一、信息安全保障

1.关于我国加强信息安全保障工作的主要原则，以下说法错误的是（D）

A、立足国情，以我为主，坚持技术与管理并重

B、正确处理安全和发展的关系，以安全保发展。在发展中求安全

C、统等规划，突出重点，强化基础工作，

D、全面提高信息安全防护能力，保护公众利益，维护国家安全

2.关于信息安全保障技术框架（IATF）说法不正确的是（D）

A.分层策略允许在适当的时候采用低安全级保障解决方案以便降低信息安全保障的成

B、IATF从人、技术和操作三个层面提供一个框架实施多层保护，使攻击者即使攻破一层也无法破坏整个信息基础投施

C、允许在关键区域（例如区域边界）使用高安全级保障解决方案，确保系统安全性

D.IATF深度防御战略要求在网络体系结构的各个可能位置实现所有信息安全保障机制

3.我国信息安全保障建设包括信息安全组织与管理体制。基础设施。技术体系等方面，以下关于信息安全保障建设主要工作内容说法不正确的是（C）

A、健全国家信息安全组织与管理体制机制，加强信息安全工作的组织保障

B、建设信息安全基础设施，提供国家信息安全保障能力支撑

C、建立信息安全技术体系，实现国家信息化发展的自主创新

D、建立信息安全人才培养体系，加快信息安全学科建设和信息安全人才培养

4.下列关于信息系统生命周期中实施阶段所涉及主要安全需求描述错误的是：（B）

A、确保采购定制的设备。软件和其他系统组件满足已定义的安全要求

B、确保整个系统已按照领导要求进行了部署和配置

C、确保系统使用人员已具备使用系统安全功能和安全特性的能力

D、确保信息系统的使用已得到授权

5.进入21世纪以来，信息安全成为世界各国安全战略关注的重点，纷纷制定并颁布网络空间安全战略，但各国历史、国情和文化不同，网络空间安全战略的内容也各不相同，以下说法不正确的是（B）

A、与国家安全、社会稳定和民生密切相关的关键基础设施是各国安全保障的重点

B、美国尚未设立中央政府级的专门机构处理网络信息安全问题，信息安全管理职能由不同政府部门的多个机构共同承担

C、各国普遍重视信息安全事件的应急响应和处理

D、在网络安全战略中，各国均强调加强政府管理力度，充分利用社会资源，发挥政府与企业之间的合作关系

A208年1月2日，美因发布第54号总统令，建立国家网络安全计划（（Ccortbmt.

National cybersecurity Initiative.oc）.act 计划建立三组防线，第一道功线，减

少漏洞和隐患，预防入侵；第二道防钱，全面应对各类成胁；第三道防线，强化未来安全环境，从以上内容，我们可以看出以下源种分析是正确的（A）

A、CNCI是以风险为核心，三制线管要的任务是降低其网络所面临的风险

B、从CNCI可以看出，般胁主要总来自外部的，而漏洞和隐患主要是存在于内部的

C、CNCl的目的是尽快研发并部器新技术彻底改变其槽核的网络安全现状。而不是在现

在的网络基础上修修补补

D、CNC1彻底改变了以往的美国信息安全战略，不再把关健基础设施视为信息安全仅障重点，而是追求所有网络和系统的全面安全保障

7.美围的关键信息基础设施（criticalInformation Infrastructure，CI）包括商用设施、政府设施、交通系统、饮用水和废水处理系统、公共健康和医疗、能源、银行和金融、国防工业基地等等，美国政府强调重点保障这些基础设施信息安全，其主要原不包括（c）

A、这些行业都关系到国计民生，对经济运行和国家安全影响深远

B、这些行业都是信息化应用广泛的领域

C、这些行业信息系统普遍存在安全隐患，而且信息安全专业人才缺乏的现象比其他行业更突出

D、这些行业发生信息安全事件，会造成广泛而严重的损失

8.以下哪一项不是我国信息安全保障工作的主要目标（C）

A.保障和促进信息化发展

B.维护企业与公民的合法权益

C、构建高效的信息传播渠道

D、保护互联网知识产权

9.我国信息安全保障工作先后经历了启动、逐步展开和积极推逃以及深化落实三个阶段，

以下关于我国信息安全保障各阶段说法不正确的是（c）

A、2001年，国家信息化领导小组重组，网络与信息安全协调小组成立，我国信息安全保障工作正式启动

B、203年7月，国家信息化领导小组制定出台了《关于加强信息信息安全保障工作的意见》（中办发27号文件），明确了“积极防饰、综合防范”的国家信息安全保障工作方针

C.2003年，中办发27号文件的发布标志着我国信息安全保障进入深化落实阶段

1. 在深化落实阶段，信息安全法律法规、标准化，信息安全基础设施建设，以及信息安全等级保护和风险评估取得了新进展

10.人们开始使用防火墙、防病毒工具、公钥基础设施（Public Key Infrastructure，PK）

和虚拟专用网（Virtual Privaey Network，VPN)等安全产品，此阶段是哪个信息安全发展阶段（C）

A、通信安全

B、计算机安全

C、信息系统安全

D、信息安全保障

11.以下哪一项不是我国国务院信息化办公室为加强信息安全保障明确提出的九项重点工作内容之一（A）

A、提高信息技术产品的国产化率

B、保证信息安全资金投入

C、加快信息安全人才培养

D、重视信息安全应急处理工作

12.随着信息技术的不断发展，信息系统的重要性也越来越突出，而与此同时，发生的信息安全事件也越来越多。综合分析信息安全问题产生的根源，下面描述正确的是（c）

A、信息系统自身存在脆弱性是根本原因。信息系统越来越重要，同时自身在开发、部器和使用过程中存在的脆弱性，导致了诸多的信息安全事件发生。因此，杜绝脆弱性的存在是解决信息安全问题的根本所在

B、信息系统面临诸多黑客的威胁，包括恶意攻击者和恶作剧攻击者。信息系统应用越来越广泛，接触信息系统的人越多，信息系统越可能遭受攻击。因此，避免有恶意攻击可能的人接触信息系统就可以解决信息安全问题

C、信息安全问题产生的根源要从内因和外因两个方面两个方面分析，因为信息系统自身存在脆弱性，同时外部又有威胁源，从而导致信息系统可能发生安全事件。因此，要防范信息安全风险，需从内外因同时着手

D、信息安全问题的根本原因是内因、外因和人三个因素的综合作用，内因和外因都可能导致安全事件的发生，但最重要的还是人的因素外部攻击者和内部工作人员通过远程攻击、本地破坏和内外勾结等手段导致安全事件发生。因此，对人这个因素的防范应是安全工作重点。

13.关于信息安全保障技术框架（Information Assurance Tehnical Franewor，IATF），下面描述错误的是（A）

A、IATF最初由美国国家安全局（NSA）发布，后来由国际标准化组织（IS0）转化为国际标准，供各个国家信息系统建设参考使用

B、IATF是一个通用框架，可以用到多种应用场景中，通过对复杂信息系统进行解构和描述，然后再以此框架讨论信息系统的安全保护问题

C.IATF旷提出了观度制刻的被略思想，并提供一个概要进行多层保护。以此防范信也系统刻临的各种威物

D.强调人、技术和操作是深度动制的三个主要法面，也就是说讨论人在技术支排下送行维护的信息安全保障问题

14.2003年以来。我国高度意视信息安全保障工作，先后就定并发布了多个文件，从政策层

面为开属并推进信息安全保障工作进行了规划。下面选项中哪个不是我国发布的文件

A.《国家信息化额导小组关于加强信息安全保确工作的意见》

B.《国家网络安全综合计化（CNCI）》

C.《国家信息安全故略报告》

D.《关于大力推进信息化发展和切实保师信息安全的若干意见）

15.在信息安全保障工作中，人才是非常

重要的因素，近年来，我国一直高度重视我国信息安全人才和征的知养和建设，在以下关于我国关于人才指养工作的指料，错误的是（c）

A.在《国家信息化领导小组关于加强信息安全保障工作的意见》中，针对信息安全人才建设与培养工作提出了“加快信息安全人才培养，增强全民信息安全意识”的指导精神

B.2015年，为加快网路空间安全高层次人才培养，经报国务院学位委员会批准，国务成学位委员会，教用部决定在“工学”门类下增设“网络空同安全”一级学科，这对于我网络信息安全人才成体系化、规模化、系统化培养起到积极的推动作用

C.经过十余年的发展，我国信息安全人才培养已经成热和体系化，每年培养的信息安全从业人员的从业的数量较多，基本能同社会实际需求相匹配；同时，高校信息安全专业毕业人才的综合能力要求较高、知识更全面，因而社会化指养应重点放在非安全专业人才培养上

D.除正规大学教育外，我国信息安全人才非学历教育已基本形成了以各种认证为核心，辅以各种职业技能培训的信息安全人才培训体系，包括“注册信息安全专业人员（C1SP）”资质认证和一些大型企业的信息安全资质认证

16.从历演进程看，信息安全的发展经历了多个阶段，其中有一个阶段的特点是：网络信息系统的逐步形成，信息安全注重保护信息在存储、处理和传输过程中免受非授权访间，开始使用防火墙，防病毒，PKI和VPN等安全产品，这个阶段是（C）

A、通信安全阶段：搭线窃听，密码学分析

B、计算机安全阶段：非授权访问，恶意代码，弱口令

C、信息系统安全阶段：网络入侵

D、信息安全保障阶段：黑客，恐怖分子

17.在设计信息安全保障方案时，以下哪个做法是错误的（C）

A.要充分切合信息安全需求并且实际可行

B、要充分考虑成本效益，在满足合规性要求和风险处置要求的前提下，尽量控制成本

C、要充分采取新技术，在使用过程中不断完善成熟，精益求精，实现技术投入保值要求

D、要充分考虑用户管理和文化的可接受性，减少系统方案实施障碍

18.《信息安全保障技术框架》（Information Assurance Technical Framework，IATF）是

由下面哪个国家发布的（B）

A.中国

B.美国

C.俄罗斯

D.欧盟

19.关于我国信息安全保障工作发展的几个阶段，下列哪个说法不正确（C）

A、2001-2002年是启动阶段，标志性事件是成立了网络与信息安全协调小组，该机构是我

国信息安全保障工作的最高领导机构

B、2003-2005年是逐步展开和积极推进阶段，标志性事件是发布了指导性文件《关于加强

信息安全保障工作的意见》（中办发27号文件）并颁布了国家信息安全战略

C、2005-至今是深化落实阶段，标志性事件是奥运会和世博会信息安全保障取得圈满成功

D、2005-至今是深化落实阶段，信息安全保障体系建设取得实质性进展，各项信息安全保障

工作迈出了坚实步伐20.依据国家标准/T20274《信息系统安全保障评估框架》，信息系统安全目标（ISST）中，安全保障目的指的是（D）

A、信息系统安全保障目的

B、环境安全保障目的洛

C、信息系统安全保障目的和环境安全保障目的

D、信息系统整体安全保障目的、管理安全保障目的、技术安全保障目的和工程安全保障目

21.以下哪一项是数据完整性得到保护的例子（B）A、某网站在访问量突然增加时对用户连接数量进行了限制，保证已登录的用户可以完成操作

B、在提款过程中ATM终端发生故障，银行业务系统及时对该用户的账户余额进行了冲正操

C、某网管系统具有严格的审计功能，可以确定哪个管理员在何时对核心交换机进行了什么操作

D、李先生在每天下班前将重要文件锁在档案室的保密柜中，使伪装成清洁工的商业间课无法查看

22.与PDR模型相比，P2DR模型多了哪一个环节（D）

A、防护

B、检测

C、反应

D、策略

23.下列对于信息安全保障深度防御模型的说法错误的是（D）

A、信息安全外部环境：信息安全保障是组织机构安全、国家安全的一个重要组成部分，因此对信息安全的讨论必须放在国家政策、法律法规和标准的外部环境制约下。

B、信息安全管理和工程：信息安全保障需要在整个组织机构内建立和完善信息安全管理体系，将信息安全管理综合至信息系统的整个生命周期，在这个过程中，我们需要采用信息系统工程的方法来建设信息系统。

C、信息安全人才体系：在组织机构中应建立完善的安全意识，培训体系也是信息安全保障的重要组成部分。

D、信息安全技术方案：“从外而内、自下而上、形成边界到端的防护能灯。

24.下面关于信息系统安全保障的说法不正确的是（B）

A、信息系统安全保障与信息系统的规划组织、开发采购、实施交付、运行维护和废弃等生命周期密切相关

B、信息系统安全保障要素包括信息的完整性、可用性和保密性

C、信息系统安全需要从技术、工程、管理和人员四个领域进行综合保障

D、信息系统安全保障需要将信息系统面临的风险降低到可接受的程度，从而实现其业务使命

25.关于信息安全保障的概念，下面说法错误的是（C）

A、信息系统面临的风险和威胁是动态变化的，信息安全保障强调动态的安全理念

B、信息安全保障已从单纯的保护和防御阶段发展为集保护、检测和响应为一体的综合阶段

C、在全球互联互通的网络空间环境下，可单纯依靠技术措施来保障信息安全

D、信息安全保障把信息安全从技术扩展到管理，通过技术、管理和工程等措施的综合融合形成对信息、信息系统及业务使命的保障

26.某学员在学习国家标准《信息系统安全保障评估框架第一部分：简介和一般模型》（GB/T 20274.1-2006）后，绘制了一张简化的信息系统安全保障模型图，如下所示。请为图中括号空白处选择合适的选项（D）

生命周期（从规划、实施到废弃）

（ ）

安全特性（CIA）

A.安全保障（方针和组织）

B.安全防护（技术和管理）

C.深度防御（策略、防护、检测、响应）

D.保障要素（管理、工程、技术、人员）

27、下列我国哪一个政策性文件明确了我国信息安全保障工作的方针和总体要求以及加强

信息安全工作的主要原则？（C）

A.《关于加强政府信息系统安全和保密管理工作的通知》

B.《中华人民共和国计算机信息系统安全保护条例》

C.《国家信息化领导小组关于加强信息安全保障工作的意见》

D.《关于开展信息安全风险评估工作的意见》

28、下列选项中，哪个不是我国信息安全保障工作的主要内容（B）

A.加强信息安全标准化工作，积极采用“等同采用、修改采用、制定”等多种方式，尽快建立和完善我国信息安全标准体系

B.建立国家信息安全研究中心，加快建立国家急需的信息安全技术体系，实现国家信息安全自主可控目标

C.建设和完善信息安全基础设施，提供国家信息安全保障能力支撑

D.加快信息安全学科建设和信息安全人才培养

29、关于我国信息安全保障的基本原则，下列说法中不正确的是（A）

A.要与国际接轨，积极吸收国外先进经验并加强合作，遵循国际标准和通行做法，坚持管理与技术并重

B.信息化发展和信息安全不是矛盾的关系，不能牺牲一方以保证另一方

C.在信息安全保障建设的各项工作中，既要统筹规划，又要突出重点

D.在国家信息安全保障工作中，要充分发挥国家、企业和个人的积极性，不能忽视任何一方的作用

30、下面关于信息系统安全保障模型的说法不正确的是（D）

A.国家标准《信息系统安全保障评估框架第一部分：简介和一般模型》（GB/TA.国家标准《信息系统安全保障评估框架第一部分：简介和一般模型》（GB/T20274.1-2006）中的信息系统安全保障额型将风险和策略作为基础和核心

B.模型中的信息系统生命周期模型是抽象的概念性说明模型，在信息系统安全保障具体操作时，可根据具体环境和要求进行议动和细化

C.信息系统安全保障强调的是动态持续性的长效安全，而不仅是某时间点下的安全

D.信息系统安全保障主要是确保信息系统的保密性、完整性和可用性，单位对信息系统运行维护和使用的人员在能力和培训方面不需要投入

31、P20R模型是一个用于描述网络动态安全的模型，这个模型经常使用图形的形式来形象表达，如下图所示，请问图中空白处应填写的是（B）



A.执行（do）

B.检测（detection）

C.数据（data）

D.持续（duration）

32、目前，信息系统面临外部攻击者的恶意攻击威胁，从威胁能力和掌握资源分，这些威胁可以按照个人威胁、组织威胁和国家威胁三个层面划分，则下面选项中属于组织威胁的是（B）

A.喜欢恶作剧，实现自我挑战的娱乐型黑客

B.实施犯罪，获取非法经济利益网络犯罪团伙

C.搜集政治、军事、经济等情报信息的情报机构

D.巩固战略优势，执行军事任务，进行目标破坏的信息作战部队

二、信息安全监管

1.2005年4月1日正式施行的《电子签名法》，被称为“中国首部真正意义上的信息化法律”，自此电子签名与传统手写签名和盖章具有同等的法律效力。以下关于电子签名说法错误的是（D）

A、电子签名一—是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签

名人认可其中内容的数据

B、电子签名适用于民事活动中的合同或者其他文件、单证等文书

C、电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务

D、电子签名制作数据用于电子签名时，属于电子签名人和电子认证服务提供者共有

2.以下关于信息安全法治建设的意义，说法错误的是（C）

A、信息安全法律环境是信息安全保障体系中的必要环节

B、明确违反信息安全的行为，并对该行为进行相应的处罚，以打击信息安全犯罪活动

C、信息安全主要是技术问题，技术漏洞是信息犯罪的根源

D、信息安全产业的逐渐形成，需要成熟的技术标准和完善的技术体系

3.信息安全等级保护分级要求，第三级适用正确的是（B）

A、适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益

B、适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害

C、适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害

D、适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统。其受到破坏后，会对国家安全、社会秩序，经济建设和公共利益造成特别严重损

