网络与信息安全管理员（四级）样卷 B

一、判断题（共 40 题；共 20 分）

1.（0.5 分）CMVP(CryptographicModuleValidationProgram)评估需要为模块改进提供帮助

正确

错误

标准答案：正确

2.（0.5 分）ISO/IEC21827 将安全工程服务提供者的能力划定为四个级别

正确

错误

标准答案：错误

3.（0.5 分）密码技术标准工作组(WG3)，研究提出商用密码技术标准体系；研究制定商用密码算法、商用密码模块和商用密钥管理等相关标准。

正确

错误

标准答案：正确

4.（0.5 分）信息安全标准体系与协调工作组(WG1)，研究信息安全标准体系；跟踪国际标准发展动态。

正确

错误

标准答案：正确

5.（0.5 分）关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行 2 次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门

正确

错误

标准答案：错误

6.（0.5 分）自主访问控制是基于请求者的身份以及访问规则来进行访问控制的。自主访问控制的安全性相对较低

正确

错误

标准答案：正确

7.（0.5 分）信息系统安全风险评估是指由于系统存在的脆弱性，人为或自然的威胁导致安全事件发生所造成的影响

正确

错误

标准答案：错误

8.（0.5 分）风险评估是采用适当的方法与工具确定威胁利用脆弱性导致信息系统灾难发生的可能性。

正确

错误

标准答案：错误

9.（0.5 分）关于建立有效的计算机病毒防治体系，使用技术机制是收集信息的主要渠道之一

正确

错误

标准答案：正确

10.（0.5 分）当发生一般的网络安全事件或威胁，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但可能对个别公民、法人或其他组织的利益造成损害，应发布蓝色预警，特别轻微的可以不发布预警

正确

错误

标准答案：正确

11.（0.5 分）在网络安全保护对象可能受到损害的程度方面。较大的损害，是指可能造成或已造成网络或信息系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除负面影响所需付出的代价较小

正确

错误

标准答案：错误

12.（0.5 分）判定网络安全保护对象的重要程度宜综合考虑其所服务的用户量、日活跃用户数、交易额、信息安全等级保护的级别、数据敏感程度等因素

正确

错误

标准答案：正确

13.（0.5 分）在重要信息系统中发生的最大级别事件为特别重大事件

正确

错误

标准答案：错误

14.（0.5 分）在电子系统和计算机系统中，固件一般指持久化的内存、代码和数据的结合体。

正确

错误

标准答案：正确

15.（0.5 分）针对侧信道攻击（利用非通信信道物理信息如能量消耗变化、电磁辐射变化进行分析攻击），尽管学术界和工业界提出了很多防御技术，但是目前尚无能够抵抗所有攻击方法的防御技术。

正确

错误

标准答案：正确

16.（0.5 分）为了分析密码模块能量消耗的变化，二阶/高阶 DPA(DifferentialPowerAnalysis，差分能量分析)使用了统计方法(如均值差、相关系数)对能量消耗进行统计分析，从而获取密钥值。

正确

错误

标准答案：错误

17.（0.5 分）传导干扰，主要是电子设备产生的干扰信号通过导电介质或公共电源线互相产生干扰。

正确

错误

标准答案：正确

18.（0.5 分）计算机电磁辐射干扰器大致可以分为两种：白噪声干扰器和相关干扰器。

正确

错误

标准答案：正确

19.（0.5 分）TEMPEST 技术（TransientElectroMagneticPulseEmanationStandard，瞬态电磁辐射标准），是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取防辐射措施，从而达到减少计算机信息泄漏的最终目的。

正确

错误

标准答案：正确

20.（0.5 分）屏蔽室是一个导电的金属材料制成的大型六面体，能够抑制和阻挡电磁波在空气中传播。

正确

错误

标准答案：正确

21.（0.5 分）代码签名基于 PKI 体系，包括签名证书私钥和公钥两部分，私钥用于代码的签名，公钥用于签名的验证。

正确

错误

标准答案：正确

22.（0.5 分）PKI 是利用公开密钥技术所构建的、解决网络安全问题的、普遍适用的一种基础设施。PKI 利用非对称的算法，提供密钥协商能力

正确

错误

标准答案：正确

23.（0.5 分）随着大数据和云计算技术的发展，网络的匿名性将逐渐消失。

正确

错误

标准答案：错误

24.（0.5 分）在信息安全等级保护实施中，安全运行维护阶段是对信息系统的过时或无用部分进行报废处理的过程，主要涉及对信息、设备、存储介质或整个信息系统的废弃处理

