网络安全等级测评师（中级）考核试题

一、判断题

1、通过白名单方式绑定无线接入终端设备的 MAC 地址，则认为对参与无线通信的设备进行了身份鉴别。 [判断题] *

对

错 √

2、发电厂的不同机组之间的网络边界可以不采取入侵防范措施。 [判断题] *

对 √

错

3、安全事件的可能性，由资产价值和脆弱性决定。 [判断题] *

对

错 √

4、针对第三级等级保护对象进行测评时，测评对象在数量上抽样，种类上全部覆盖。 [判断题] *

对

错 √

5、测评记录中应明确记录测评方法和证据来源，记录必要的对象特征和细节描述，应提供充分的符合性判定依据。 [判断题] *

对 √

错

6、作为云租户的测评委托单位全部职责包括：测评前备份系统和数据，并了解测评工作基本情况；协

助测评机构获得现场测评授权；安排测评配合人员,配合测评工作的开展；对风险告知书进行签字确认；配合人员如实回答测评人员的问询，对某些需要验证的内容上机进行操作，协助测评人员实施工具测试并提供有效建议，降低安全测评对系统运行的影响，完成业务相关内容的问询、验证和测试，对测评证据和证据源进行确认，确认测试后被测设备状态完好。 [判断题] *

对

错 √

7、ISO/IEC 27000 标准族中的核心标准包括 ISO/IEC 27001 《信息安全管理体系-要求》、ISO/IEC 27002 《信息安全管理实用规则》。 [判断题] *

对 √

错

8、安全区域边界对象主要根据系统中网络访问控制设备的部署情况来确定。 [判断题] *

对

错 √

9、安全区域边界如果以串接方式部署了访问控制设备，并启用了合理的访问控制策略，则可认为“跨越边界的访问和数据流通过边界设备提供的受控接口进行通信”。 [判断题] *

对

错 √

10、只有在边界访问控制设备访问控制规则最后一条为全拒绝时，才认为该边界“默认情况下除允许通信外受控接口拒绝所有通信”。 [判断题] *

对

错 √

11、防病毒网关能够对通过的所有应用协议进行恶意代码检测和防护。 [判断题] *

对

错 √

12、交换机在收到未知源地址的帧时直接丢弃。 [判断题] *

对 √

错

13、可信验证的目标是保证系统和应用的信息不被非授权对象访问。 [判断题] *

对

错 √

14、密码协议指两个或两个以上参与者使用密码算法，为达到加密保护或安全认证目的而约定的交互规则。 [判断题] *

对 √

错

15、SSL VPN 主要用于数据发送者的不可否认性。 [判断题] *

对

错 √

16、侧信道攻击是利用密码的物理实现过程获取的信息进行的攻击，而不是利用算法的理论弱点或者进行穷举攻击。 [判断题] *

对 √

错

17、WindowsXP 的密码存放在系统所在的 下 HOST 文件中。 [判断题] *

对

错 √

18、网络安全核心目标 CIA 每个字母分别代表机密性、完整性、可用性。 [判断题] *

对 √

错

19、根据网络安全等级保护第四级测评要求，验证移动应用软件管理策略的有效性，应核查系统中对移动应用软件配置的管理策略是否合理，并检查是否存在多余或者过期规则。 [判断题] *