4.有关危害国家秘密安全的行为的法律责任，正确的是（A）

A、严重违反保密规定行为只要发生，无论是否产生泄密实际后果，都要依法追究责任

B、非法获取国家秘密，不会构成刑事犯罪，不需承担刑事责任

C、过失泄露国家秘密，不会构成刑事犯罪，不需承担刑事责任

D、承担了刑事责任，无需再承担行政责任或其他处分

5.为推动和规范我国信息安全等级保护工作，我国制定和发布了信息安全等级保护工作所需要的一系列标准，这些标准可以按照等级保护工作的工作阶段大致分类。下面四个标准中，（B）规定了等级保护定级阶段的依据对象、流程、方法及等级变更等内容。

A、GB/T 20271-2006《信息系统通用安全技术要求》

B.GB/T 22240-2008《信息系统安全保护等级定级指南》

C.GB/T 25070-2010《信息系统等级保护安全设计技术要求》

D、GB/T20269-2006《信息系统安全管理要求》

6.GB/T 1836《信息技术安全性评估准则》是测评标准类中的重要标准，该标准定义了评信对象（Target of Evaluation，T0）、保护轮廓（Protection Profile，即）和安全标（Security Target，ST）等术语。关于安全目杯ST），下面选项中描述错误的是（D）

A、ST阐述了安全要求，具体说明了一个既定被评估产品或评估对象的安全功能

B、ST包括该TOE的安全要求和用于满足安全要求的特定安全功能和保证措施

C、ST对于产品和系统来讲，相当于要求了其安全实现方案

D、ST从用户角度描述，代表了用户想要的东西，而不是厂商声称提供的东西

7.下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范图的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项由国家保密工作部门省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定

8.标准是标准化活动的成果，是为了在一定范围内获得最佳秩序，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，关于标准和标准化，以下选项中理解错误的是（D）

A、标准化是一项活动，标准化工作的主要任务是定标准、组织实施以及对标准的实施进行监督，主要作用是为了预期的目的而改进产品、过程或服务的实用性，防止壁垒，促进合作

B、标准化的对象不应是孤立的一件事或一个事物，而是共同的、可重复的事物，标准化的工作同时也具有动态性，即应随着科学的发展和社会的进步而不断修订标准

C、标准在国际贸易中有着重要作用，一方面，标准能打破技术壁垒，促进国际间的发贸发展和科学、技术、文化交流和合作；另一方面，标准也能成为新的技术壁垒，起到限制他国产品出口、保护本国产业的目的

D、标准有着不同的分类，我国将现有标准分为强制性标准、推荐性标准和事实性标准三类，国家标准管理机构对这三类标准通过采取不同字头的方式分别编号后公开发布

9.下面哪部法律或文件不是我国颁布的（B）

A、《关于进一步加强互联网管理工作的意见》（中办发【2004】32号文件）

B、（国家网络安全综合倡议CCI国安54号，国土23号

C、《国家信息安全战略报告》2005年5月国家信息化领导小组

D、《国家信息化战略》

10、指定请求评论（Request For Couments，RFC）文件的形式发布，包含了著名的互联网密钥交换（QnternetKey Exchange，IKE）和互联网协议安全（Internet Protocol Security，IPsec）协议的制定单位是哪个？（C）

A、欧洲计算机制造联合会（ECMA）

B、美国国家标准委员会（DES）

C、互联网工程任务组（TETF）

D、美国电气和电子工程师协会（IEEE）11.由中华人民共和国第十二届全国人大常委会第十五次2015年7月七日审议通过的一部

信息安全国家法律叫什么？（A）

A、《网络安全法》

B、《保守国家秘密法

C、《国家秘密法

D、（国土安全法议法》

12.美国围家标准与技术研究（NationalInstituto of Standards and Toatnology.NIST)隶属于美国商务部，NIST发布的很多关于计策机安全的指南文档。下面哪个文档是由NIST发布的（C）

A、IS027001《Information techmology-Security techniques-Informt.ionA、IS027001（Information techmology-Security techniques-Informt.ion security management systems-Requirements》

B、x509《Information Techmology-0pen Systens-The Directory：Authentication Framework》

C、SP80-37《Guide for Amlying Risk Manaseent Franork to FoderalC、SP80-37（Guide for Amlying Risk Manaseent Franork to Foderal Information Systems》

D、RFC2402《IP Authentication lleader》

13.安全管理体系，国际上有标准（Inforaation technology security tochntqten information systems）（IS0/IC 2701：2013），而我国发布了《信息技术安全管理体系要求》GB/T2080-2008）。请问，这两个标准的关系是（D）

A、IDT（等同采用），此国家标准等同于该国际标准，仅有或没有编辑性修改

B、EQV（等效采用），此国家标准等效于该国家标准，技术上只有很小差异

C、AEQ（等效采用），此国家标准不等效于该国家标准

D、没有采用与否的关系，两者之间版本不同，不应直接比较

14.以下有关法律说法错误的是（B）

A.法律是国家意志的统一体现，有严密的逻辑体系和效力

B.法律是可以公开的，也可以是内部的

C.一旦制定，就比较稳定，长期有效，不允许经常更改

D.法律对违法犯罪的后果有明确规定，是一种硬约束

15.为推动和规范我国信息安全等级保护工作，我国制定和发布了信息安全等级保护工作所需要的一系列标准，这些标准可以按照等级保护工作的工作阶段大致分类。下面四个标准中，（A）提出和规定了不同安全保护等级信息系统的最低保护要求，并按照技术和管理两个方面提出了相关基本安全要求。

A.GB/T22239-2008《信息系统等级保护安全设计技术要求》

B.GB/T222402008《信息系统安全保护等级定级指南》

C.GB/T250702010《信息系统等级保护安全设计技术要求》

D.GB/T28449-2012《信息系统安全等级保护测评过程指南》

16.RFC系列标准是由（D）发布的。

A、国际标准化组织（IS0）

B、国际电工委员会（IEC）

C、国际贸易中心（TTC）

D、互联网工程任务组IETFD、互联网工程任务组IETF

17.自2004年1月起，国内各有关部门在申报信息安全国家标准计划项目时，必须经由以下哪个组织提出工作意见，协调一致后由该组织申报（B）

A、全国通信标准化技术委员会（TC485）

B、全国信息安全标准化技术委员会（TC260）

C、中国通信标准化协会（CCSA）

D、网络与信息安全技术工作委员会

18.有关危害国家秘密安全的行为，包括（A）

A、严重违反保密规定行为、定密不当行为、公共信息网络运营商及服务商不履行保密义务的行为、保密行政管理部门的工作人员的违法行为

B、严重违反保密规定行为、公共信息网络运营商及服务商不履行保密义务的行为、保密行政管理部门的工作人员的违法行为，但不包括定密不当行为

C、严重违反保密规定行为、定密不当行为、保密行政管理部门的工作人员的违法行为，但不包括公共信息网络运营商及服务商不履行保密义务的行为

D、严重违反保密规定行为、定密不当行为、公共信息网络运营商及服务商不履行保密义务的行为，但不包括保密行政管理部门的工作人员的违法行为

19.信息系统建设完成后，（A）的信息系统的运营使用单位应当选择符合国家规定的测

评机构进行测评合格后方可投入使用。

A、二级以上

B、三级以上

C、四级以上

D、五级以上

20.有关国家秘密，错误的是（B）

A、国家秘密是关系国家安全和利益的事项

B、国家秘密的确定没有正式的法定程序

C、除了明确规定需要长期保密的，其他的国家秘密都是有保密期限的

D、国家秘密只限一定范围的人知悉

31.对涉密系统进行安全保密测评应当依据以下哪个标准（B）

A、BMB20-2007《涉及国家秘密的计算机信息系统分级保护管理规范》

B、BMB22-2007《涉及国家秘密的计算机信息系统分级保护测评指南》

C、GB17859-1999《计算机信息系统安全保护等级划分准则》

D、GB/T20271-2006《信息安全技术信息系统统用安全技术要求》

22.ISO/IEC27001《信息技术安全技术信息安全管理体系要求》的内容是基于（B）

A、BS7799-1《信息安全实施细则》

B、BS7799-2《信息安全管理体系规范》

C、信息技术安全评估准则（简称ITSEC）

D、信息技术安全评估通用标准（简称CC）

23.为了保障网络安全，维护维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，加强在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。2015年6月，第十二届全国人大常委会第十五次会议初次审议了一部法律草案，并于7月6日起在网上全文公布，向社会公开征求意见，这部法律草案是（B）

A.《中华人民共和国保守国家秘密法（草案）》

B.《中华人民共和国网络安全法（草案）》

C.《中华人民共和国国家安全法（草案）》

D.《中华人民共和国互联网安全法（草案）》2么.为了进一步提高信息安全的保障能力和防护水平，保障和促进信息化建设的健康发

24.为了进一步提高信息安全的保障能力和防护水平，保障和促进信息化建设的健康发展，公安部等四部门联合发布《关于信息安全等级保护工作的实施意见》（公通字[2004]66号），对等级保护工作的开展提供宏观指导和约束。明确了等级保护工作的基本内容、工作要求和实施计划，以及各部门工作职责分工等。关于该文件，下面理解正确的是（A）

A.该文件是一个由部委发布的政策性文件，不属于法律文件

B.该文件适用于2004年的等级保护工作。其内容不能约束到2005年及之后的工作

C.该文件是一个总体性指导文件，规定了所有信息系统都要纳入等级保护定级范围

D.该文件使用范围为发文的这四个部门，不适用于其他部门和企业等单位

25、以下行为不属于违反国家保密规定的行为（D）

A.将涉密计算机、涉密存储设备接入互联网及其他公共信息网络

B.通过普通邮政等无保密措施的渠道传递国家秘密载体

C.在私人交往中涉及国家秘密

D.以不正当手段获取商业秘密

26、很多行业用户在进行信息安全产品选项时，均要求产品需通过安全测评。关于信息安

全产品测评说法不正确的是（D）

A、测评建立了信息安全产品的市场准入制度；

B、测评对信息安全产品，设计、建设、使用和管理安全的信息系统提供科学公正的专业指导。

C、测评对研究、开发、生产以及信息安全服务的组织提供严格的规范引导和质量监

D、测评为信息安全产业发展创造一个良好的竞争环境27、以下哪项制度或标准被作为我国的一项基础制度加以推行，并且有一定强制性，其实施的主要目标是有效的提高我国信息和信息系统安全建设的整体水平，重点保障基础信息网络和重要信息系统的安全（B）

A.信息安全管理体系（ISM5）

B.信息安全等级保护

C.NIST SP800

D.ISO270000系列

28、按照我国信息安全等级保护的有关政策和标准，有些信息系统只需要自主定级、自主保护，按照要求向公安机关备案即可，可以不需要上级或主管部门来测评和检查。此类信息系统应属于（C）

A.零级系统

B.一级系统

C.二级系统

D.三级系统

29、信息安全标准化工作是我国信息安全保障工作的重要组成部分之一，也是政府进行宏观管理的重要依据，同时也是保护国家利益、促进产业发展的重要手段之一，关于我国信息安全标准化工作，下面选项中描述错误的是（B）

A.我国是在国家质量监督检验检疫总局的管理下，由国家标准化管理委员会同意管理全国标准化工作，下设有专业技师委员会

B.因事关国家安全利益，信息安全因此不能和国际标准相同，而是要通过本国组织和专家制定标准，切实有效地保障国家利益和安全

C.我国归口信息安全方面标准的是“全国信息安全标准技术委员会”，为加强有关工作，2016在其下设立“大数据安全特别工作组”

D.信息安全标准化工作是解决信息安全问题的重要技术支撑，其主要作用突出地体现在能够确保有关产品、设施的技术先进性、可靠性和一致性

三、信息安全管理

1、关于信息安全管理，说法错误的是（D）

A、信息安全管理是管理者为实现信息安全目标（信息资产的CIA等特性，以及业务送作的持续）而进行的计划、组织、指挥和控制的一系列活动。

B、信息安全管理是一个多层面、多因素的过程，依赖于建立信息安全组织、明确信息

安全角色及职责、制可信息安全方针策略标准规范、建立有效的监督审计机制等多方面的非技术性的努力。

C、实现信息安全，技术和产品是基础，管理是关键。

D、信息安全是人员、技术、操作三者紧密合作的系统工程，是一个静态过程。

2.文档体系建设是信息安全管理体系（ISMS）建设的直接体现，下列说法不正确的是（B）

A、组织内的信息安全方针文件、信息安全规章制度文件，信息安全相关操作规范文件等文档是组织的工作标准，也是ISMS审核的依据

B、组织内的业务系统日志文件、风险评估报告等文档是对上一级文件的执行和记录，对这些记录不需要保护和控制

C、组织在每份文件的首页，加上文件修订跟踪表，以显示每一版本的版本号、发布日期、编写人、审批人、主要修订等内容

D、层次化的文档是ISMS建设的直接体现，文档体系应当依据风险评估的结果建立3.信息安全管理体系（Information Security Manageuent Systen，ISMS）的内部审核和管理审核是两项重要的管理活动，关于这两者，下面描述错误的是（C）

A、内部审核和管理评审都很重要，都是促进ISMS持续改进的重要动力，也都应当按醒一定的周期实施

B、内部审核的实施方式多采用文件审核和现场审核的形式，而管理评审的实施方式多采用召开管理评审会议的形式进行

C、内部审核的实施主体由组织内的ISMS内审小组，而管理评审的实施主体是由国家政策指定的第三方技术服务机构

D、组织的信息安全方针，信息目标和有关ISM5文件等，在内部审核中作为审核准则做用，但在管理评审中，这些文件是被审对象4.在信息安全管理体系的实施过程中，管理者的作用对于信息安全管理体系能否成功实施非常重要，但是以下选项中不属于管理者应有职责的是（D）

A、制定并颁布信息安全方针，为组织的信息安全管理体系建设指明方向并提供总体的领，明确总体要求

B.确保组领的信息安全管理体系目标和相应的计划得以制定，目标应明确、可度量、计划应具体、可实施

C、向组织传达满足信息安全的重要指示传达满足信息安全要求、达成信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性

D、建立健全信息安全制度，明确信息安全风险管理作用，实施信息安全风险评估过程，确保信息安全风险评估技术选择合理、计算正确

5.层次化的文档是信息安全管理体系《information Security Management Systen，ISMS》建设的直接体系，也是ISMS建设的成果之一，通常将ISMS的文档结构规划为4层金字塔结构，那么，以下选项（D）应放入到一级文件中。

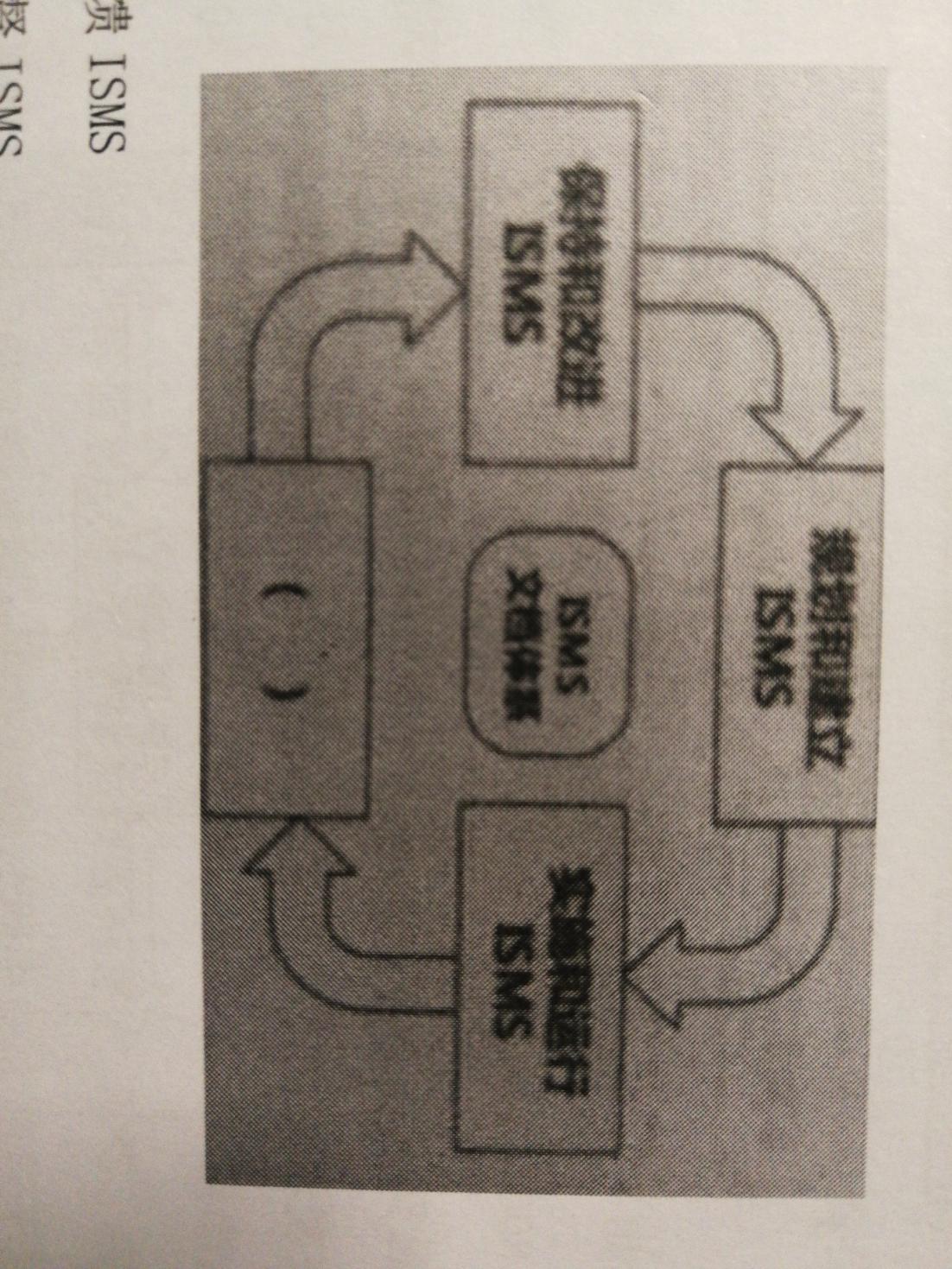
A、《风险评估报告》

B、《人力资源安全管理规定

C、《ISMS内部审核计划》

D、《单位信息安全方针》

6.小李去参加单位组织的信息安全培训后，他把自己对信息安全管理体系（Information Security Managenent Systen.ISMS）的理解面了以下一张图，但是他还存在一个空白处未填写，请帮他选择一个最合适的选项（C）。