正确

错误

标准答案：错误

25.（0.5 分）GB/T28448－2012《信息安全技术信息系统安全等级保护测评要求》阐述了等级测评的原则、测评内容、测评强度、单元测评要求、整体测评要求、等级测评结论的产生方法等内容，用于规范和指导测评人员如何开展等级测评工作。

正确

错误

标准答案：正确

26.（0.5 分）网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

正确

错误

标准答案：正确

27.（0.5 分）《计算机信息系统安全保护等级划分准则》是强制性国家标准，是等级保护的基础性标准。

正确

错误

标准答案：正确

28.（0.5 分）信息的时效性与可利用价值成反比

正确

错误

标准答案：错误

29.（0.5 分）组织信息是一种物质形态的社会财富，可以划分为组织内部信息和组织外部信息。

正确

错误

标准答案：错误

30.（0.5 分）安装了防火墙等访问控制设备之后，计算机系统就没有可能被黑客突破。

正确

错误

标准答案：错误

31.（0.5 分）任何个人和组织不得窃取个人信息，不得非法出售或者非法向他人提供个人信息，但是可以以其他方式获得。

正确

错误

标准答案：错误

32.（0.5 分）监视全网运行和安全告警信息是系统管理员的主要职责之一

正确

错误

标准答案：错误

33.（0.5 分）在系统日常运行及发生信息网络安全事件时，单位、组织可能需要一些公共基础设施方面的支持。

正确

错误

标准答案：正确

34.（0.5 分）实现自然人身份识别的电子信息和涉及该自然人隐私的信息都可以电子化并通过网络存储、使用和处理。

正确

错误

标准答案：正确

35.（0.5 分）信息安全连续性控制措施与一般信息安全测试和验证相似，应在变更测试外执行。

正确

错误

标准答案：错误

36.（0.5 分）应制定面向全员的信息安全意识的教育计划和措施(如发行信息安全简报)以及针对不同岗位的信息安全知识和技能的培训计划和措施(如培训信息安全管理体系内审员)

正确

错误

标准答案：错误

37.（0.5 分）政府、工业和公众都依赖密码技术来为电子商务、关键设施和其他应用领域中的信息和通信提供保护。在产品和系统中使用密码模块(包含密码算法)来提供机密性、完整性、鉴别等安全服务

正确

错误

标准答案：正确

38.（0.5 分）业务一致性管理是指为保护组织的利益、声誉、品牌和价值创造活动，找出对组织有潜在影响的威胁，提供建设组织有效反应恢复能力的框架的整体管理过程。

正确

错误

标准答案：错误

39.（0.5 分）业务连续性管理框架中，确定 BCM 战略是指通过演练证明 BCM 的计划是有效的，并不断地维护，保持更新。

正确

错误

标准答案：错误

40.（0.5 分）我国密码行业标准 GM/T0028－2014 规定的安全要求涵盖了有关密码模块的安全设计、实现、运行与废弃的安全元素(域)。

正确

错误

标准答案：正确

二、单选题（共 60 题；共 60 分）

41.（1 分）以下哪一项不是动态分析调试技术的优点？

A.执行速度较快、效率高

B.无需创建认为导致错误的场景

C.支持跟踪软件中可能引起安全混乱的细微逻辑错误

D.无需访问软件真正的源代码

标准答案：A

42.（1 分）下列哪个是识别是否发生系统攻击所必须的？

A.分布式防病毒系统

B.状态检测防火墙

C.被动式蜜罐

D.日志分析

标准答案：D

43.（1 分）在数据管理中，对于重要的数据应该进行全生命周期的管理，除加强审计监控外，以下哪项技术也有助于对数据的生命周期进行追踪？

A.漏扫技术

B.脱敏技术

C.加密技术

D.水印技术

标准答案：D

44.（1 分）以下哪个在邮件附件后缀中出现的扩展名最有可能是病毒？

A..ppt.exe

B..com.vbs.txt

C..wmv.bat

D..doc

标准答案：A

45.（1 分）对保护数据来说，哪种软件更为重要

A.备份软件

B.网络软件

C.数据库软件

D.系统软件

标准答案：A

46.（1 分）《计算机病毒防治管理办法》不包括{input}

A.建立了计算机病毒防治体系

B.明确规定了禁止行为

C.明确规定了计算机信息系统使用单位的职责

D.赋予公安机关管理职责

标准答案：A

47.（1 分）关于秘钥管理,下列说法错误的是:

