年预期损失怎么计算？
A)年发生率X(单一损失预期-暴露因子)
B)资产价值X暴露因子

C)单一预期损失/暴露因子
D)单一预期损失X年发生率
答案:D
解析:

46.[单选题]Diffie-Hellman 算法是用于?
A)加密
B)数字签名
C)密钥交换
D)抵不可依赖性
答案:C
解析: Diffie Hellman 是一种密钥交换算法，其优势在于计算的难度
由大主数生成的有限域中的离散对数。虽然RSA和
Diffie Hellman在数学理论上相似，但它们的实现方式有些
不同。该算法已向公众发布。
它是用于密钥交换的
 RSA 算法的主要替代方案。

47.[单选题]在应用开发过程中的软件担保(software assurance)用于?
A)防止产生易受攻击的软件
B)鼓励开发开源软件
C)有助于生成可信计算基(TCB)系统
D)有助于生成高可用性的系统
答案:A
解析:略
章节：模拟考试202201

48.[单选题]SDN 实现的哪一层使用程序通过 API 来传达对资源的需求?
A)数据平面
B)控制平面
C)应用平面
D)监控平面
答案:C
解析:软件定义网络 (SDN) 的应用程序平面是应用程序运行的地方,这些应用程序使用应用程序编程接口 (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。

49.[单选题]有两个以上执行域或特权级别的体系结构被称为：
A)环结构
B)环分层
C)网络环境
D)安全模型
答案:A
解析: In computer science, hierarchical protection domains, often called protection rings, are a
Mechanism to protect data and functionality from faults (fault tolerance) and malicious
Behavior (computer security). This approach is diametrically opposite to that of capability
Based security.

50.[单选题]在为灾备中心选址时,影响最小的因素是?
A)经过飞机航线的区域
B)所在地区的犯罪发生率