A、监控和反馈ISMSA、监控和反馈ISMS

B、批准和监督ISMSB、批准和监督ISMS

C、监视和评审ISMSC、监视和评审ISMS

D、沟通和咨询ISMSD、沟通和咨询ISMS

7.信息安全管理体系（information seurity Manmgenent Systa.简称IS85）要求建立过程体系，该过程体系是在如下（D）基础上构建的。

A、IATF（Information Assurance Technical Framework）

B.p2DR（Policy，Protection，Detection，Response）

C、mcRF（fPreparation，Detection.Contaiment，Eradicatin，Becowery.Followup）

D、PDCA（Plan，Do，Check，Act）

8.小王在学信息安全管理体系相关知识之后，对于建立信息安全管理体系，自己总结了下面四条要求，其中理解不正确的是（B）

A、信息安全管理体系的建立应参照国际国内有关标准实施，因为这些标准是标准化组织在总结研究了很多实际的或潜在的问题后，制定的能共同的和重复使用的规则

B、信息安全管理体系的建立应基于最新的信息安全技术，因为这是国家有关信息安全的法律和法规方面的要求，这体现以预防控制为主的思想

C、信息安全管理体系应强调全过程和动态控制的思想，因为安全问题是动态的，系统所处的安全环境也不会一成不变的，不可能建设永远安全的系统

D.信息安全管理体系应体现料学性和全面性的特点，因为要对信息安全管理设计的方方面面实施较为均衡的管理，避免遗漏某些方面而导致组织的整体信息安全水平过低

9、IS027002（Information technology-Security techniques-Code of pratices、IS027002（Information technology-Security techniques-Code of pratice forinforeation security smanagcacnt）是重要的信息安全管理标准之一，下图是关于其演进变化示意图，图中括号空白处应填写（B）

BS 7799|BS 7799.1|-（）ISO27002

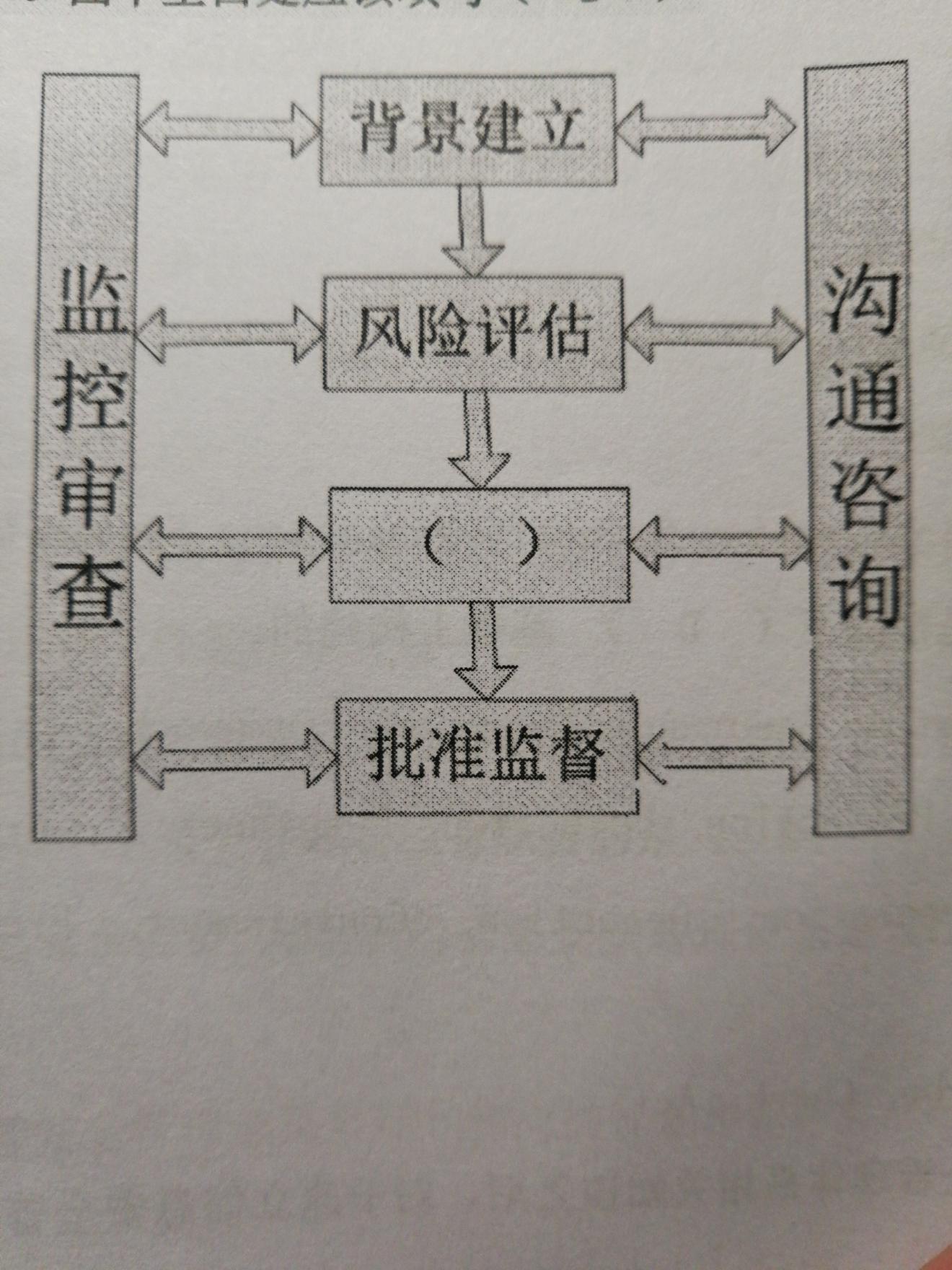
A、BS7799.1.3

B、I5017799

C、AS/NZS4630

D、NIST SP800-37

10.我国标准《信息安全风险管理》（CB/Z24364）给出了信息安全风险管理的内容和过程，可以用下图来表示。图中空白处应该填写（D）



A、风险计算

B、风险评价

C、风险预测

D、风险处理

11.在信息安全管理过程中，背果建立是实施工作的第一步。下面哪像理解是错误的（B）

A、背景建立的依据是国家、地区或行业的相关政策、法律、法规和标准，以及机构的使命、信息系统的业务目标和特性

B、背景建立阶段应识别需要保护的资产、面临的或胁以及存在的脆弱性并分别赋值，同时确认已有的安全措施，形成需要保护的资产清单

C、背景建立阶段应调查信息系统的业务目标、业务特性、管理特性和技术特性，形成信息系统的描述报告

D、背景建立阶段应分析信息系统的体系结构和关键要素，分析信息系统的安全环境和要求，形成信息系统的安全要求报告

12.随着信息安全涉及的范围越来越广，各个组织对信息安全管理的需求越来越迫切，越来越多的组织开始尝试使用参考IS027001介绍的ISMS来实施信息安全管理体系，提高组织的信息安全管理能力。关于ISMS，下面描述错误的（A）

A、在组织中，应有信息技术责任部门（如信息中心）制定并颁布信息安全方针，为组织的ISMS建设指明方向并提供总体纲领，明确总体要求

B、组织的管理层应确保ISIS自标和相应的计划得以制定，信息安全管理目标应明确、可度量，风险管理计划应具体、具备可行性

C、组织的信息安全目标、信息安全方针和要求应传达到全组织范围内，应包括全体员工，同时，也应传达客户、合作伙件和供应商等外部各方

D、组织的管理层应全面了解组织所面临的信息安全风险，决定风险可接受级别和风险可接受准则，并确认接受和相关残余风险

13.GB/T 22080-2008《信息技术安全技术信息安全管理体系要求》指出，建立信息安全管理体系应参照PDCA模型进行，即信息安全管理体系应包括建立ISMS、实施和运行ISMS、监视和评审ISMS、保持和改进ISMS等过程，并在这些过程中应实施若干活动。请选出以下描述错误的选项（D）

A、“制定ISM5方针”是建立ISMS阶段工作内容

B、“实施培训和意识教育计划”是实施和ISMS阶段工作内容

C、“进行有效性测量”是监视和译ISMS阶段工作内容

D、“实施内部审核”是保持和改进ISMS阶段工作内容

14.若一个组织声称自己的ISMS符合1S0/TC 27001或GB/T2080标准要求，其信息安全控制措施通常在以下方面实施常规控制，不包括哪一项（D）

A、信息安全方针、信息安全组织、资产管理

B、人力资源安全、物理和环境安全、通信和操作管理

C、访问控制、信息系统获取、开发和维护、符合性

D、规划与建立ISMSD

15.信息安全组织的管理涉及内部组织和外部各方两个控制目标。为了实现控制外部各方的目标应该包括下列哪个选项（D）

A、信息安全的管理承诺、信息安全协调、信息安全职责的分配

B、信息处理设施的授权过程、保密性协议、与政府部门的联系

C、与特定利益集团的联系、信息安全的独立评审

D、与外部各方相关风险的识别、处理外部各方协议中的安全问题

16.若一个组织声称自己的ISMS符IS0/IEC27001或GB/T22080标准要求，其信息安全措施通常需要在资产管理方面实施常规控制，资产管理包含对资产负责和信息分类两个业制目标。信息分类控制的目标是为了确保信息受到适当级别的保护，通常采取以下哪项投制措施（D）

A、资产清单

B、资产责任人

C、资产的可接受使用

D、分类指南、信息的标记和处理

17.层次化文档是ISMS建设直接体现，是ISMS建设的成果。通常ISMS文档结构分为因层金字塔结构，以下哪项属于四级文件（A）

A.数字证书签发系统日志

B.人力资源安全管理规定

C.病毒防范指南

D.信息安全方针政策

18.关于信息安全管理体系，下面描述错误的是（D）

A.信息安全管理体系是组织在整体或特定范围内建立信息安全方针和目标，以及完感这些目标所用的方法的体系，包括：组织架构，方针，职责及相关实践要求

B.管理体系是为达到组织目标的策略程序指南和相关资源框架，信息安全管理体系是管理体系思想和方法在信息安全领域的应用

C.概念上，信息安全管理有广义和获义之分，狭义的信息安全管理体系是指技层IS027001标准制定的管理体系，它是一个组织整体管理体系的组成部分

D.同其他管理体系一样，信息安全管理体系也要建立信息安全管理组织机构，健全信息安全管理制度，构建信息安全技术体系，加强人员的安全意识等内容。

19.若一个组织声称自己的ISMS符ISO/IEC27001或T2080标准要求，其信息安全控。措施通常漏要在人力资源安全方面实施常规控制，人力资源安全划分为3个控制阶段，不包括哪一项（D）

A.任用之前B.任用中C.任用终止或变化D.任用后

20.信息安全管理体系（ISMS）的建设和实施是一个组织的战略性举措。若一个组织声称自己

的ISMS符合ISO/TEC27001或GR/T22080标准要求，则需实施准要求，则需实施以下ISMS建设的各项工作，哪一项不属于ISMS建设的工作（D）。

A.规划与建立IsMS

B.实施和运行ISMS

B.实施和运行ISMS

C.监视和评审ISMS

D.保持和审核ISMS

21.关于信息安全管理，下面理解片面的是（C）。

A.信息安全管理是组织整体管理的重要、固有组成部分，它是组织实现其业务目标的重要保障

B.信息安全管理是一个不断演进、循环发展的动态过程，不是一成不变的

C.在信息安全建设中，技术是基础，管理是拔高，即有效的管理依赖于良好的技术基础

D.坚持管理与技术并重的原则，是我国加强信息安全保障工作的主要原则之一

22.PDCA循环又叫戴明环，是管理学常用的一种模型。关于PDCA四个字母，下面理解错误的是（D）

A.P是Plan，指分析问题、发现问题、确定方针、目标和活动计划

B.D是Do，指实施、具体运作，实现计划中的内容

C.C是Check，指检查、总结执行计划的结果，明确效果，找出问题

D.A是Aim，指瞄准问题，抓住安全事件的核心，确定责任

28.小王是某大学计算科学与技术专业的毕业生，大四上学期开始找工作，期望谋求一份技术管理的职位，一次面试中，某公司的技术经理让小王谈一谈信息安全风险管理中的“背景建立”的基本概念与认识，小王的主要观点包括：（1）背景建立的目的是为了明确信息安全风险管理的范围和对象，以及对象的特性和安全要求，完成信息安全风险管理项目的规划和准备；（2）背景建立根据组织机构相关的行业经验执行，雄厚的经验有助于达到事半功倍的效果；（3）背景建立包括：风险管理准备、信息系统调查、信息系统分析和信息安全分析：（）背景建立的阶段性成果包括：风险管理计划书、信息系统的描述报告、信息系统的分析报告、信息系统的安全要求报告。请问小王的所述论点中错误的是哪项（B）

A、第一个观点，背景建立的目的只是为了明确信息安全风险管理的范围和对象

B、第二个观点，背景建立的依据是国家、地区域行业的相关政策、法律、法规和标准

C、第三个观点，背景建立中的信息系统调查与信息系统分析是同一件事的两个不同名字

D、第四个观点，背景建立的阶段性成果中不包括有风险管理计划书

24.风险管理的监控与审查不包含（D）

A、过程质量管理

B、成本效益管理

C、跟踪系统自身或所处环境的变化

D、协调内外部组织机构风险管理活动

25.以下哪一项不是信息安全管理工作必须遵循的原则（C）

A、风险管理在系统开发之初就应该予以充分考虑，并委贯穿于整个系统开发过程之中

B、风险管理活动应成为系统开发、运行、维护、直至废弃的整个生命周期内的持续性工作

C、由于在系统投入使用后部署和应用风险控制措施针对性会更强，实施成本会相对较低

D、在系统正式运行后，应注重残余风险的管理，以提高快速反应能力

26.以下哪些是需要在信息安全策略中进行描述的（B）

A、组织信息系统安全架构

B、信息安全工作的基本原则

C、组织信息安全技术参数

D、组织信息安全实施手段

27.下面的角色对应的信息安全职责不合理的是（B）

A、高级管理层——最终责任

B、信息安全部门主管——提供各种信息安全工作必须的资源

C、系统的普通使用者—一遵守日常操作规范

D、审计人员——检查安全策略是否被遵从

28.为了不断完善一个组织的信息安全管理，应对组织的信息安全管理方法及实施情况进行独立评审，这种独立评审（C）

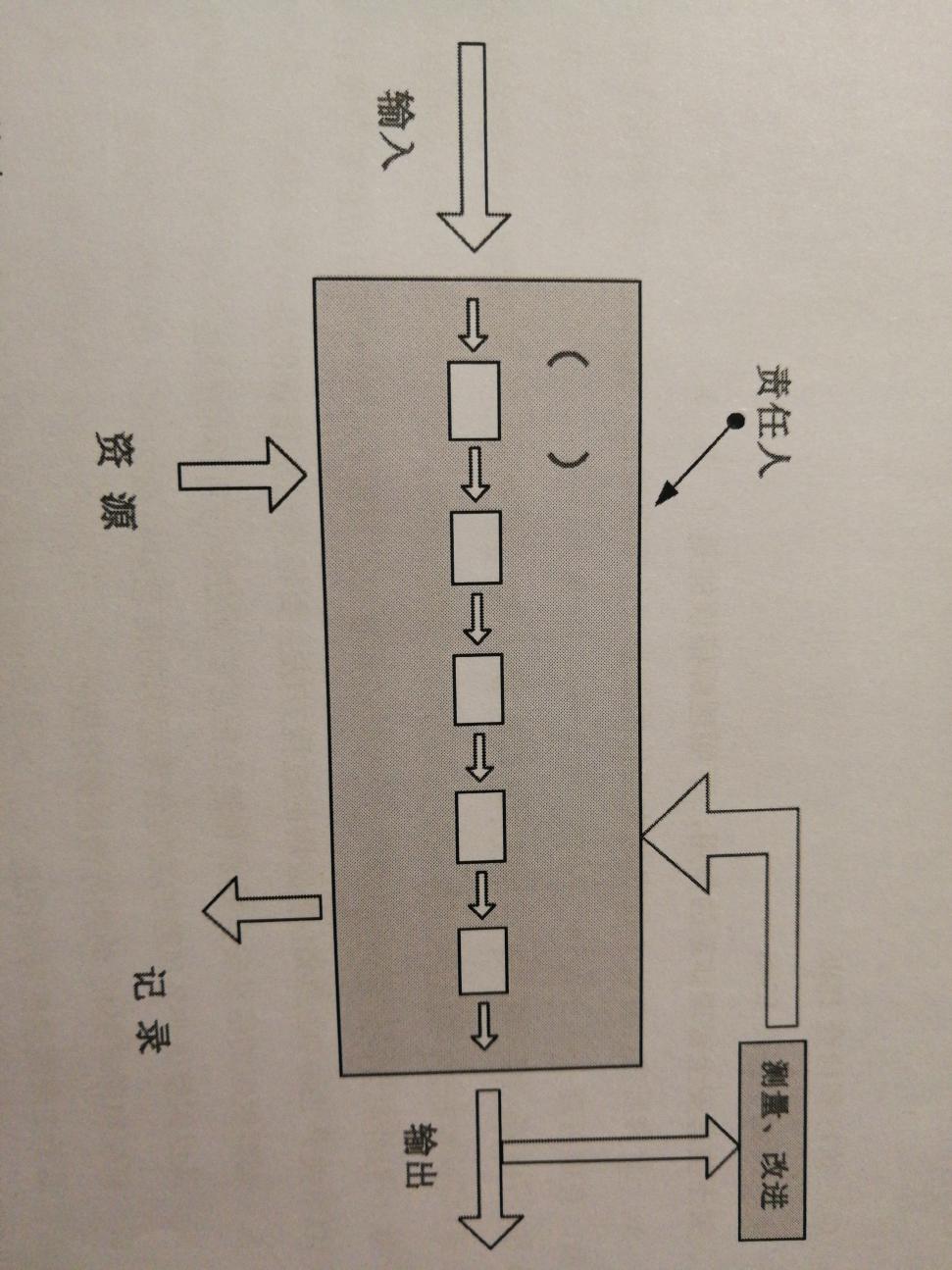
A、必须按固定的时间间隔来进行

B、应当由信息系统的运行维护人员发起

C、可以由内部审核部门或专业的第三方机构来实施

D、结束后，评审者应组织针对不符合安全策略的问题设计和实施纠正措施

29.IS09001-2000标准在制定、实施质量管理体系以及改进其有效性时采用过程方法，通过满足顾客要求增进顾客满意。下图是关于过程方法的示意图，图中括号空白处应填写（D）