A.科克霍夫原则指出算法的安全性不应基于算法的保密,而应基于秘钥的安全性

B.保密通信过程中,通信方使用之前用过的会话秘钥建立会话,不影响通信安全

C.秘钥管理需要考虑秘钥产生、存储、备份、分配、更新、撤销等生命周期过程的每一个环节

D.在网络通信中，通信双方可利用 Diffie-He11man 协议协商出会话秘钥

标准答案：B

48.（1 分）下列对网络认证协议(Kerberos)描述正确的是：

A.该协议使用非对称密钥加密机制

B.密钥分发中心由认证服务器、票据授权服务器和客户机三个部分组成

C.该协议完成身份鉴别后将获取用户票据许可票据

D.使用该协议不需要时钟基本同步的环境

标准答案：C

49.（1 分）以下关于直接附加存储(DirectAttachedStorage,DAS)说法错误的是:

A.DAS 能够在服务器物理位置比较分散的情况下实现大容量存储是一种常用的数据存储方法

B.DAS 实现了操作系统与数据的分离,存取性能较高并且实施简单

C.DAS 的缺点在于对服务器依赖性强,当服务器发生故障时,连接在服务器上的存储设备中的数据不能被存取

D.较网络附加存储(NetworkAttachedStorage,NAS),DAS 节省硬盘空间,数据非常集中,便于对数据进行管理和备份

标准答案：D

50.（1 分）关于业务连续性计划(BCP)以下说法最恰当的是:

A.组织为避免所有业务功能因重大事件而中断,减少业务风险而建立的控制过程;

B.组织为避免关键业务功能因重大事件而中断,减少业务风险而建立的一个控制过程;

C.组织为避免所有业务功能因各种事件而中断,减少业务风险而建立的一个控制过程;

D.组织为避免信息系统功能因各种事件而中断,减少信息系统而建立的一个控制过程。

标准答案：B

51.（1 分）关于源代码，描述错误的是（）

A.源代码审核有利于发现软件编码中存在的安全问题

B.源代码审核过程遵循 PDCA 模型

C.源代码审核方式包括人工审核和工具审核

D.源代码审核工具包括商业工具和开源工具

标准答案：B

52.（1 分）在软件保障成熟度模型(SoftwareAssuranceMaturityMode,SAMM)中,规定了软件开发过程中的核心业务功能,下列哪个选项不属于核心业务功能:

A.治理,主要是管理软件开发的过程和活动

B.构造,主要是在开发项目中确定目标并开发软件的过程与活动

C.验证,主要是测试和验证软件的过程与活动

D.购置,主要是购买第三方商业软件或者采用开源组件的相关管理过程与活动

标准答案：D

53.（1 分）在业务持续性方面，如果要求不能丢失数据，则：

A.RT0 为 0

B.RPO 为 O

C.RTO 和 RPO 都为 O

D.和 RTO、RPO 没有关系

标准答案：C

54.（1 分）某电子商务网站在开发设计时，使用了威胁建模方法来分折电子商务网站所面临的威胁，STRIDE 是微软 SDL 中提出的威胁建模方法，将威胁分为六类，为每一类威胁提供了标准的消减措施，Spoofing 是 STRIDE 中欺骗类的威胁，以下威胁中哪个可以归入此类威胁?

A.网站竞争对手可能雇佣攻击者实施 DDoS 攻击，降低网站访问速度

B.网站使用 http 协议进行浏览等操作,未对数据进行加密,可能导致用户传输信息泄露,例如购买的商品金额等

C.网站使用 http 协议进行浏览等操作，无法确认数据与用户发出的是否一致，可能数据被中途篡改

D.网站使用用户名、密码进行登录验证，攻击者可能会利用弱口令或其他方式获得用户密码，以该用户身份登录修改用户订单等信息

标准答案：D

55.（1 分）电子认证服务提供者签发认证证书内容不必须包括以下哪一项：

A.电子认证服务提供者名称，证书持有人名称

B.证书序列号，证书有效期

C.证书使用范围

D.电子认证服务提供者的电子签名

标准答案：C

56.（1 分）以某政府机构委托开发商开发了一款 OA 系统，其中公文分发模块使用了 FTP 协议，系统上线后被黑客利用 FTP 漏洞进行了攻击，对脚本文件进行了篡改，安全专家建议使用 HTTPS 协议代替 FTP 实现公文分发功能，该安全问题的产生主要是在以下哪个开发阶段产生的（）