对 √

错

二、选择题

1、综合得分单项基准分的计算方式为 。() [单选题] *

A.100/ 要求项总数

B.100/ 适用项总数 √

C.100/ 测评单项总数

D.100/ 测评且适用的单项总数

2、测评对象选取的说法正确的是。() [单选题] *

A.相同配置设备：一、二级 1 台；三、四级 2 台

B.相同配置设备：一级 1 台；二级 2 台；三、四级 3 台

C.相同配置设备：所有级别 2 台

D.相同配置设备：一级 1 台；二、三级 2 台；四级 3 台 √

3、依据 GB/T 22239 ，应采用密码技术保证重要审计数据的 。() [单选题] *

A.保密性

B.可用性

C.完整性 √

D.一致性

4、某业务系统收集了用户的身份证号，应采用 密码技术进行加密存储。（）[单选题] *

A.MD5

B.RSA 1024

C.DES

D.SM4 √

5、等级测评风险主要包括 。（）[单选题] *

A.影响系统正常运行的风险

B.敏感信息泄露风险

C.木马植入风险

D.以上都是 √

6、 是项目管理中最重要的角色，是由执行组织委派，领导团队实现项目目标的个人。（）[单选题] *

A.项目经理 √

B.技术专家

C.项目专家

D.单位领导

7、关于访谈、核查和测试三种测评方法，以下说法正确的是 。（）[单选题] *

A.针对单项测评，只需要使用一种测评方法；

B.访谈应全面，尽量发散性提出问题，以获得更多更具体的证据；

C.测试包括功能测试、性能测试和渗透测试等； √

D.核查即针对制度文档进行观察和分析。

8、如果客户想要一个可完全操作得环境，需要很少的维护或管理，那么哪种云服务模型可能是最好的。（）[单选题] *

A.IaaS

B.PaaS

C.SaaS √

D.混合云

9、以下哪项不适合纳入 SLA? （）[单选题] *

A.指定时段允许的用户账户数量

B.云服务商和云服务客户双方都有哪些人员负责和授权宣布紧急情况，并将服务转换到应急允许状态 √

C.允许云服务商和云服务客户之间传输和接收的数据量

D.从正常操作转换到应急操作允许的时间

10、下列哪一项是 RFID 的逻辑安全机制。（）[单选题] *

A.Kill 命令机制

B.干扰

C.散列锁定 √

D.阻塞标签

11、物联网的核心技术是 。（）[单选题] *

A.射频识别 √

B.集成电路

C.无线电

D.操作系统

12、以下哪一项不属于工具测试的作用。（）[单选题] *

A.完成对信息系统的授权模拟攻击，发现系统安全性方面的问题 √

B.可以直接获得目标系统本身存在的操作系统、应用方面的漏洞

C.通过在不同区域接入测试工具得到的测试结果，判断不同区域之间的访问控制情况

D.与其他核查手段结合，为测试结果的客观性和准确性提供保证

13、以下哪一项不属于工具测试的流程。（）[单选题] *

A.收集目标系统信息

B.规划接入点

C.现场测试

D.漏洞发现 √

14、对于动态开放端口的应用协议（如 OPC 协议），如何实现安全的访问控制?（）[单选题] *

A. 通过限定源目的地址为单个 IP 地址，并配置目的端口为“任意”的策略来保障动态开放端口的协议数据流可通过访问控制设备

B. 通过抓包分析该协议通信的端口使用情况，再以最小开放方式人工配置五元组策略

C. 访问控制设备分析通信过程中的端口协商数据包，后台自动以最小开放方式配置五元组策略 √

D. 配置全通策略，保障动态开放端口协议通信可用性

15、《中华人民共和国密码法》施行时间？（）[单选题] *

A.2019 年 10 月 26 日

B.2020 年 1 月 1 日 √

C.2020 年 5 月 1 日

D.2021 年 1 月 1 日

16、以下_____算法被国家密码管理局警示是有风险的算法。（）[单选题] *

A.MD5

B.SHA-1

C.DES

D.以上都是 √

17、从一张数字证书无法得到_____信息。（）[单选题] *

A.证书用途

B.主体公钥信息

C.有效日期

D.证书签发机构公钥信息 √

18、《密码法》中所称的密码，是指采用特定变换的方法对信息进行____、____的技术、产品和服务。（）[单选题] *

A.机密性保护、完整性保护

B.加密解密、签名验签

C.加密保护、安全认证 √

D.标识、认证

19、我国密码标准定义的杂凑密码是_____。（）[单选题] *

A.SHA256

B.SM2

C.SM3 √

D.SM4

20、以 GM/T 开头的标准，属于_____。（）[单选题] *

A. 密码国家标准

B. 密码行业标准 √

C. 密码企业标准

D. 密码地方标准

21、下面关于密码设计原则中不正确的是。（）[单选题] *

A.算法公开，密钥保密

B.算法不能公开，密钥可以公开 √

C.算法应能抵御已知的攻击

D.算法应尽可能提高运算效率

22、下面密码算法中，哪一个不属于商用密码算法？（）[单选题] *

A. SM2

B. SM3

C. DES √

D. SM4