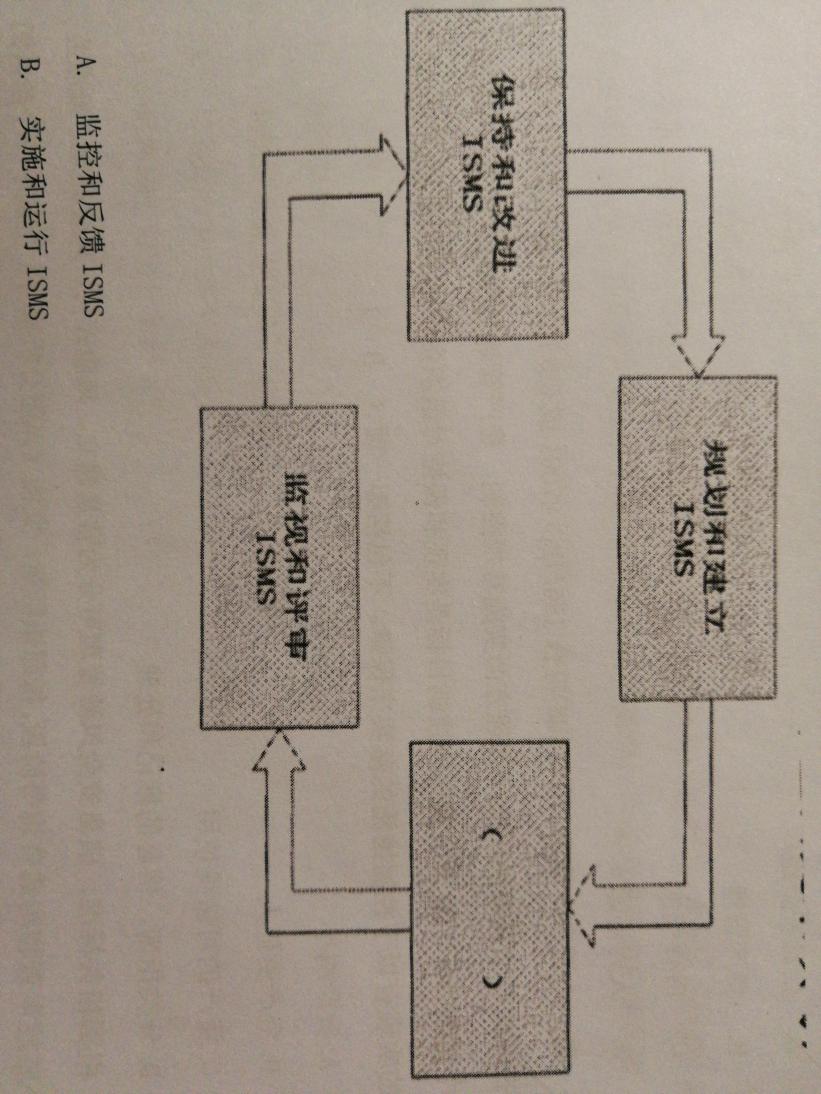
A.策略

B.管理者

C.组织

D.活动

30小李在学习信息安全管理体系（Information Security Management Systen，ISMs）的有关知识后，按照自己的理解画了一张图来描述安全管理过程，但是他存在一个空白处未填写，请帮他选择一个最合适的选项（B）



A.监控和反馈ISMSA.监控和反馈ISMS

B.实施和运行ISMSB.实施和运行ISMS

C.执行和检查ISMS

D.沟通和咨询ISMS

31、关于信息安全管理体系的作用，下面理解错误的是（B）

A.对内而言，有助于建立起文档化的信息安全管理规范，实现有“法”可依，有意可循，有据可查

B.对内而言，是一个光花钱不挣钱的事情，需要组织通过其他方面收入来弥补投入

C.对外而言，有助于使各利益相关方对组织充满信心

D.对外而言，能起到规范外包工作流程和要求，帮助界定双方各自信息安全责任

82、以下关于ISO/IEC27001所应用的过程方法主要特点说法错误的是（D）

A.理解组织的信息安全要求和建立信息安全方针与目标的标准

B.从组织整体业务风险的角度管理组织的信息安全风险

C.监视和评审ISMS的执行情况和有效性

D.基于主观测量的持续改进

38、“通知相关人员ISMS的变更”是建立信息安全管理体系哪个阶段的活动（D）

A、规划和建立

B.实施和运行

C.监视和评审

D.保持和改进

34、IS027002中描述的11个信息安全管理的控制领域不包括（C）

A信息安全组织

B.资产管理

C.内容安全

D.人力资源安全

35、若一个国家声称自己的ISMS符合IS0/IBC27001或6B/T22080标准要求，其信息安全控制措施通常需要在资产管理方面实施常规控制，资产管理包含对资产负责和信息分类两个控制目标。对资产负责的控制目标是实现和保持对组织资产的适当保护。这一控制目标的实现有以下控制措施的落实来保障。不包括哪一项（D）

A.资产清单

B.资产责任人

C.资产的可接受使用

D.分类指南，信息的标记和处理

36、根据相关标准，信息安全风险管理可分为背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询等阶段，按照该框架，文档《风险分析报告》应属于哪个阶段的输出成果（A）

A.风险评估

B.风险整理

C.批准监督

D.监控审查

37、若一个组织声称自己的ISMS符合ISO/IEC27001或CGB/T22080标准要求，其信息安全控制措施通常需要在物理和环境安全方面实施常规控制。物理和环境安全区域和设备安全两个控制目标。安全区域的控制目标是防止对组织场所和信息的未授权物理访问、损坏和干扰，关键或敏感的信息及信息处理设施应放在安全区域内，并受到相应保护。该目标可以通过以下控制措施来实现，不包括哪一项（D）

A.物理安全边界、物理入口控制

B.办公室、房间和设施的安全保护、外部和环境威胁的安全防护

C.在安全区域工作，公共访问、交接区安全

D.人力资源安全

28、若一个组织声称自己的ISMS符合IS0/TEC27001或6B/T22080标准要求，其信息安全控制措施通常需要在符合性方面实施常规控制。符合性常规控制这一领域不包括以下哪项控制目标（D）

A.符合法律要求

B.符合安全策略和标准以及技术符合性

C.信息系统审核考虑

D.访问控制的业务要求，用户访问管理

39、王工是某单位的系统管理员，他在某次参加了单位组织的风险管理工作时，根据任务安排他使用了Nessus工具来扫描和发现数据库服务器的漏洞。根据风险管理的相关理论，他这个扫描活动属于下面哪一个阶段的工作（B）

A.风险分析

B.风险要素识别

C.风险结果判定

D.风险处理

40、以下列哪种处置方法属于转移风险？（D）

A.部署综合安全审计系统

B.对网络行为进行实时监控

C.制订完善的制度体系

D.聘用第三方专业公司提供维护外包服务

41、风险管理四个步骤的正确顺序是：（A）

A.背景建立、风险评估、风险处理、批准监督

B.背景建立、风险评估、审核批准、风险控制

C.风险评估、对象确立、审核批准、风险控制

D.风险评估、风险控制、对象确立、审核批准4、在风险管理的过程中，“建立背景”（即“对象确立”）的过程是哪四个活动？（A）

A.风险管理准备、信息系统调查、信息系统分析、信息安全分析

B.风险管理准备、信息系统分析、信息安全分析、风险政策的制定

C.风险管理准备、风险管理政策的制定、信息系统分析、信息安全分析

D.确定对象、分析对象、审核对象、总结对象

43对操作系统打补丁和系统升级是以下哪种风险控制措施？（A）

）A.降低风险B.规避风险C.转移风险D.接受风险

44.以下哪一项可认为是具有一定合理性的风险？（C）

A.总风险原最小化风险C.可接受风险D.残余风险

45.风险管理中使用的控制措施，不包括以下哪种类型？（B）

A.预防性控制措施B.管理性控制措施

C.检查性控制措施D.纠正性控制措施

四~六略

七、信息安全支撑技术

1.下列哪一种方法属于基于实体“所有”鉴别方法（D）

A、用户通过自己设置的口令登录系统，完成身份鉴别

B、用户使用个人指纹，通过指纹识别系统的身份鉴别

C、用户利用和系统协商的秘密函数，对系统发送的挑战进行正确应答，通过身份鉴别

D、用户使用集成电路卡（如智能卡）完成身份鉴别

2.为防范网络欺诈确保交易安全，网银系统首先要求用户安全登录，然后使用“智能卡+短信认证”模式进行网上转账等交易，在此场景中用到下列哪些鉴别方法（A）

A、实体“所知”以及实体“所有”的鉴别方法

B、实体“所有”以及实体“特征”的鉴别方法

C、实体“所知”以及实体“特征”的鉴别方法

D、实体“所有”以及实体“行为”的鉴别方法

3.以下场景描述了基于角色的访问控制模型（Role-based Access Control.RBAC）：根据组织的业务要求或管理要求，在业务系统中设置若干岗位、职位或分工，管理员负责将权限（不同类别和级别的）分别赋予承担不同工作职责的用户。关于R阳AC模型，下列说法错误的是（D）

A、当用户请求访问某资源时，如果其操作权限不在用户当前被激活角色的授权范围内，

访问请求将被拒绝

B、业务系统中的岗位、职位或者分工，可对应RBC模型中的角色

C、通过角色，可实现对信息资源访间的控制

D、RBAC模型不能实现多级安全中的访问控

4.来移动精能全制文情猫过都发识期都做系统的动能，与微统的整于口令的整期技术相比。

关于此种鉴别技术说法不正确的是（c）

A、所选择的特征（指纹）便于收集、测量和比较

B、每个人所拥有的指纹都是独一无二的

C.指纹信息是每个人独有的，指纹系统不存在安全威胁问题

D、此类系统一般用户指纹信息采集和指纹信息识别两部分组成

9.由于发生了一起针对服务器的口令暴力破解攻击，管理员决定对服务器设置账户锁定策略以对抗口令暴力破解。他设置了以下账户锁定策略：复位账户锁定计数器5分钟，账户锁定时间10分钟，账户锁定阀值3次无效登录，以下关于以上策略设置后的说法哪个是正确的（B）

A、设置账户锁定策略后，攻击者无法再进行口令暴力破解，所有输错了密码的用户就会被锁住

B、如果正常用户不小心输错了3次密码，那么该用户就会被锁定10分钟，10分钟内即使输入正确的密码，也无法登录系统。

C、如果正常用户不小心连续输入错误密码3次，那么该用户账号就被锁定5分钟，5分钟内即使提交了正确的密码也无法登录系统

D、攻击者在进行口令破解时，只要连续输错3次密码，该用户就被锁定10分钟，而正常用户登录不受影响

20.在网络信息系统中对用户进行认证识别时，口令是种传统但仍然使用广泛的方法，口令认证过程中常常使用静态口令和动态口令，下面描述错误的是（C）

A.所谓静态口令方案，是指用户登录验证身份的过程中，每次输入的都是固定、静态不变的

B.使用静态口令方案时，即使对口令简单加密或HASH后进行传输，攻击者依然可以重放攻击来欺骗信息系统的身份认证模块

C.动态口令方案中通常需要使用密码算法产生较长的口令序列，攻击者如果连续获取足够的历史口令，则有可能预测出下次要使用的口令

D.通常，动态口令实现方式分为口令序列，时间同步以及挑战/应答等几种类型。

31.分组密码算法是一类十分重要的密码算法，下面描述中，错误的是（C）

A.分组密码算法要求输入明文按组分成固定长度的块

B.分组密码算法每次计算得到固定长度的密文输出块

C.分组密码算法也称为序列密码算法

D.常见的DES、IDEA算法都属于分组密码算法

32.实体身份鉴别一般依据以下三种基本情况或这三种情况的组合：实体所知的鉴别方法、实体所有的鉴别方法和基于实体特征的鉴别方法。下面选项中属于实体特征的鉴别方法是（D）

A.将登录口令设置为出生日期

B.通过询问和核对用户的个人隐私信息来鉴别

C.使用系统定制的、在本系统专用的IC卡进行鉴别

D.通过扫描和识别用户的脸部信息来鉴别

36.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制模型的设计思路。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和方法是（A）

A.访问控制列表（ACL）

B.能力表（CL）

C.BLP模型

D.Bida模型

八、物理与网络通信安全

1.某公司已有漏洞扫描和入侵检测系统（Intrusien Detection Systen，IDS）产品，需要购买防火墙，以下做法应当优先考虑的是（D）

A、选购当前技术最先进的防火墙即可

B、选购任意一款品牌防火墙

C、任意选购一款价格合适的防火墙产品

D、选购一款同已有安全产品联动的防火墙

3.数据在进行传输前，需要由协议栈自上而下对数据进行封装，TCP/TP协议中，数据封装的顺序是（B）

A、传输层、网络接口层、互联网络层

B、传输层、互联网络层、网络接口层

C、互联网络层、传输层、网络接口层

D、互联网络层、网络接口层、传输层

4.传输控制协议（TCP）是传输层协议，以下关于TCP协议的说法，哪个是正确的（D）

A、相比传输层的另外一个协议UDP，TCP既提供传输可靠性，还同时具有更高的效率，因此具有广泛的用途

B、TCP协议包头中包含了源IP地址和目的IP地址，因此TCP协议负责将数据传送到正确的主机

C、TCP协议具有流量控制、数据校验、超时重发、接收确认等机制，因此TCP协议能完全替代IP协议

D、TCP协议虽然高可靠，但是相比UDP协议机制过于复杂，传输效率要比UDP低

8.某网站管理员小邓在流量监测中发现近期网站的入站ICMP流量上升了250%，尽管网业有发现任何的性能下降或其他问题，但为了安全起见他仍然向主管领导提出了应对措施。作为主管负责人，请选择有效的针对此问题的应对措施（A）

A、在防火墙上设置策略，阻止所有的ICMP流量进入（关掉ping）

B、删除服务器上的ping.exe程序

C、增加带宽以应对可能的拒绝服务攻击

D、增加网站服务器以应对即将来临的拒绝服务攻击

9.以下关于安全亲接层（Gcurity sctets layer，s）说法错误的是：（A）

A、受到.防护的山服务器比没有sL的6b服务器要安全

B、当测览器上的统一资源定位符nifoB、当测览器上的统一资源定位符Uniform Resource Locator，URL）出现https 时，说明用户正使用配置了SSL协议的web 服务器

C、SSL可以看到浏览器与服务器之间的安全通道

D、SSL提供了一种可靠地端到端的安全服务

13.异常入侵检测是入侵检测系统常用的一种技术，它是识别系统或用户的非正常行为或者对于计算机资源的非正常使用，从而检测出入侵行为。下面说法错误的是（B）

A、在异常入侵检测中，观察到的不是已知的入侵行为，而是系统运行过程中的异常现象

B、实施异常入侵检测，是将当前获取行为数据和己知入侵攻击行为特征相比较，若匹配则认为有攻击发生

C、异常入侵检测对以通过获得的网络运行状态数据，判断其中，并通过多种手段向管理员报警

D、异常入促检测不但可以发现从外部的攻击，也可以发现内部的恶意行为

14.某网络安全公司基于网络的实时入侵检测技术，动态探测来自于外部网络和内部网络的所有访问行为。当检测到来自内外网络针对或通过防火墙的攻击行为。会及时响应，并通过防火墙实时阻断攻击源，从而进一步提高了系统的抗攻击能力，更有效地保护了网络资源提高了防御体系，但入侵检测技术不能实现以下哪种功能（C）

A、检测并分析用户和系统的活动

B、核查系统的配置漏洞，评估系统关键和数据文件的完整性

C、防止IP地址欺骗

D、识别违反安全策略的用户活动

15.入侵检测系统有其技术优越性，但也有其局限性。下列说法错误的是（A）

A、对用户知识要求高，配置，操作和管理使用过于简单，容易遭到攻击

B、高虚警率，入侵检测系统会产生大量的警告消息和可疑的入侵行为记录，用户处理负担很重

C、入侵检测系统在应对自身攻击时，对其他数据的检测可能会被抑制或者受到影响

D、警告消息记录如果不完整，可能无法与入侵行为关联

16.安全域是由一组具有相同安全保护需求并相互信任的系统组成的逻辑区域，下面哪项描述是错误的（A）

A、安全域划分主要以业务需求、功能需求和安全需求为依据，和网络、设备的物理部署位置无关

B、安全域划分能把一个大规模复杂系统的安全问题，化解为更小区域的安全保护问题

C、以安全域为基础，可以确定该区域的信息系统安全保护等级和防护手段，从而使同

一安全域内的资产实施统一的保护

D、安全域边界是安全事件发生时的抑制点，以安全域为基础，可以对网络和系统进行安全检查和评估，因此安全域划分和保护也是网络防攻击的有效防护方式。

17.某个新成立的互联网金融公司拥有10个与互联网直接连接的IP地址，但是该网络内有15台个人计算机，这些个人计算机不会同时开机并连接网联网。为解决公司员工的上网问题，公司决定将这10个互联网地址集中起来使用，当任意一台个人计算机开机并连接网络时，管理中心从这10个地址中任意取出一个尚未分配的IP地址分配给这个人的计算机。他关机时，管理中心将该地址收回，并重新设置为未分配。可见。只要同时打开的个人计算机数量少于或等于可供分配的IP地址，那么，每台个人计算机可以获取一个IP地址，并实现与互联网的连接。该公司使用的IP地址规划方式是（B）