A.程序员在进行安全需求分析时，没有分析出 OA 系统开发的安全性需求

B.程序员在软件设计时，没遵守降低攻击面的原则，设计了不安全的功能

C.程序员在软件编码时，缺乏足够的经验，编写了不安全的代码

D.程序员在进行软件测试时，没有针对软件安全需求进行安全测试

标准答案：A

57.（1 分）关于标准，下面哪项理解是错误的（）

A.标准是在一定范围内为了获得最佳秩序，经协商一致制定并由公认机构批准，共同重复使用的一种规范性文件，标准是标准化活动的重要成果

B.国际标准是由国际标准化组织通过并公开发布的标准。同样是强制性标准，当国家标准和国际标准的条款发生冲突时，应以国际标准条款为准

C.行业标准是针对没有国家标准而又需要在全国某个行业范围内统一的技术要求而制定的标准。同样的强制性标准，当行业标准和国家标准的条款发生冲突时，应以国家标准为准

D.地方标准由省、自治区、直辖市标准化行政主管部门制定，并报国务院标准化行政主管部门和国务院有关行政主管部门备案，在公布国家标准之后，该地方标准即应废止

标准答案：B

58.（1 分）小赵是某大学计算机科学与技术专业的毕业生，在前往一家大型企业应聘时，面试经理要求他给出该企业信息系统访问控模型的设计思路。如果想要为一个存在大量用户的信息系统实现自主访问控制功能，在以下选项中，从时间和资源消耗的角度，下列选项中他应该采取的最合适的模型或方法是（）

A.访问控制列表（ACL）

B.能力表（CL）

C.BLP 模型

D.Biba 模型

标准答案：A

59.（1 分）在应急处置中，()的目标是把所有被攻破的系统和网络设备彻底地还原到它们正常的任务状态

A. 检测

B. 根除

C. 恢复

D. 回顾总结

标准答案：C

60.（1 分）在网络安全预警分级中，用户量亿级或日活跃用户千万级的互联网重要应用属于()

A. 一般重要的保护对象

B. 重要的保护对象

C. 特别重要的保护对象

D. 不需要保护的对象

标准答案：C

61.（1 分）网络安全预警的分级主要考虑两个要素：网络安全保护对象的重要程度与()

A. 网络安全保护对象可能受到损害的程度

B. 网络安全保护对象的复杂程度

C. 网络安全保护对象的采购成本

D.网络安全保护对象的承载用户数量

标准答案：A

62.（1 分）信息基础设施风险评估工具包括()和渗透性测试工具

A.脆弱点评估工具

B.渗透性评估工具

C.脆弱点测试工具

D.系统评估工具

标准答案：A

63.（1 分）安全风险计算模型包含()、脆弱性、威胁等关键要素

A.信息资产

B.安全措施

C.风险

D.残余风险

标准答案：A

64.（1 分）风险评估要素关系模型中，业务战略依赖于()去完成

A.风险

B.残余风险

C.脆弱性

D.资产

标准答案：D

65.（1 分）根据破坏程度进行分类，计算机病毒可以分为()和恶性计算机病毒两类

A.初级计算机病毒

B.良性计算机病毒

C.工业控制系统病毒

D.手机病毒

标准答案：B

66.（1 分）组织应合理地设立分权岗位，建立包括物理的和()的系统访问权限管理制度

A. 虚拟

B. 逻辑

C. 网络

D. 数据

标准答案：B

67.（1 分）在录用信息安全人员时，应在签订《劳动合同》的同时签订()

A. 奋斗者协议

B. 专业培训协议

C. 高级培训协议

D. 劳动合同补充协议

标准答案：D

68.（1 分）信息资源的()直接决定了接触和管理该信息资源的岗位对人员安全等级的要求

A. 可信度

B. 密级

C. 可靠性

D. 来源

标准答案：B

69.（1 分）应用开发管理员的主要职责不包括()