23、Oracle 数据库中，以下_____命令可以删除整个表中的数据，并且无法回滚。（）[单选题] *

A.Drop

B.Delete

C.Truncate √

D.Cascade

24、应保证移动终端_____、_____并_____终端管理客户端软件。（）[单选题] *

A.管理、注册、卸载

B.安装、运行、卸载

C.安装、注册、运行 √

管理、注册、运行

25、移动终端应接受移动终端管理服务端的_____管理、设备远程控制，如：远程锁定、远程擦除等。

（）[单选题] *

A. 全功能

B. 设备硬件接口

C.策略

D.设备生命周期

三、多选题

1、MES 系统等级测评需要增加的工业控制安全扩展部分要求有 。（） [多选题] *

A.安全通信网络 √

B.安全区域边界 √

C.安全计算环境

D.安全管理中心

2、“访谈”方法应用时，应注意以下要求。（） [多选题] *

A.访谈不能有诱导性 √

B.问题应具有开放性 √

C.访谈所获取的结论性内容主要作为实证

D.优先采用访谈测评方法

3、密码是目前世界上公认的，保障网络与信息安全 的关键核心技术。（） [多选题] *

A.最有效 √

B.最可靠 √

最经济

D.最实用

4、以下属于对称密码算法的是。（） [多选题] *

A.ZUC 算法 √

B.RSA 算法

C.SM4 算法 √

D.DES 算法 √

5、在等级测评过程中可以通过采取以下措施规避风险。（） [多选题] *

A.签署委托测评协议 √

B.签署保密协议 √

C.签署现场测评授权书 √

D.验证测试避开业务高峰期 √

6、云计算等级测评实施时，测评对象确定还需考虑以下方面。（） [多选题] *

A.虚拟设备 √

B.云操作系统、云业务管理平台、虚拟机监视器 √

C.云服务客户网络控制器 √

D.云应用开发平台 √

7、等级测评方法主要包括。（） [多选题] *

A.访谈 √

B.核查 √

C.测试 √

D.交流

、根据 GB/T 22240-2020　给出的定级对象基本特征和 GB/T 35589-2017　给出的大数据参考架构，大数据相关等级保护对象可以抽象为 等组件。（）［多选题］*

A.大数据资源

B.大数据管理平台

C.大数据应用 √

D.大数据平台 √

9、以下属于大数据应用的是。（）［多选题］*

A.文字搜索系统 √

B.翻译系统 √

C.邮件系统

D.产品推送广告系统 √

10、项目具有的特性有 。（）［多选题］*

A.独特性 √

B.临时性

C.复杂性 √

D.渐进明细 √

11、一般项目的制约因素有 ，除了这四大主要因素外，还需要考虑风险、资源和干系人等。（）［多选题］*

A.质量 √

B 范围 √

C.成本 √

D.进度 √

、项目管理是指在项目活动中运用专门的 ，使项目能够在有限资源限定条件下，实现或超过设定的需求和期望的过程。() [多选题] *

A.知识

B.技能 √

C.工具 √

D.方法 √

13、相较于 2019 版等级测评报告模板，2021 版等级测评报告模板的主要修订内容包括 。() [多选题] *

A.将数据作为独立测评对象 √

B.删除控制点得分计算 √

C.调整综合得分计算公式 √

D.规范了等级测评结论扩展表 √

14、针对二级以上云租户系统，以下可以判定为高风险的场景包括 。() [多选题] *

A.云计算平台承载高于其安全保护等级(SxAxGx)的业务应用系统

B.业务应用系统部署在低于其安全保护等级(SxAxGx)的云计算平台上 √

C.业务应用系统部署在未进行等级保护测评的云计算平台上 √

D.业务应用系统部署在测评报告超出有效期的云计算平台上 √

15、依据 GB/T 28448-2019 测评要求，等级保护第三级重要数据传输过程的保密性，所涉及的测评对象主要为哪些 。() [多选题] *

A. 业务应用系统 √

B. 数据库管理系统 √

C. 中间件和系统管理软件 √

交换机

16、依据 GB/T 28448-2019　测评要求，等级保护第三级身份鉴别第一条关于用户身份及身份鉴别信息的要求，测评实施内容主要包括哪些 。（）［多选题］*

A. 应核查用户在登录时是否采用了身份鉴别措施

B. 应核查用户列表确认用户身份标识是否具有唯一性 √

C. 应核查用户配置信息或测试验证是否不存在空口令用户 √

D. 应核查用户鉴别信息有复杂度要求并定期更换 √

17、以下哪些产品可以实现数据的集中审计和分析。（）［多选题］*

A.SOC（安全运营中心） √

B.日志分析系统 √

C.网络安全态势感知系统 √

D.SIEM（安全信息和事件管理） √

18、基于 IaaS 模式，云服务商实现自身控制部分的集中监测，可以包括 。（）［多选题］*

A.租户应用

B.租户网络

C.虚拟机使用情况 √

D.物理机使用情况 √

19、基于 IaaS 模式，云服务客户实现自身控制部分的集中监测，可以包括 。（）［多选题］*

A.租户应用 √

B.租户网络 √

C.虚拟机使用情况 √

D.物理机使用情况