A、静态分配地址

B、动态分配地址

C、静态NAT分配地址

D、端口NAT分配地址

18.VPN中的P是什么具体的含义是意思？（B）

A、sPecial use专用

B、Privacy私有

2Permit 允许

D、Public公共的

19.TCP/IP协议把网络安全分为多少层（B）

A、3B、4C、5D、6

20.关于ARP欺骗原理和防范措施，下面理解错误的是（D）

A、ARP欺骗是指攻击者直接向受害者主机发送错误的ARP应答报文，使得受害者主机将错误的硬件地址映射关系存入到ARP缓存中，从而起到冒充主机的目的

B、单纯利用ARP欺骗攻击时，ARP欺骗通常影响的是内部子网，不能跨越路由实施攻击

C、解决ARP欺骗的一个有效方法是采用“静态”的ARP缓存，如果发生硬件地址的更改，则需要人工更新缓存

D、彻底解决ARP欺骗的方法是避免使用ARP协议和ARP缓存，直接采用IP地址和其他主机进行连接

22.IPEC协议标准的设计目标是在IPV4和IPV6环境中为网络层流量提供灵活透明的安全服务，保护TCP/IP通信免遭窃听和篡改，保证数据完整和机密性，下列描述哪一个是错误的（A）

A.IPSEC协议不支持使用数字证书

B.IPSEC协议对于1Pv4和IPv6网络都适用

C.IPSEC有两种功能工作模式：传输模式和隧道模式

B.IPSEC协议包括封装安全载奋（E5P）和鉴别头（AH）两种通信保护机制

23.TCP/IP协议是Internet最基本协议，也是Intornet构成的基础，TCP/IP通常被认为是一个N层协议，每一层都是用它的下一层所提供的网络服务完成自己的能，这里的的应等于（A）

A.4

B.5

C.6

D.7

24.关于UDP协议说法，哪个是错误的（D）

A.UDP具有简单高效的特点，常被攻击者用来实施流量型拒绝服务攻击

B.UDP协议包头中包含了源端口号和目的端口号，因此UDP可通过端口号将数据包送达正确的程序

C.相比TCP协议，UDP协议的系统开销更小，因此常用来传送如视频这一类高流量需求的应用数据

D.UDP协议不仅具有流量控制，超时重发等机制，还能提供加密等服务，因此常用来传输如视频会话这类需要隐私保护的数据

25.由于Internet的安全问题日益突出，基于TCP/IP协议，相关组织和专家在协议的不同层次设计了相应的安全通信协议，用来保障网络各层次的安全，中，属于或依附于传输层的安全协议是（C）

A.PPTP

B.L2TP

C.SSL

D.IPSec

26.防火墙是网络信息系统建设中常常采用的一类产品，他在内外网隔方面的作用是（c）

A.既能物理隔离，又能逻辑隔离

B.能物理隔离，不能逻辑隔离

C.不能物理隔离，能逻辑隔离

D.不能物理隔离也不能逻辑隔离

27.IPV4协议在设计之初并没有过多地考虑安全问题，为了能够使网络方便地进行互联、互通，仅仅依靠IP头部的校验和字段来保证IP包的安全，因此IP包很容易被窜改，并重新计算校验和。IETF于1994年开始制定IPSec协议标准，其设计目标是在IPV4和IPV6环境中为网络层流量提供灵活、透明的安全服务，保护TCP/1P通信免道窃听和算改，保证数据的充整性和机密性，有效抵御网络攻击，同时保持易用性，下列选项中说法错误的是（C）.

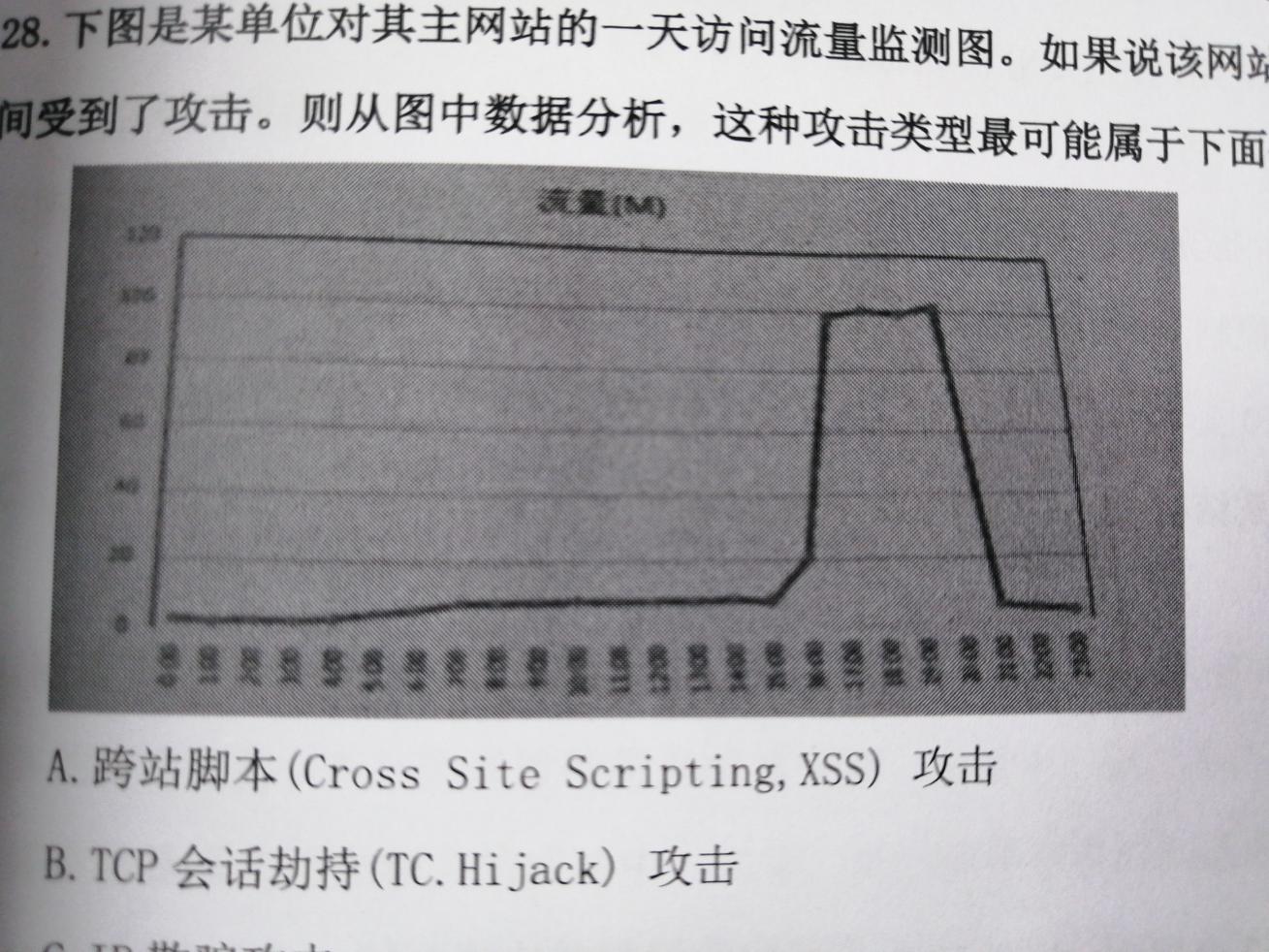
A.对于IPv4，IPSec是可选的，对于IPv6，IPSec是强制实施的。

B.IPSec协议提供对IP及其上层协议的保护。

C.IPSec是一个单独的协议。

D.IPSec安全协议给出了封装安全载荷和鉴别头两种通信保护机制。

28.下图是某单位对其主网站的一天访问流量监测图。如果说该网站在当天17：00到20：00间受到了攻击。则从图中数据分析，这种攻击类型最可能属于下面什么攻击。（D）



A.跨站脚本（Cross Site Scripting，XSS）攻击

B.TCP会话劫持（TC.Hijack）攻击4444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444444

C.IP欺骗攻击

D.拒绝服务（Denialof Service，DoS）攻击

29.某市环卫局网络建设是当地政府投资的重点项目。总体目标就是用交换式千兆以太网为主干，超五类双绞线作水平布线由大型的交换机和路由器连通几个主要的工作区域，在各区域建立一个闭路电视监控系统，再把信号通过网络传输到各监控中心，其中对交换机和路由器进行配置是网络安全中的一个不可缺少的步骤，下面对于交换机和路由器的安全配置，操作错误的是（A）

A.保持当前版本的操作系统，不定期更新交换机操作系统补丁

B.控制交换机的物理访问端口，关闭空闲的物理端口

C.可以利用单独的VLAN号进行带内管理，如果不能实现的话，可以利用单独的VLAN

D.安全促置它要的网路服务，关闭不必要的网络服务

30.私有IP地址是一段保留的IP地址。只使用在局域网中，无法在1atormot上做用。关于私有地址，下面描述正确的是（C）

A.A类和B类地此中没有私有地址，C类地址可以设置私有地址

B.A类地进中没有私有地址，B类和类地址中可以设置私有地址

C.A类、B类和C类地址中都可以设置私有地址

D.A类、B类和C类地址中都没有私有地址

31.以下哪一现不是工作在网络第二层的隧道协议（A）

A、VIP

B、L2F

C、PPTP

D、L2TP

32.下面哪一项不是虚拟专用网络（VN）协议标准（C）

A、第二层隧道协议（L.2Tp）

B、Internet 安全性（IPSEC）

C、终端访问控制器访问控制系统（TACACS+）

D、点对点隧道协议（PPTP）

33.在ISO的0SI安全体系结构中，以下哪一个安全机制可以提供抗抵赖安全服务（B）

A、加密

B、数字签名

C、访问控制

D、路由控制

34.在0SI参考模型中有7个层次，提供了相应的安全服务来加强信息系统的安全性，以下哪一层提供了保密性、身份鉴别、数据完整性服务（A）

A、网络层

B、表示层

C、会话层

D、物理层

35.以下关于互联网协议安全（Internet Protocol Security，IPsec）协议说法错误的是（D）

A、在传送模式中，保护的是IP负载

B.验证头拨（authentication liead.，A）和IP封装安全载荷协议EncapsulatinmgsecurityB.验证头拨（Authentication Head，AH）和IP封装安全载荷协议Encapsulatinmgsecurity Payload，ESP）都能以传输模式和隧道模式工作

C.在隧道模式中，保护的是整个互联网协议（1ntermetrotacol，I9包，包括IP头

D、IPsec仅能保证传输数据的可认证性和保密性

36.入保防御系统（IPS）是继入侵检测系统（IDS）后发展期出来的一项新的安全技术，它与IDS有着许多不同点，请指出下列哪一项描述不符合IPS的特点（D）

A、串接到网络线路中

B、对异常的进出流量可以直接进行阻断

C、有可能造成单点故障

D、不会影响网络性能

37.以下哪个不是导致地址解析协议（ARP）欺骗的根源之一（D）

A、ARP协议是一个无状态的协议

B、为提高效率，ARP信息在系统中会缓存

C、ARP缓存是动态的，可被改写

D、ARP协议是用于寻址的一个重要协议

39.随着高校业务资源逐渐向数据中心高度集中，Web成为一种普适平台，上面承载了越来越多的核心任务。Web的开放性带来丰富资源、高效率、新工作方式的同时，也使机构的重要信息暴露在越来越多的威胁中。去年，某个本科生院网站遭遇SQL.注入QMass SQL Injection.）攻击，网站发布的重要信息被靠改成为大量签名，所以该校在某信息安全公司的建议下配置了状态检测防火墙，其原因不包括（C）

A.状态检测防火墙可以应用会话信息决定过滤规则

B.状态检测防火墙具有记录通过每个包的详细信息能力

C.状态检测防火墙过滤规则与应用层无关，相比于包过滤防火墙更易安装和使用

D.状态检测防火墙结合网络配置和安全规定做出接纳、拒绝、身份认证或报警等处理动作

40.某集团公司的计算机网络中心内具有公司最重要的设备和信息数据。网络曾在一段时间内依然遭受了几次不小的破坏和干扰，虽然有防火墙，但系统管理人员也未找到真正的事发原因。某网络安全公司为该集团部署基于网络的入侵检测系统（NIDS），将IDS部署在防火墙后，以进行二次防御。那么NIDS不会在（D）区域部署。

A.DMZ

B.内网主干

C.内网关键子网

D.外网入口

41.小王是来通信运营商公司的网络安全架构师，为该公司推出的一项新型通讯系统项目做出安全架构规划，项目客户要求对他们的大型电子商务网络进行安全域的划分，化解为小区域的安全保护，每个逻辑区域有各自的安全访日控制和边界控制策略，以实现大规模电子商务系统的信息保护。小王对信息系统安全域（保护对象）的划分不需要考虑的是（D）

A.业务系统逻辑和应用关联性，业务系统是否需要对外连接

B.安全要求的相似性，可用性、保密性和完整性的要求是否类似

C.现有网络结构的状况，包括现有网路、地域和机房等

D.数据库的安全维护

43、“统一威胁管理”是将防病毒、入侵检测和防火墙等安全需求统一管理，目前市场已经出现了多种此类安全设备。这里“统一威胁管理”常常被简称为（A）

A.UTM

B.FW

C.IDS

D.SOC

44、IP地址用来标识不同的网络、子网以及网络中的主机。所调IP地址规划，是指根据IP编址特点，为所设计的网络中的节点、网络设备分配合适的IP地址。如某个小型网络拥有10个与互联网直接连接的IP地址，但是该网络内有15台个人计算机。假如这些计算机不会同时开机并连接互联网，那么可以将这10个互联网地址集中起来使用，当任意一台个人计算机开机并连接网络时，管理中心从这10个地址中任意抽取一个尚未分配的IP台个人计算机开机并连接网络时，管理中心从这10个地址中任意抽取一个尚未分配的IP 地址分配给这台计算机。他关机时，管理中心将该地址收回，并重新设置为未分配，那么上述的IP地址分配方式为（A）

A.动态分配地址

B.静态分配地址

C.NAT池分配地址

D.端口NAT分配地址

45.布式拒绝服务（Distributed Denial of srvice，o）或击指借助于客户/服务爆技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDos攻击，从而最倍地提高拒绝服务政击的成力，一般来说，DDoS攻击的主要目的是破坏目标系统的（C）

A.保密性

B.完整性

C.可用性

D.真实性

九、计算环境安全

1.以下关于SMTP和POP3协议的说法哪个是错误的（D）

A、SMTP和P0P3协议是一种旅于ASCI1编码的请求/响应模式的协议

B、SMTP和P0P3协议明文传输数据，因此存在数据震漏的可能

C、SMTP和P0P3协议缺乏严格的用户认证。因此导致了垃圾邮件问题

D、SMTP和POP3协议由于协议简单，易用性更高，更容易实现远程管理邮件

2.关于恶意代码，以下说法错误的是（B）

A、从传播范围来看，恶意代码呈现多平台传播的特征。

B、按照运行平台，恶意代码可以分为网络传播型病毒。文件传播型病毒。

C、不感染的依附性恶意代码无法单独执行

D、为了对目标系统实施攻击和破坏活动，传播途径是恶意代码赖以生存和紧确的基本条件

3.小王在某Wob软件公司工作，她在工作中主要负责对互联网信息服务（Intarm Information ervices，IIS）软件进行安全配置，这是属于（A）方面的安全工作。

A、Web服务支撑软件

B、Web应用程序

C、Web浏览器

D、通信协议

4.公司甲做了很多政府网站安全项目，在为网游公司乙的网站设计安全保障方案时，借鉴以前项目经验，为乙设计了多重数据加密安全措施，但用户提出不需要这些加密推施，理由是影响了网站性能，使用户访问量受限，双方引起争议。下面说法哪个是错误的（A）

A、乙对信息安全不重视，低估了黑客能力，不舍得花钱

B、甲在需求分析阶段没有进行风险评估，所部署的加密针对性不足，造成浪费

C、甲未充分考虑网游网站的业务与政府网站业务的区别

D、乙要综合考虑业务。合规性和风险，与甲共同确定网站安全需求

5.某公司系统管理员最近正在部署一台Web服务器，使用的操作系统是Windows，在进行日志安全管理设置时，系统管理员拟定四条日志安全策略给领导进行参考，其中能有效应对攻击者获得系统权限后对日志进行修改的策略是（A）

A、在网络中单独部署syslog服务器，将Web服务器的日志自动发送并存储到该syslog日志服务器中

B、严格设置Web日志权限，只有系统权限才能进行读和写等操作

C、对日志属性进行调整，加大日志文件大小，延长日志覆盖时间，设置记录更多信息等

D、使用独立的分区用于存储日志，并且保留足够大的日志空间

6.安全的运行环境是软件安全的基础，操作系统安全配置是确保运行环境安全必不可少的工作，某管理员对即将上线的Windows操作系统进行了以下四项安全部署工作，其中哪项设置不利于提高运行环境安全（B）