A. 对系统核心技术保密等

B. 不得对系统设置后门

C. 系统投产运行前，完整移交系统相关的安全策略等资料

D. 认真记录系统安全事项，及时向信息安全人员报告安全事件

标准答案：D

70.（1 分）计算机安全的目的是确保信息系统资产(包括硬件、软件、固件和被处理、存储和通信的信息)的()、完整性和可用性

A.共享性

B.保密性

C.可压缩

D.可识别

标准答案：B

71.（1 分）代码签名技术能够保证软件发布者身份的合法性。一个基本的签名过程不包括()。

A.应用发布者向 CA 申请数字证书。

B.发布者开发出代码，先计算代码 Hash 值，然后采用签名工具和自己的私钥对该 Hash 值签名，从而生成一个包含软件代码、发布者证书、代码签名的软件包。

C.用户通过各种途径获取软件包，并验证证书的有效性。

D.用户验证结束以后更新数字证书。

标准答案：D

72.（1 分）张三触犯了侵犯公民个人信息罪，因侦查需要收集他的聊天记录，则应当由()以上侦查人员进行。

A.两名

B.三名

C.四名

D.五名

标准答案：A

73.（1 分）以下属于电子数据的是()

A.李磊与好友的 qq 聊天记录

B.某故意伤害案中以数字化形式记载的被告人供述

C.某互联网公司 CEO 在其员工即将出版著作序言上的签名

D.知名大学教授在研讨会上就“辱母案”发表的法学言论

标准答案：A

74.（1 分）下列不属于受保护的个人电子数据是()。

A.医院在线挂号信息

B.电子邮件的收件人

C.登录网购网站的姓名和密码

D.某明星的实名微博认证

标准答案：D

75.（1分）以下关于LTLM值“Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23AA724774CE6CC:::”说法不正确的是

A.该值的NT值为C8825DB10F2590EAAAD3B435B51404EE

B.该值的LM值为C8825DB10F2590EAAAD3B435B51404EE

C.该用户为admin

D.该pid为1

标准答案：A

76.（1分）浏览网页时，弹出“最热门的视频聊天室”的页面，遇到这种情况，一般怎么办？_____

A.现在网络主播很流行，很多网站都有，可以点开看看

B.安装流行杀毒软件，然后再打开这个页面

C.访问完这个页面之后，全盘做病毒扫描

D.弹出的广告页面，风险太大，不应该去点击

标准答案：D

77.（1分）注册或者浏览社交类网站时，不恰当的做法是：（）

A.尽量不要填写过于详细的个人资料

B.不要轻易加社交网站好友

C.充分利用社交网站的安全机制

D.信任他人转载的信息

标准答案：D

78.（1分）账户为用户或计算机提供安全凭证，以便用户和计算机能够登录到网络，并拥有响应访问域资源的权利和权限。下列关于账户设置安全，说法错误的是：

A.禁用guest账户

B. 为常用文档添加 everyone 用户

C. 限制用户数量

D. 删除未用用户

标准答案：B

79. （1 分）收到银行号码发来的中奖信息及银行升级通知修改密码并给有相关链接地址应该怎么做（）

A. 反正也没什么影响点开链接看看怎么回事

B. 核对电话号码无误后点开链接

C. 拨打官方电话进行询问

D. 对该短信进行转发

标准答案：C

80. （1 分）在旅行中或出差时等办公室之外的地方使用便携电脑以下哪种使用方式不符合公司规定（）？

A. 乘飞机旅行时，将便携电脑随身携带

B. 外出时将便携电脑锁在保险柜中

C. 在候机室等公共场合打开便携电脑对保密文件办公

D. 便携电脑丢失后及时报告当地的安全部门及上级主管

标准答案：C

81. （1 分）解析漏洞修复方案中不包括（）

A. 升级中间件并打补丁

B. 检查文件内容，不允许上传带有敏感字的任何文件

C. 限制上传文件类型及上传后缀

D. 上传文件目录不设置执行权限

标准答案：B

82. （1 分）下列有关隐私权的表述,错误的是()

A. 网络时代,隐私权的保护受到较大冲击

B. 由于网络是虚拟世界,所以在网上不需要保护个人的隐私

C.虽然网络世界不同于现实世界,但也需要保护个人隐私

D.可以借助法律来保护网络隐私权

标准答案：B

83.（1 分）某网站”网站吸纳会员时要求交纳相应会费，交纳后网站就会给购买者一个会员编号和一个会员“昵称”，该购买者就正式成为网站会员。成为会员后，就可自由发展下线，收取提成，形成五五复制的上下级关系。这种行为属于（）。