A、操作系统安装完成后安装最新的安全补丁，确保操作系统不存在可被利用的安全漏

B、为了方便进行数据备份，安装Windows操作系统时只使用一个分区C，所有数据和操作系统都存放在C盘

C、操作系统上部署防病毒软件，以对抗病毒的威胁

D、将默认的管理员账号Administrator改名，降低口令暴力破解攻击的发生可能

7.账号锁定策略中对超过一定次数的错误登录账号进行锁定是为了对抗以下哪种攻击（C）

A、分布式拒绝服务攻击（DDos）

B、病毒传染

C、口令暴力破解

D、缓冲区溢出攻击

8.数据库的安全很复杂，往往需要考虑多种安全策略，才可以更好地保护数据库的安全，以下关于数据库常用的安全策略理解不正确的是（B）

A、最小特权原则，是让用户可以合法的存取或修改数据库的前提下，分配最小的特权使得这些信息恰好能够完成用户的工作

B、最大共享策略，在保证数据库的完整性.保密性和可用性的前提下，最大程度地共享数据库中的信息

C、粒度最小策略，将数据库中的数据项进行划分，粒度越小，安全级别越高，在实际中需要选择最小粒度

D、按内容存取控制策略，不同权限的用户访问数据库的不同部分

9.应用软件的数据存储在数据库中，为了保证数据安全，应设置良好的数据库方护策略，以下不属于数据库防护策的是（D）

A、安装最新的数据库软件安全补丁

B、对存储的敏感数据进行安全加密

C、不使用管理员权限直接连择数据库系统

D、定期对数据库服务器进行重启以确保数据库运行良好

10.安全专家在对某网站进行安全部署时，调整了Apache的运行权限，从root权限降低为nobody用户，以下操作的主要目的是（C）

A、为了提高Apache 软件运行效率

B、为了提高Apache软件的可靠性

C.为了避免政击者通过Aache 获得root权限

D、为了减少Apache上存在的漏洞

11.在对某面向互联网提供服务的某应用服务器的是一算构安全的安全问题，服务器上开放了以下几个应用，除了一个应用外其他应用都存在明文传输数据的问题，作为一名检测人员，你需要告诉用户对应用进行安全整改以解决明文传输数据的问题，以下哪个应用已经解决了明文传输数据问题（A）

A、SSH

B、HTTP

C、FTP

D、SMTP

12.某linux系统由于root口令过于确单，被攻击者猜解后，管理员更改了root口令，并请安全专家对系统进行检测，在系统中发现有一个文件的权限如下：-r-s--x 1test test 10704 apr 15 2002/hone/test/sh请问以下描述哪个是正确的（D）

A、该文件是一个正常文件，test用户使用的shell，test不能读该文件，只能执行

B、该文件是一个正常文件，是test用户使用的shel1，但test用户无权执行该文件

C、该文件是一个后门程序，该文件被执行时，运行身份是root，test用户间接获得了root 权限

D、该文件是一个后门程序，由于所有者是test，因此运行这个文件时文件执行权限为test

13.在提高阿帕奇系统（Apache HTTP Server）系统安全性时，下面哪项措施不属于安全配置内容（A）

A、不在Windows下安装Apache，只在Linux和UNIX下安装

B、安装Apache时，只安装需要的组件模块

C、不使用操作系统管理员用户身份运行Apache，而是采用权限受限的专用用户账号来运行

D、积极了解Apache的安全通告，并及时下载和更新

14.某公司开发了一个游戏网站，但是由于网站软件存在问题，结果在软件上线后被黑客攻击，其数据库中的网游用户真实身份数据被黑客看到。关于此案例，下面描述正确的是（A）

A、该网站软件出现了保密性方面安全问题

B、该网站软件出现了完整性方面安全问题

C、该网站软件出现了可用性方面安全问题

D、该网站软件出现了不可否认性方面问题

15.以下关于账户密码策略中各项策略的作用说明，哪个是错误的（C）

A、“密码必须符合复杂性要求”是用于避免用户产生诸如1234、1111这样的弱口令

B、“密码长度最小值”是强制用户使用一定长度以上的密码

C、“强制密码历史”是强制用户不能再使用曾经使用过的任何密码

D、“密码最长存留期”是为了避免用户使用密码时间过长而不更改

16.某政府机构委托开发商开发了一个0A系统，其中有一个公文分发，公文通知等为WORD文档，厂商在进行系统设计时使用了FTP来对公文进行分发，以下说法不正确的是（C）

A、FTP协议明文传输数据，包括用户名和密码，攻击者可能通过会话过程嗅探获得FTPA、FTP协议明文传输数据，包括用户名和密码，攻击者可能通过会话过程嗅探获得FTP密码，从而威胁0A系统

B、FTP协议需要进行验证才能访问在，攻击者可以利用FTP进行口令的暴力破解

C、FIP协议已经是不太使用的协议，可能与新版本的浏览器存在兼容性问题

D、FTP应用需要安装服务器端软件，软件存在漏洞可能会影响到OA系统的安全

17.某公司在互联网区域新建了一个B网站，为了保护该网站主页安全性，尤其是不能让攻击者修改主页内容，该公司应当购买并部署下面哪个设备（B）

A、负载均衡设备

B、网页防篡改系统

C、网络防病毒系统

D、网络审计系统

18.以下可能存在sq1注入攻击的部分是（D）

A、get 请求参数

B、post 请求参数

C、cookie值

D、以上均有可能

19.以下关于Windows 系统账号存储管理机制SAM（Security Accounts Manager）的说法哪个是正确的（D）

A、存储在注册中的账号数据是管理员组用户都可以访问，具有较高的安全性

B、存储在注册表中的账号数据只有administrator账户才有权访问，具有较高的安全性

C、存储在注册表中的账号数据任何用户都可以直接访问，灵活方便

D、存储在注册表中的账号数据有只有System账户才能访问，具有较高的安全性

20.关于数据库恢复技术，下列说法不正确的是（D）

A.数据库恢复技术的实现主要依靠各种数据的冗余和恢复机制技术来解决。当数据库中数据被破坏时，可以利用冗余数据来进行修复

B、数据库管理员定期地将整个数据库或部分数据库文件备份到磁带或另一个磁盘上保存起来，是数据库恢复中采用的基本技术

C、日志文件在数据库恢复中起着排常重要的作用，可以用来进行事务故障恢复和系统故障恢复，并协助后备副本进行介质故障恢复

D、计算机系统发生故障导致数据未储存到固定存储器上，利用日志文件中故障发生的数据值，将数据库恢复到故障发生前的完整状态，这一对事务的操作称为提交

21.在windos7中，通过控制面板（管理工具-本地安全策略-安全设置-账户策略）可以进行操作系统的密码策略设置界面，下面哪项内容不能在该界面进行设置（D）

A、密码必须符合复杂性要求

B、密码长度最小值

C、强制密码历史

D、账号锁定时间

22.Linux系统中常用数字来表示文件的访问权限，假设某文件的访问权限使用了755 表示，则下面哪项是正确的（B）

A、这个文件可以被任何用户读和写

B、这个文件可以被任何用户读和执行

C、这个文件可以被任何用户写和执行

D、这个文件不可以被所有用户写和执行

23.Windows系统中，安全标识符（SID）是标识用户、组和计算机账户的唯一编码，在操作系统内部使用。当授予用户、组、服务或者其他安全主体访问对象的权限时，操作系统会把SID和权限写入对象的ACL中。小刘在学习了SID的组成后，为了巩固所学知识，在自己计算机的Windows 操作系统中使用whoami/users操作查看当前用户的SID。得到的SID为S-1-5-21-1534169462-1651380828-111620651-500。下列选项中，关于此SID的理解错误的是（D）

A、前三位S-1-5表示此SID是由Windows NT颁发的

B、第一个子颁发机构是21

C、Windows NT的SID的三个子颁发机构是1534169462、1651380828、111620651

D、此SID以500结尾，表示内置guest账户

24. /etc/passwd 文件是UNIX/Linux安全的关键文件之一。该文件用于用户登录时校验用户的登录名、加密的口令数据项、用户ID（UTD）、默认的用户分组ID（GID）、用户信息、

用户登录目录以及登录后使用的shel1程序。某黑客设法窃取了银行账户管理系统的passwd文件后，发现每个用户的加密的口令数据都显示为’x'。下列选项中，对此现的的解释正确的是（C）

A、黑客窃取的passwd文件是假的

B、用户的置录口令经过不可逆的加密算法加密结果为”x

C、加密口令被转移带了另一个文件里

D、这些账户都被禁用了

25.Linux系统的安全设置主要从磁盘上分区、账户安全设置、禁用危险服务、远程登录安全、用户鉴别安全、审计策略、保护root账户、使用网络防火墙和文件权限操作共10个方面来完成。小张在学习了Linux系统安全的相关知识后，尝试为自己计算机上的Linux 系统进行安全配置。下列选项是他的部分操作。其中不合理的是（A）

A、编辑文件/etc/passwd，检查文件中用户ID，禁用所有ID=0的用户

B、编辑文件/etcf/ssh/sshd\_config。将PermitRootLogin设置为no

C、编辑文件/etc/pam.d/systerauth，设置authrequire pamtally，so onerr-fai1deny-6 unlock-time=300

D、编辑文件/etc/profile，设置TMOUT=600

27.Apacheleb服务器的配置文件一般位于/usr/1ocal/apache/conf目录，如果需要修改配置文件禁止显示Banner 信息应该修改稿Apache目录的配置文件是（A）

A、httpd.conf

B、srm.conf

C、access，conf

D、inetd.conf

28.查询系统获得一个用户的SID值为：S-1-5-21-1559272821-92556266-105528598-500，请问关于一下SID的解读错误的是（A）

A、是一个GUEST用户

B、第一项S表示该字符串是SIDB、第一项S表示该字符串是SID

C、第二项1表示SID的版本号

D、三项5表示颁发机构就是NT，值是5

29.金女士经常通过计算机网络购物，从安全角度看，下面哪项是不好的操作习惯？（A）

A、使用专用上网购物用计算机，安装好软件后不要对该计算机上的系统软件应用软件进行升级

B、为计算机安装具有良好声誉的安全防范软件，包括病毒查杀、安全检查和安全加固方面的软件

C、在IE的配置中，设置只能下载和安装经过签名的、安全的Activex控件

D、在使用网络浏览器时，设置不在计算机中保留网络历史记录和表单数据

30.在1inux中，使用1s-al查看到一下文件权限为：rwsr-xr-x 3 user admin 1024 Sep 13：11：59 test 请问这个文件权限设置了哪个特殊的权限（A）

A、setUID位

B、setGID位

C、Set sticky位

D、设置执行权限

32.下面四款安全测试软件中，主要用于WEB安全扫描的是（B）

A、Cisco Auditing Tools

B.Acunetix Web Valnerability Scnmner

C、IAP

D.ISS Database Scanner

33.口令破解是针对系统进行攻击的常见方法，windova系统安全策略中应对口令破解的策略主要是帐户锁定策略和密码策略，关于这两个策略说明错误的是（C）

A.密码策略的主要作用是通过策略避免用户生产弱口令及对用户使用的口令进行管控

B.密码策略对系统所有用户都有效

C.帐户锁定策略的主要作用是应对口令暴力破解攻击，能有效的保护所有系统用户应对口令破解

D.帐户锁定策略只适用普通用户，无法保护管理员adaninistrator账户应对口令暴力破解攻击

34.加密文件系统（EFS）是windows操作系统的一个组件，下面说法错误的说（c）

A.EFS采用加密算法实现对文件的加密和解密，任何不具有解密密钥的个人或者程序都不能解密数据

B.EFS以公钥加密为基础，利用了windows系统中CryptoAPI体系结构

C.EFS加密系统用于NTFS和FAT32系统（windows环境下）

D.EFS加密过程对用户透明，EFS加密的用户验证过程是在登录windows时进行验证的

35.LINUX系统中，下列哪项内容不包括在/etc/passwd中（B）

A.用户名

B.用户口令明文

C.用户主目录

D.用户登录后使用的shel1

36.应用安全，一般是指保障应用程序使用过程和结果的安全，以下内容不属于应用安全的是（D）

A.身份鉴别，登录的用户进行身份鉴别

B.安全标记，在应用系统层面对主体和客体进行标记

C.剩余信息保护，加强硬盘内存或缓冲区中剩余信息的保护

D.机房与设施安全，保证应用系统处于一个有安全保障的环境，包括机房的建造和装修等

37.关于恶意代码的守护进程的功能，以下说法正确的是（D）

A.隐藏恶意代码

B.加大检测难度

C.传播恶意代码

D.监视恶意代码主体程序是否正常

39.相比文件配置表（FAT）文件系统，以下以哪个不是新技术文件系统NTS）所具有的优势（D）

A、NIRS使用事务日志自动记录所有文件夹和文件更新，当出现系统损坏和电源故障等问题而引起操作失败后，系统能利用日志文件重做或恢复未成功的操作

B.TFS的分区上，可以为每个文件或文件夹设置单独的许可权限

C、对于大磁盘，NTFS文件系统比FAT有更高的磁盘利用率

D、相比NTFS文件系统，FAT文件系统能有效的兼容Linux 下EXT2文件格式

40.关于1inux下的用户和组，以下描述不正确的是（C）

A、在1inux中，每一个文件和程序都归属于一个特定的“用户”

B、系统中的每一个用户都必须至少属于一个用户组

C、用户和组的关系可以是多对一，一个组可以有多个用户，一个用户不能属于多个组

D、root 是系统的超级用户，无论是否文件和程序的所有者都具有访问权限

41.在数据库安全性控制中，授权的数据对象（A），授权子系统就越活

A、粒度越小B、约束越细致C、范围越大D约束范围大

42.下面哪一项安全控制措施不是用来检测未经授权的信息处理活动的（A）

A、设置网络连接时限

B、记录并分析系统错误日志

c、记录并分析用户和管理员操作日志

D、启用时钟同步

43.假设一个系统已经包含了充分的预防控制措施，那么安装监测控制设备（c）

A、是多余的，因为它们完成了同样的功能，但要求更多的开销

B、是必须的，可以为预防控制的功效提供检测

C、是可选的，可以实现深度防御

D、在一个人工系统中是需要的，在一个计算机系统中则是不需要的，因为预防控制的功能已经足够

44.操作系统用于管理计算机资源，控制整个系统运行，是计算机软件的基础。操作系统安全是计算、网络及信息系统安全的基础。一般操作系统都提供了相应的安全配置接口。小王新买了一台计算机，开机后首先对自带的Windows操作系统进行配置。他的主要操作有：1）关闭不必要的服务和端口；2）在“在本地安全策略”重配置账号策略、本地策略、公钥策略和IP安全策略；3）备份敏感文件，禁止建立空连接，下载最新补丁；4）关闭审核策略，开启口令策略，开启账号策略。这些操作中错误的是（D）

A.操作（1），应该关闭不必要的服务和所有端口

B.操作（2），在“本地安全策略”中不应该配置公钥策略，而应该配置私钥策略

C.操作（3），备份敏感文件会导致这些文件遭到窃取的几率增加

D.操作（4），应该开启审核策略

46.从Linux内核2.1版开始，实现了基于权能的特权管理机制，实现了超级用户的特权分割，打破了UWIX/LINMUX操作系统中超级用户/普通用户的概念，提高了操作系统的安全性。下列选项中，对特权管理机制的理解错误的是（B）

A.普通用户及其shel1没有任何权能，而超级用户及其shel1在系统启动之初拥有全部权能

B.系统管理员可以剥夺和恢复超级用户的某些权能

C.进程可以放弃自己的某些权能

D.当普通用户的某些操作设计特权操作时，仍然通过setuid实现

48.关系数据库的完整性规则是数据库设计的重要内容，下面关于“实体完整性”的描述正确的是（B）

A.指数据表中列的完整性，主要用于保证操作的数据（记录）完整、不丢项

B.指数据表中行的完整性，主要用于保证操作的数据（记录）非空、唯一且不重复

C.指数据表中列必须满足某种特定的数据类型或约束，比如取值范围、数值精度等约束

D.指数据表中行必须满足某种特定的数据类型或约束，比如在更新、插入或删除记录时，要将关联有关的记录一并处理才可以

49.安全多用盖互联网邮件护展（Scure ultipurose Imtornet MailPxtansicn，SAmE）是指一种保障邮件安全的技术，下面描述错误的是（C）

A.SAE采用了非对称密码学机制

B.S/MIME支持数字证书

C.SAE采用了邮件防火墙技术

D.S/MIME支持用户身份认证和邮件加密

5l.Apache HTP Server（简称Apache）是一个开放源码的Wab服务运行平台，在使用过程中，该软件默认会将自己的软件名和版本号发送给客户端。从安全角度出发，为隐藏这些信息，应当采取以下哪种措施（B）

A不选择Windows平台，应选择在Linux平台下安装使用

B.安装后，修改配置文件httpd.conf中的有关参数

C.安装后，删除Apache HTTP Server码

D.从正确的官方网站下载Apeche HTTP Server，并安装使用

58.Internet Explorer，简称IE，是微软公司推出的一款Web浏览器，TE中有很多安全设置选项，用来设置安全上网环境和保护用户隐私数据。以下哪项不是IE中的安全配置项目（C）

A设置Cookie安全，允许用户根据自己安全策略要求者、设置Cookie策略，包括从阻止所有Cookie到接受所有Cookie，用户也可以选择删除已经保存过的Cookie从阻止所有Cookie到接受所有Cookie，用户也可以选择删除已经保存过的Cookie

B.禁用自动完成和密码记忆功能，通过设置禁止IE自动记忆用户输入过的Web地址和表单，也禁止IE自动记忆表单中的用户名和口令信息

C.设置每个连接的最大请求数，修改MaxKeepAlivREquests，如果同时请求数达到阅值就不再响应新的请求，从而保证了系统资源不会被某个链接大量占用

D.为网站设置适当的浏览器安全级别，用户可以将各个不同的网站划分到Internet、本地Internet、受信任的站点、受限制的站点等不同安全区域中，以采取不同的安全访问策略

53.下面对“零日（zero-day）漏洞”的理解中，正确的是（D）

A.指一个特定的漏洞，该漏洞每年1月1日零点发作，可以被攻击者用来远程攻击，获取主机权限

B.指一个特定的漏洞，特指在2010年被发现出来的一种漏洞，该漏洞被“震网”病

毒所利用，用来攻击伊朗布什尔核电站基础设施

C指-类漏洞几特别好被利用，一旦成功，可以在1天内完成攻击，且成功达到攻击目标

D指一类漏洞，即刚被发现后立即被恶意利用的安全部洞。一般来说，那些已经被小部分人发现，但是还未公布、还不存在安全补丁的漏洞都是零日漏洞

54.为达到预期的政击目的，恶意化码通常会采用各种方法将自己隐藏起来。关于隐藏方法，下面理解错误的是（C）

A.隐藏悉意代码进程，即将恶意代码进程隐藏起来，或者改名和使用系统进程名，以更好的躲避检测，迷惑用户和安全检测人员

B.隐藏恶意代码的网络行为，复用通用的网络端口，以躲避网络行为检测和网络监控

C.隐藏恶意代码的源代码，删除或加密源代码，仅留下加密后的二进制代码，以躲避用户和安全检测人员

D.隐藏恶意代码的文件，通过隐藏文件、采用流文件技术或K技术、以躲避系统文件检查和清除

57、小张新购入了一台安装了Windovs操作系统的笔记本电脑，为了提升操作系统的安全性，小张在Windors系统的“本地安全策略”中，配置了四类安全策略：账号策略、本地策略、公钥策略和IP安全策略。那么该操作属于操作系统安全配置内容中的（B）

A.关闭不必要的服务

B.制定操作系统安全策略

C.关闭不必要的端口

D.账户审核策略

十．软件安全开发

2.当前，应用软件安全已经日益引起人们的重视，每年新发现的应用软件漏洞已经占新发现漏洞总数一半以上。下列选项中，哪个与应用软件漏洞成因无关（C）

A、传统的软件开发工程未能充分考虑安舍因素

B、开发人员对信息安全知识掌握不足

C、相比操作系统而言，应用软件编码所采用的高级语言更容易出现漏洞

D、应用软件的功能越来越多，软件越来越复杂，更容易出现漏洞

4.为了保障系统安全，某单位需要对其跨地区大型网络实时应用系统进行渗透测试，以下关于渗透测试过程的说法不正确的是（D）

A、由于在实际渗透测试过程中存在不可预知的风险，所以测试前要提醒用户进行系统

和数据备份，以便出现问题时可以及时恢复系统和数据

B、渗透测试从“逆向”的角度出发，测试软件系统的安全性，其价值在于可以测试软

件在实际系统中运行时的安全状况

C、渗透测试应当经过方案制定、信息收集、漏洞利用、完成渗透测试报告等步骤

D、为了深入发掘该系统存在的安全威胁，应该在系统正常业务运行高峰期进行渗透测试

6.为增强Web应用程序的安全性，某软件开发经理决定加强Web软件安全开发培训，下面哪项内容不需要在他的考虑范围内（D）

A、关于网站身份签别技术方面安全知识的培训

B、针对OpenSSL心脏出血漏洞方面安全知识的培训

C、针对SOQL注入漏洞的安全编程培训

D、关于ARM系统漏洞挖掘方面安全知识的培训

8.业务系统运行中异常错误处理合理的方法是（D）

A、让系统自己处理异常

B、调试方便，应该让更多的错误更详细的显示出来

C、捕获错误，并抛出前台显示

D、捕获错误，只显示简单的提示信息，或不显示任何信息

9.由于频繁出现软件运行时被黑客远程攻击获取数据的现象，某软件公司准备加强软件安全开发管理，在下面做法中，对于解决问题没有直接帮助的是（A）

A、要求开发人员采用敏捷开发模型进行开发

B、要求所有的开发人员参加软件安全意识培训

C、要求规范软件编码，并制定公司的安全编码准则

D、要求增加软件安全测试环节，尽早发现软件安全问题

10.某购物网站开发项目经过需求分析进入系统设计阶段，为了保证用户账户的安全，项目开发人员决定用户登录时如果用户名或口令输入错误，给用户返“用户名或口令输入错误”信息，输入错误达到三次将暂时禁止登录该账户，请问以上安全设计遵循的是哪项安全设计原则（C）

A、最少共享机制原则

B、经济机制原则

C、不信任原则

D、默认故障处理保护原则

11.某网站为了开发的便利，sa连接数据库，由于网站满本中被发现存在SQL注入漏洞，导致政击者利用内置存储过程XP\_CDSELL删除了系统中的一个重要文件，在进行问题分析时，作为安全专家，你应该指出该网站设计违反了以下哪项原则（B）

A、权限分离原则

B、最小特权原则

C、保护最薄弱环节的原则

D、纵深防御的原则

13.某集团公司根据业务需要，在各地分支机构部署前置机，为了保证安全，集团总部要求前置机开放日志共享，由总部服务器采集进行集中分析，在运行过程中发现攻击者也可通过共享从前置机中提取日志，从而导致部分敏感信息泄露，根据降低攻击面的原则，应采取以下哪项处理措施？（D）

A、由于共享导致了安全问题，应直接关闭日志井享，禁止总部提取日志进行分析

B.为配合总部的安全策略，会带来一定的安全问题，但不影响系统使用，因此接受此风险

C、日志的存在就是安全风险，最好的办法就是取消日志，通过设置让前置机不记录日志

D、只允许特定的IP地址从前置机提取日志，对日志共享设置访问密码且限定访问的时间

16.某网站为了更好向用户提供服务，在新版本设计时提供了用户快捷登录功能，用户如果使用上次的IP地址进行访问，就可以无需验证直接登录，该功能推出后，导致大量用户账号被盗用，关于以上问题的说法正确的是（D）

A、网站问题是由于开发人员不熟悉安全编码，编写了不安全的代码导致攻击面增大，

产生此安全问题

B、网站问题是由于用户缺乏安全意识导致，使用了不安全的功能，导致网站攻击面增大，产生此问题

C、网站问题是由于使用便利性提高带来网站用户数增加，导致网络攻击面增大，产生此安全问题

D、网站问题是设计人员不了解安全设计关键要素，设计了不安全的功能，导致网站攻击面增大，产生此安全问题

20.某网站在设计时经过了威胁建模和和功击面分析，在开发时要求程序编写安全代码，由于管理员将备份存放在Web目录导致了攻击者可以直接下载备份，为了发现类似问题，以下哪种测试方式是最佳的测试方式（C）

A.模糊测试

B.源代码测试

C.渗透测试

D.软件功能测试

21.对抗检测技术，哪一个是动态反调试技术（C）

A加亮B.代码混滑C.禁止跟踪中断D.加密

22.关于源代码审核，下列说法正确的是（D）.

A.源代码审核往往需要大量的时间，采用人工审核费时费力，但可以通过多人并行审核来弥补这个缺点

B.源代码审核工具应当以检查源代码的功能是否完整、是否执行正确为主要功能

C.使用源代码审核工具自动化执行代码检查和分析，能够极大提高软件可靠性并节省软件开发和测试的成本，已经取代了人工审核方式

D.源代码审核是指无需运行被测代码，仅对源代码检查分析检测并报告源代码中可能隐藏的错误和缺陷

23.某购物网站开发项目经过需求分析进入系统设计阶段，项目开发人员决定用户输入的信息，无论是用户名、口令，还是查询内容，都需要进行校验或检查，请问以上安全设计遵循的是哪项安全设计原则（B）

A.公开设计原则

B.不信任原则

C.隐私保护原则

D.心理可接受程度原则

你验证就可以样决真需要求司求音称介入，严想政市者细可

B.该问题的产生不是网站的问题，应报警要，本了高享在发生

26.小李在检查公司对外服务网站的源代网时，发现诸如没有找到资源、数据库连接错误、写临时文件错等问题，会将详细的错误原因在结果页面显示出来。从安全角度考虑，小李决定修改代码，将详细的错误原因隐藏起来，在页面上仅显示“抱歉，发生内部错误”，请问这样做的主要目的是（D）。

A.避免缓冲区溢出

B.安全处理系统异常

C.安全使用临时文件

D.最小化反馈信息

27.某单位开发了一个面向互联网提供服务的应用网站，该单位委托软件测评机构对软件进行了源代码分析、模据测试等软件安全性测试在应用上线前，项目经理提出了还需要对应用网站进行一次渗透性测试，作为安全主管，你需要提出渗透性测试相比源代码测试模糊测试的优势给领导做决策，以下哪条是渗透性测试的优势（A）

A、渗透测试以攻击者的思维模拟真实攻击，能发现如配置错误等运行维护期产生的漏洞

B、渗透测试是用软件代替人工的一种测试方法，因此测试效率更高

C、渗透测试使用人工进行测试，不依赖软件，因此测试更准确

D、渗透测试中必须要查看软件源代码，因此测试中发现的漏洞更多

28.软件安全设计和开发中应考虑用户稳私保护，以下关于用户隐私保护的说法哪个是错误

的（c）

A、告诉用户需要收集什么数据及搜集到的数据会如何披使用

B、当用户的数据由于某种原因要被使用时，给用户选择是否允许

C、用户提交的用户名和密码属于稳私数据，其它都不是

D、确保数据的使用符合国家、地方、行业的相关法律法规

29.某单位人员管理系统在人员离职时进行账号删除，需要离职员工所在部门主管经理和人事部门人员同时进行确认才能在系统上执行，该设计是遵循了软件安全设计中的哪项原则（B）

A、最小权限B、权限分离C、不信任D、纵深防御

31.在进行应用系统的测试时，应尽可能避免使用包含个人稳私和其它敏感信息的实际生产系统中的数据，如果需要使用时，以下哪一项不是必须做的（B）

A、测试系统应使用不低于生产系统的访问控制措

B、为测试系统中的数据部署完善的备份与恢复措

C、在测试完成后立即清除测试系统中的所有敏感数

D、部署审计措施，记录生产数据的拷贝和使用

32.为了保证系统日志可靠有效，以下哪一项不是日志必需具备的特征（D）

A、统一而精确地的时间

B、全面覆盖系统资产

C、包括访问源、访问目标和访问活动等重要信息

D.可以让系统的所有用户方便的读取

36、某购物网站开发项目经过需求分析进入系统设计阶段，为了保证用户账户的安全，项目开发人员决定用户登录时除了用户名口令认证方式外，还加入基于数字证书的身份认证功能，同时用户口令使用SHA-1算法加密后存放在后台数据库中，请问以上安全设计遵循的是哪项安全设计原则（C）

A.最小特权原则

B.职责分离原则

C.纵深防御原则

D.最少共享机制原则

37、某单位需要开发一个网络，为了确保开发出安全的软件，软件开发商进行了0A系统的威胁建模，根据威胁建模，SQL注入是网站系统面临的攻击威胁之一，根据威胁建模的消减威胁的做法，以下哪个属于修改设计消除威胁的做法（C）

A、在编码阶段程序员进行培训，避免程序员写出存在漏洞的代码

B、对代码进行严格检查，避免存在SOL注入漏洞的脚本被发布

C、使用静态发布，所有面向用户发布的数据都使用静态页面

D、在网站中部署防SQL注入脚本，对所有用户提交数据进行过滤

38、某银行网上交易系统开发项目在设计阶段分析系统运行过程中可能存在的攻击，请问以下拟采取的安全措施中，哪一项不能降低系统的受攻击面（B）

A、临时用户访问需进行身份认证

B、某些用户访问时具有管理员权限

C、关闭服务器端不必要的系统服务

D、访问其他账户信息时使用严格的身份认证机制

39、以下关于模糊测试过程的说法正确的是（C）

A.模糊测试的效果与覆盖能力，与输入样本选择不相关

B.为保障安全测试的效果和自动化过程，关键是将发现的异常进行现场保护记录，系统可能无法恢复异常状态进行后续的测试

C.通过异常样本重现异常，人工分析异常原因，判断是否为潜在的安全副洞，如果是安全漏洞，就需要进一步分析其危害性、影响范围和修复建议

D.对于可能产生的大量异常报告，需要人工全部分析异常报告

40.某单位门户网站开发完成后，测试人员使用模糊测试进行安全性测试，以下关于模糊测试过程的说法正确的是（D）

A.模拟正常用户输入行为，生成大量数据包作为测试用例

B.数据处理点.数据通道的入口点和可信边界点往往不是测试对象

C.监测和记录输入数据后程序正常运行的情况

D.深入分析网站测试过程中产生崩溃或异常的原因，必要时需要测试人员手工重现并分析

复习题（二）

2.张主任的计算机使用Windows7操作系统，他常登录的用户名为zhang，张主任给他个人文件夹设置了权限为只有zhang这个用户有权访问这个目录，管理员在某次维护中无意将zhang这个用户删除了，随后又重新建了一个用户名为zhang，张主任使用zhang这个用户登录系统后，发现无法访问他原来的个人文件夹，原因是：（B）

A.任何一个新建用户都需要经过授权才能访问系统中的文件B

B.Windows7不认为新建立的用户zhang与原来的用户zhang是同一个用户，因此无权访问

C.用户被删除后，该用户创建的文件夹也会自动删除，新建用户找不到原来用户的文件夹，因此无法访问

D.新建的用户zhang会继承原来用户的权限，之所以无权访问是因为文件夹经过了加密

3.Windows文件系统权限管理访问控制列表（Access Control List，ACL）机制，以下哪个说法是错误的：（C)

A.安装Windows系统时要确保文件格式使用的是NTFS，因为Windows的ACL机制需要NTFS文件格式的支持

B.由于Windows操作系统自身有大量的文件和目录，因此很难对每个文件和目录设置严格的访问权限，为了使用上的便利，Windows上的ACL存在默认设置安全性不高的问题

C.Windows的ACL机制中，文件和文件夹的权限是与主体进行关联的，即文件夹和文件的访问权限信息是写在用户数据库中

D.由于ACL具有很好的灵活性，在实际使用中可以为每一个文件设定独立用户的权限

4.加密文件系统（Encrypting File System，EFS）是Windows操作系统的一个组件。以下说法错误的是（C）。

A.EFS采用加密算法实现透明的文件加密和解出，任何不拥有合适密切的个人或者程序不能加密数据

B.EFS以公钥加密为基础，并利用了Windows系统中的Cry0toAP1体系结构

C.EFS加密系统话用于NTFS文件系统和FAT32文件系统（Windows7环境下）

B.ES加密过程对用户遗明，ES加密的用户验证过程是在登录windows时进行的

5.某单位发生的管理员小张在繁忙的工作中接到了一个电话，来电者：小张吗？我是科技处李强，我的邮箱密码忘记了，现在打不开邮件，我着急收个邮件，麻频你先帮我把密码改成123，我收完邮件自己修改掉密码。热心的小张很快的满足了来电者的要求。随后，李强发现有向系统登录异常。请问以下说法哪个是正确的？（C）

A.小张服务态度不好，如果把李强的邮件收下来亲自教给李强就不会发生这个问题

B.事件属于服务器故障，是偶然事件，影响单位领导申请购买新的服务器

C.单位缺乏良好的密码修改操作流程或者小张没按操作流程工作

D.事件属于邮件系统故障，是偶然事件，应向单位领导申请升级邮件服务软件

6.某单位计划在今年开发一套办公自化（OA）系统，将集团公司各地的机构通过互联网进行协同办公，在0A系统的设计方案评审会上，提出了不少安全开发的建议，作为安全专家，请指出大家提供的建议中不太合适的一条？（C）

A.对软件开发商提出安全相关要求，确保软件开发商对安全足够的重视，投入资源解决件

安全问题

B.要求软件开发人员进行安全开发培训，使开发人员掌握基本软件安全开发知识

C.要求软件开发商使用Java而不是ASP作为开发语言，避免产生SQL注入漏洞

D.要求软件开发商对软件进行模块化设计，各模块明确输入和输出数据格式，并在使用前对输入数据进行校验

7.下面有关软件安全问题的描述中，哪项应是由于软件设计缺陷引起的（c）

A.设计了三层WEB架构，但是软件存在SQL注入漏洞，导致被黑客攻击后直接访问数据

B.使用C语言开发时，采用了一些存在安全问题的字符串处理函数，导致存在缓冲区滋出漏洞

C.设计了缓存用户隐私数据机制以加快系统处理性能，导致软件在发布运行后，被黑客攻击获取到用户隐私数据

D.使用了符合要求的密码算法，但在使用算法接口时，没有按照要求生成密。导致黑客政击后能破解并得到明文数据

21.以下哪种风险被认为是合理的风险（D）

A.最小的风险

B.残余的风险

C.未识别的风险

D.可接受的风险

22.在Linux系统中，下列哪项内容不包含在/etc/passwd文件中（B）、

A.用户名B.用户口令C.用户主目录D.用户登录后使用的SHELL

26.访问控制是对用户或用户访问本地或网络上的域资源进行法令一种机制。在windows2000以后的操作系统版本中，访问控制是一种双重机制，它对用户的授权基于用户

权限和对象许可通常使用ACI、访问令牌和授权管理器来实现访问控制功能，以下造项中对Windows操作系统访同控制实现方法的理解错误的是（A）

A.ACL只能由管理员进行管理

B.ACL是对象安全描述的基本组成部分，它包括有权访问对象的用户和级的SID

C.访问令牌存储着用户的SID，组信息和分配给用户的权限

D.通过授权管理器，可以实现基于角色的访问控制

27.2016年9月，一位安全研究人员在CoglecloudIP上通过扫播，发现了完整的美国路易斯安邦州290万选民数据库。这套数据库中囊括了诸如完整姓名、电子邮箱地址、性别与种族、选民状态注册日期与编号政党代码和密码，以防止攻击者利用以上信息进行（）攻击。（B）