A.网络钓鱼

B.网络攻击

C.网络诈骗

D.网络传销

标准答案：D

84.（1 分）以下不可以防范口令攻击的是（）

A.设置的口令要尽量复杂些，最好由字母、数字、特殊字符混合组成

B.在输入口令时应确认无他人在身边

C.定期改变口令

D.选择一个安全性强复杂度高的口令，所有系统都使用其作为认证手段

标准答案：D

85.（1 分）2014 年，互联网上爆出近几十万 12306 网站的用户信息，12306 官方网站称是通过（）方式泄露的

A.拖库

B.撞库

C.信息明文存储

D.木马

标准答案：D

86.（1 分）2010 年 7 月，某网站在网上公开了数十万份有关阿富汗战争、伊拉克战争、美国外交部相关文件，引起轩然大波，称为（）

A.维基解密

B.icloud 泄密

C.越狱

D.社会工程

标准答案：A

87.（1分）2014年2月，我国成立了（），习近平总书记担任领导小组组长。

A.中央网络安全和信息化领导小组

B.中央网络技术和信息化领导小组

C.中央网络安全和信息技术领导小组

D.中央网络信息和安全领导小组

标准答案：A

88.（1分）2014年2月27日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平2月27日下午主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。他强调，_____和_____是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。

A.信息安全、信息化

B.网络安全、信息安全

C.网络安全、信息化

D.安全、发展

标准答案：C

89.（1分）MySQL提供了非标准的命令{input}，可以建立用户并赋予其相应的权限

A.GRANT

B.INSERT

C.SELECT

D.ALTER

标准答案：A

90.（1分）信息系统验收时进行安全评估的最主要目的是：

A.发现信息系统的代码层安全隐患

B.发现信息系统的抗攻击能力

C.发现系统安全现状与建设之初安全目标的符合程度

D.发现系统安全现状与相应安全等级的差异

标准答案：C

91.（1 分）系统定期重启在信息安全方面最重要的好处是：

A.便于安装系统更新或补丁

B.将系统性能维持在最佳状态

C.清除不必要的垃圾数据

D.防止重启时出现严重故障

标准答案：D

92.（1 分）IT 部门在发现近期发生多起勒索软件病毒事件后，进行了事件分析，发现病毒主要通过邮件方式传播，那么应最先采取以下哪些措施可以最有效预防类似事件再次发生？

A.做好文件备份工作

B.发送安全提醒邮件给全体员工

C.将病毒来源邮件地址加入邮件接收黑名单列表

D.加强反病毒/垃圾邮件库更新频率

标准答案：D

93.（1 分）一个好的信息安全意识教育活动的主要目的是

A.指导信息安全部门的员工如何开展工作

B.宣传信息安全违规行为的处罚条例，从而教育员工

C.协助人员资源管理部获取所需的信息

D.激发参与者的自觉合规意识

标准答案：D

94.（1 分）Session 与 Cookie 状态之间的最大区别在于

A.类型不同

B.存储的位置不同

C.容量不同

D.生命周期不同

标准答案：B

95.（1 分）下列关于 SSL 的安全漏洞，那一项需要升级 OpenSSL 解决？

A.SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞

B.SSL3.0POODLE 攻击信息泄露漏洞

C.SSL/TLS 中间人攻击漏洞(CCS 注入)

D.MITM(Man-in-the-MiddleAttack)中间人攻击

标准答案：C

96.（1 分）下列哪个类型漏洞可用于钓鱼植入攻击？

A.永恒之蓝

B.CPU 幽灵、熔断漏洞

C.SQL 注入漏洞

D.Office 文件格式漏洞

标准答案：D

97.（1 分）为了保护网页，我们将被保护的网页分类，并放置于不同的目录下，这是为了{input}

A.便于访问

B.便于管理

C.调用方便

D.便于网站的改版

标准答案：B

98.（1 分）以下哪个不是属于 web 应用的漏洞？

A.SQL 注入

B.XSS

C.bufferoverflow

D.CRSF

标准答案：C

99.（1 分）GB/T20274.1-2006《信息系统安全保障评估框架第一部分：简介和一般模型》中描述了信息系统安全保障模型，以下关于保障要素的理解正确的是

A.信息安全人才是信息安全保障的重要因素，应加强安全保障意识教育和相关技能培训

B.安全技术是信息安全保障的主体，其他要素围绕安全技术展开

C.安全管理以人员和控制为核心，作用主要发挥在生命周期的实施交付阶段

D.工程要素阶段以安全建设为主，良好的建设方案是系统安全的根本保障

标准答案：A

100.（1 分）SHODAN 是一种专用搜索 Internet 上漏洞的搜索引擎，关于 SHODAN 可以搜索的对象，下列说法正确的是：

A.互联网上的摄像头

B.互联网上的特定类型数据库服务器

C.互联网上的无线路由器

D.皆是

标准答案：D

三、多选题（共 10 题；共 20 分）

101.（2 分）根据定级指南，信息系统安全包括哪两个方面的安全：

A.业务信息安全

B.系统服务安全

C.系统运维安全

D.系统建设安全

标准答案：A、B

102.（2 分）等级保护对象受到破坏时所侵害的客体包括的三个方面为：

A.公民、法人和其他组织的合法权益

B.社会秩序、公共利益

C.国家安全

D.个人利益

标准答案：A、B、C

103.（2 分）根据《关于信息安全等级保护的实施意见》，信息系统安全等级保护应当遵循什么原则？

A.明确责任，共同保护

B.依照标准，自行保护

C.同步建设，动态调整

D.指导监督，保护重点

标准答案：A、B、C、D

104.（2 分）关于等级保护备案，以下说法错误的是?

A.已运营(运行)或新建的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续

B.隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续

C.办理信息系统安全保护等级备案手续时，应当填写信息系统安全等级保护备案表

D.跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，由主管部门向公安部办理备案手续

E.已运营(运行)或新建的第二级以上信息系统，应当在安全保护等级确定后 60 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续

标准答案：B、D、E

105.（2 分）建立完善的计算机病毒防范制度，包括（）

A.设置专人负责计算机病毒防范工作，统一组织和实施网络的计算机病毒防范工作

B.建立计算机病毒预警机制，严格执行病毒检测及报告措施

C.建立计算机病毒预警机制，严格执行病毒检测及报告措施

D.应及时更新防病毒软件版本、杀毒引擎和病毒库

E.建立病毒监控中心，对网络内计算机感染病毒的情况进行监控

标准答案：A、B、C、D、E

106.（2 分）单点登录(SingleSignOn，简称 SSO)是目前比较流行的企业业务整合的解决方案之一。主要的单点登录协议有{input}?

A.基于 Kerberos 的单点登录协议

B.基于 FIDO 的单点登录协议

C.基于 SAML 的单点登录协议

D.基于 OpenID 的单点登录协议

E.基于 RADIUS 的单点协议

标准答案：A、C、D

107.（2 分）电子认证与身份鉴别，是指采用电子技术检验用户身份的合法性的操作，即用户通过向信息系统提供电子形式的身份信息来建立信任的过程。在该过程中，身份真实性和数据完整性是关键。针对口令的攻击方法可分为？

A.暴力破解

B.字典攻击

C.软件攻击

D.肩窥攻击

E.钓鱼攻击

标准答案：A、B、D、E

108.（2 分）以下机构、组织或个人从事攻击我国关键信息基础设施活动，造成严重后果的，依法追究法律责任（）

A.上海市某政府机构人员王五

B.主要营业地址位于美国纽约的安全机构

C.成立于台湾的某互联网提供商

D.北京某高校学生

E.某房地产大亨的独子

标准答案：A、B、C、D、E

109.（2 分）李浩从事动画设计职业，时间较为自由，2017 年 3 月 1 日拟从事网约车服务赚取外快，则他的车应该具备（）

A.价值必须在 10 万元以上

B.技术性能符合运营安全相关标准要求

C.10 座及以下乘用车

D.安装具有行驶记录功能的车辆卫星定位装置

E. 必须具有当地车牌

标准答案：B、D

110.（2 分）龙龙从事互联网广告发布工作，其发布的（）属于互联网广告

A. 在其脸书主页发布的个人照片

B. 在微信上发布的女儿跳舞的视频

C. 在搜索引擎上发布的某医院的宣传链接

D. 在网页上发布的推销化妆品的图片

E. 在 QQ 空间发布的全家照

标准答案：C、D