A.默认口令

B.字典

C.暴力

D.XSS

28.基于TCP的主机在进行一次TCP连接时简要进行三次握手，请求通信的主机A要与另一台主机B建立连接时，A需要先发一个SYN数据包向B主机提出连接请示，B收到后，回复一个ACK/SYN确认请示给A主机，然后A再次回应ACK数据包，确认连接请求。攻击通过伪造带有虚假源地址的SYN包给目标主机，使目标主机发送的ACK/SYN包得不到确认。一般情况下，目标主机会等一段时间后才会放弃这个连接等待。因此大量虚假SYN包同时发送到目标主机时，目标主机上就会有大量的连接请示等待确认，当这些未释放的连接请示数量超过目标主机的资源限制时。正常的连接请示就不能被目标主机接受，这种SYNPlood数量超过目标主机的资源限制时。正常的连接请示就不能被目标主机接受，这种SYNPlood攻击属于（A）

A.拒绝服务攻击

B.分布式拒绝服务攻击

C.缓冲区溢出攻击

D.SQL注入攻击

29.信息安全是国家安全的重要组成部分，综合研究当前世界各国信息安全保障工作，下面总结错误的是（C）

A.各国普遍将与国家安全、社会稳定和民生密切相关的关键基础设施作为信息安全保障的重点

B.各国普遮重视战略规划工作，逐步发布网络安全战略、政策评估报告、推进计划等文件

C.各国普遮加强国际交流与对话，均同意建立一致的安全保障系统，强化各国安全系统互通

D.各国普避积极推动信息安全立法和标准规范建设，廉视应急响应、安全监管和安全测评

30.某社交网站的用户点击了该网站上的一个广告。该广告含有一个跨站脚本，会将他的浏览器定向到旅游网站，旅游网站则获得了他的社交网络信息。虽然该用户没有主动访问该旅游网站，但旅游网站已经截获了他的社交网络信息（还有他的好友们的信息），于是犯罪分子便可以躲藏在社交网站的广告后面，截获用户的个人信息了，这种向Web页面插入恶意html代码的攻击方式称为（B）

A.分布式拒绝服务攻击

B.跨站脚本攻击

C.SOL注入攻击

D.缓冲区溢出攻击

31.模糊测试，也称Fuzz测试，是一种通过提供非预期的输入并监视异常结果来发现软件故障的方法。下面描述正确的是（A）

A.模糊测试本质上属于黑盒测试

B.模糊测试本质上属于白盒测试

C.模糊测试有时属于黑盒测试，有时属于白盒测试，取决于其使用的测试方法

D.模糊测试既不属于黑盒测试，也不属于白盒测试

32.某信息安全公司的团队对某款名为“红包快抢”的外挂进行分析发现此外挂是一个典型的木马后门，使黑客能够获得受害者电脑的访问权，该后门程序为了达到长期驻留在受害者的计算机中，通过修改注册表启动项来达到后门程序随受害者计算机系统启动而启动为防范此类木马的攻击，以下做法无用的是（c）

A.不下载、不执行、不接收来历不明的软件和文件

B.不随意打开来历不明的邮件，不浏览不健康不正规的网站

C.使用共享文件夹

D.安装反病毒软件和防火墙，安装专门的木马防范软件

38.超文本传输协议（HyperText Transfer Protocol，HTTP）是互联网上广泛使用的一种网络协议，下面哪种协议基于HTTP并结合SSL协议，具备用户鉴别和通信数据加密等功能（C）

A.HTTP1.0协议

B.HTTP1.1协议

C.HTTPS协议

D.HTTPO协议

43.某软件在设计时，有三种用户访问模式，分别是仅管理员可访问，所有合法用户可访问和允许匿名访问，请问采用这三种访问模式时，攻击面最高的是（C）

A.仅管理员可访问

B.所有合法用户可访问

C.允许匿名访问

D.三种方式一样

44.国家科学技术秘密的密级分为绝密级.机密级.密级，以下哪块属于绝密级的描述？（D）

A.处于国际先进水平。并且有军事用途或者对经济建设具有重要影响的

B.能够局部及应国家防制和治安实力的

C.我国独有.不要自己条件因素制约.能体现民族特色的精华，并且社会效益或者经济效益显著的传统工艺

D.国际领先。并且对国防建设或者经济建设具有特别重大影响的

47.某银行网上交易系统开发项目在设计阶段分析系统运行过程中可能存在的攻击，请问以下哪一项工作不能降低该系统的受攻击面：（D）

A.分析系统功能的重要性

B.分析从哪里可以访问这些功能

C.采取合理措施降低特权

D分析系统应满足的性能要求

51.TCP/IP协议是Intarnet最基本的协议，也是Internet构成的基础，TCP/IP通常被认为是一个N层协议，每一层都使用它的下一层所提供的网络服务来完成自己的功能，这里N应等于（A）。

A.4

B.5

C.6

D.7

53.某电子商务网站架构设计时，为了避免数据误操作，在管理员进行订单删除时，需要由审核员进行审核后该操作才能生效，这种设计是遵循了以下哪个原则：（A）

A.权限分离原则

B.最小特权原则

C.保护XXX环节的原则

D.纵深防御的原则

54.关于计算机取证描述不正确的是（C）

A.计算机取证是使用先进的技术和工具，按照标准规程全面地检查十算机系统，以提取和保护有关计算机犯罪的相关证据的活动

B.取证的目的包括：通过证据查找肇事者.通过证据推断犯罪过程.通过证据判断受害者损失程度及收集证据提供法律支持

C.电子证据是计算机系统运行过程中产生的各种信息记录及存储的电子化资料及物品。对于电子证据，取证工作主要围绕两方面进行：证据的获取和证据的保护

D.计算机取证的过程可以分为准备。保护.提取.分析和提交5个步骤

56.某攻击者想通过远程控制软件潜伏在某监控方的Unix系统的计算机中，如果攻击者打算长时间地远程监控某服务器上的存储的敏感数据，必须要能够清除在监控方计算机中存在的系统日志。否则当监控方查看自己的系统日志的时候，就会发现被监控以及访问的痕迹。不属于清除痕迹的方法是（C）

A.窃取root 权限修改wtmp/wtmpx、utmp/utmpx和last 1og三个主要日志文件

B.采用干扰手段影响系统防火墙的审计功能

C.保留攻击时产生的临时文件

D.修改登录日志，伪造成功的登录日志，增加审计难度

57.某银行网上交易系统开发项目在设计阶段分析系统运行过程中可能存在的攻击，请问以下拟采取的安全措施中，哪一项不能降低该系统的受攻击面：（B）

A.远程用户访问需进行身份管理

B.远程用户访问时具有管理员权限

C.关闭服务器端不必要的系统服务

D.当用户访问其账户信息时使用严格的身份认证机制

58.在工程实施阶段，监理机构依据承建合同、安全设计方素、实施方案、实施记录国家或地方相关标准和技术指导文件，对信息化工程（）进行安全检查，以验证项目是否实现了项目设计目标和安全等级要求。（D）

A.功能性

B.可用性

C.保障性

D.符合性

62.一个信息管理系统通常会对用户进行分组并实施访问控制。例如，在一个学校的教务统中，教师能够录入学生的考试成绩学生只能查看自己的分数，而学校教务部门的管理员能够对课程信息、学生的选课信息等内容进行修改。下列选项中，对访问控制的作用的解错误的是（A）。

A.对经过身份鉴别后的合法用户提供所有服务

B.拒绝非法用户的非授权访问请求

C.在用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理

D.防止对信息的非授权幕改和滥用

63.小陈某电器城购买了一台冰箱，并留下了个人姓名、电话和电子邮件地址等信息，第二天他收了一封邮件他中奖的邮件，查看该邮件后他按照提示操作缴纳中奖税款后并没有得到中奖奖金，再打电话询问电器城后，才得知电器城共没有中奖的活动。在此案例中，下面描述错误的是（D）

A.小陈应当注意保护自己的隐私，没有必要告诉别人的信息不要登记和公和给别人

B.小陈钱被偷走了，这类网络犯罪哪案件也应该向公安局报案

C.邮件服务运营高商通过技术手段，可以在一定程度上阻止此类的钓鱼邮件和哄骗邮件

D.小陈应当向电器城索赔，追回损失

73.与浏览器兼容性测试不需要考虑的问题是（B）

A、软件是否可以在不同的J2EE中运行

B、不同的浏览器是否可以提供合适的安全设置

C、脚本和插件是否适用于不同的浏览器

D、符合最新HTML版本的页面能否在浏览器中正确显示

74.下列关于测试方法的叙述中不正确的是（D）

A.从某种角度上讲，白盒测试与黑盒测试都属于动态测试

B.功能测试属于黑盒测试

C.结构测试属于白盒测试

D.对功能的测试通常是要考虑程序的内部结构的

75.小王学习了灾难备份的有关知识，了解到常用的数据备份方式包括完全备份、增量备份、差量备份，为巩固所学知识，小王对这三种备份方式进行对比，其中在数据恢复速度方面三种备份方式由快到慢的顺序是（B）

A、完全备份、增量备份、差量备份

B、完全备份、差量备份、增量备份

C、增量备份、差量备份、完全备份

D、差量备份、增量备份、完全备份

76.以下哪一项不属于Web应用软件表示层测试关注的范畴（B）

A、排版结构的测试

B、数据完整性测试

C、客户端兼容性的测试

D、链接结构的测试

78.以下哪些不是《国家网络安全空间战略》中阐述的我国网络安全当前任务？（D）

A.捍卫网络安全主权

B.保护关键信息基础设施

C.提升网络安全防护能力

D.阻断与国外网络连接

79.王明买了一个新的蓝牙耳机，但王明听说使用蓝牙设备有一定的安全威胁，于是王明找到了对蓝牙技术有所了解的王红，希望王红能够给自己一点建议，以下哪一条建议不可取（C）

A.在选择使用蓝牙设备时，应考虑设备的技术实现及设置是否具备防止上述安全威胁的能力

B.选择使用功能合适的设备而不是功能尽可能多的设备，尽量关闭不使用的服务及功能

C.如果蓝牙设备丢失，最好不要做任何操作

D.在配对时使用随机生成的密钥，不使用时设置不可被其他蓝牙设备发现

96.以下对Kerberos协议过程说法正确的是（D）

A.协议可以分为两个步骤；一是用户身份鉴别：二是获取请求服务

B.协议可以分为两个步骤：一是获取票据许可票据；二是获得请求服务

C.协议可以分为三个步骤：一是用户身份鉴别二是获得票据许可票据：三是获得服务许可服务

D.协议可以分为三个步骤：一是获得票据许可票据：二是获得服务许可服务；三是获得服务

复习题（二）略

复习题（三）

1.计算机漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访间或破坏系统。在病毒肆意的信息不安全时代，某公司为减少计算机系统漏洞，对公司计算机系统进行了如下措施，其中错误的是（A）

A.减少系统日志的系统开销

B.禁用或删除不需要的服务，降低服务运行权限

C.设置策略避免系统出现弱口令并对口令猜测进行防护

D.对系统连接进行限制，通过软件防火墙等技术实施对系统的端口连接进行控制

5.银行A、B分别用自己的信息系统为用户记录账户余额，第三方支付C负责银行A和B的交易管控与备份。若银行A的客户与银行B的客户发生纠纷，C作为唯一掌控交易信的第三方，与任何一方串通，都不能维护客户的合法权益。为解决类似问题，他们采用私有链技术构建仅有A、B、C三方维护的半公开网络。私有链的特别之处在于（B）

A.任何个体或者团体都可以发送交易

B.独享该区块链的写入权限

C.交易能够获得该区块链的有效确认

D.任何人都可以参与其共识过程

8.小王进行资产评估的过程中，根据资产的表现形式对资产进行了分类，可将资产分为数据、软件、硬件、服务、人员等类型。有一种类型的资产中含有源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册、各类纸质的文档等。请问这是哪种类型的资产（C）

A.软件B.硬件C.数据D.服务

13.在新的信息系统或增强已有（）的业务要求陈述中，应规定对安全控制措施的要求。信息安全的系统要求与实施安全的过程宜在信息系统项目的早期阶段被集成，在早期如设计引入控制措施的更高效和节省。如果购买产品，则宜递循一个正式的（）过程。通过（）访问的应用易受到许多网络威胁，如欺诈活动、合同争端和信息的泄露或修改。因此要进行详细的风险评估并进行适当的控制，包括验证和保护数据传输的加密方法等，保护在公共期网络上的应用服务以防治款诈行为、合同纠纷以及未经授权的（）。应保护涉及到应用服务交换的信息以防不完整的传输、路由错误、未经授权的改变、擅自披露、未经授权的（c）。

A.披露和修改：信息系统：测试和获取；公共网格；复制或重播

B.信息系统；测试和获取；披露和修改；公共网络；复制和重播

C.信息系统；测试和获取：公共网络：披露和修改；复制和重播

D.信息系统；公共网络：测试和获取；鼓露和修改；复制或重播

14.TCP/IP协议就是为实现异构网互连推出的协议规范，具有较好的开放性。Intermet是在TP/IP协议簇的基础上构建的。但由于TCP/IP协议族在设计初期过于关注其开放性和便利性，对安全性考虑较少，因此其中很多协议存在安全隐患。例如，攻击者可以利用TP便利性，对安全性考虑较少，因此其中很多协议存在安全隐患。例如，攻击者可以利用TP 协议的三次握手机制实施DoS攻击，也可以通过猜测TCP会话中的序号来伪造数据包，那么上述例子中的情况可能发生在（B）。

A.应用层B.传输层C.网络层D.链路层

18.近几年，无线通信技术迅猛发展，广泛应用于各个领域。而无线信道是一个开放性信道，它在赋予无线用户通信自由的同时也给无线通信网络带来一些不安全的因素。下列选项中，对无线通信技术的安全特点描述正确的是（c）

A.无线信道是一个开放性信道，任何具有适当无线设备的人均可通过搭线窃听而获得网络

通信内容

B.通过传输流分析，攻击者可以掌握精确的通信内容

C.对于无线局域网络和无线个人区域网络来说，它们的通信内容更容易被窃听

D.群通信方式可以防止网络外部人员获取网络内通信内容

19.由于IP协议提供无连接的服务，在传送过程中若发生差错就需要哪一个协议向源节点报告差错情况，以便源节点对此做出相应的处理（C）

A.TCP

B.UDP

C.ICMP

D.RARP

20.随着计算机网络技术的出现与发展，数据库所处的环境愈加复杂，数据库面临的各种安全威胁正与日俱增。对于数据库安全防护相关描述中，错误的是（A）

A.数据库安全防护是指保护数据库运行安全以防止不合法的使用造成的数据泄露、更改或破坏，方式只包括安全审计

B.安全审计主要是针对数据库运行期间产生的各种日志，通过多个不同维度进行综合分析，从而发现影响数据库运行安全的因素并采取相应的应对措施

C.通过安全检测尽早发现数据库存在的安全缺陷（包括软件漏洞及配置缺陷），然而通过安装补丁、调整安全设置、制定安全策略等方法进行弥补

D.可根据数据库业务需要，构建完善的防护技术体系

22.某云平台要推出一项新的加密服务，包含快速加密与加密传输的功能，与此同时需要兼顾平台有限的密钥存储空间，可以采用以下哪类方案（A）。

A.使用对称密码算法对原始信息进行加解密，使用公钥算法实现通信

B.使用公钥密码算法对原始信息进行加解密，使用公钥算法实现通信

C.使用对称密码算法对原始信息进行加解密，使用私钥算法实现通信

D.使用公钥密码算法对原始信息进行加解密，使用私钥算法实现通信

32.小张在自主学习小楼输协议后，如道，此切协议在设计时仅仅考虑了实现相应功能，缺乏安全相关的机制，因此导致了大量的安全问题，他咨询了一个楼层的软件开发人员，该软件开发人员向他列举了一些会导致的安全问题，其中错误的是（D）

A.明文传输数据B.弱验证C，缺乏状态跟踪D.广播风暴

36.入侵检测系统（Intrusion Detection System，IDS）是用于发现并报告系统中未授权或违反安全策略行为的设备，在入侵检测中有这样的一种方法，任何的正常行为都是有一定的规律的并且可以通过分析这些行为产生的日志信息（假定日志信息足够安全）总结出这些规律，而入侵和滥用行为则通常和正常的行为存在严重的差异，通过检查这些差异就可以检测这些入侵，请问该入侵检测方法为（A）。

A.基于异常的入侵检测B、基于误用的入侵检测C.基于自治代理技术D.自适应模型生成特性的入侵检测

37、恶意代码的防范在计算机网络飞速发展的今天给计算机安全性带来了新的挑战。在Internet 安全事件中恶意代码造成的损失所占比重更大。某公司为进行恶意代码防范，通过网上查询到恶意代码预防的三个方面的措施，张主管发现下列选项中有一项不属于上述的三个方面，请问是哪一项（C）

A、安全策略B、安装最新的安全补丁C、减轻威胁D、减少漏洞

39、一般地，IP分配会首先把整个网络根据地域、区域。每个子域从它的上一级区域里获取IP地址段，这种分配方法为什么分配方法（A）

A、自顶向下B、自下向上C、自左向右D、自右向左

42、划分网络安全数是指整用不同区城的不同功能目的和安全要求，将网络划分为不同的安全域，以便实施不同的安全策略，所以某大型企业需要进行网络安全域划分，为更好地进行网络的安全防护，应根据用户实际网络的具体情况来划分，以下哪一条是正确的网络安全域划分原则（C）

A.网络的拓扑结构不需要进行严格的规划、设计和管理，一经确定，不能轻易更改，如因业务需求，确实需对网络的整体拓扑结构进行调整和改变，需按照相应的运维管理流程上报

B.不需要按照网络分层设计的原则进行规划，层次划分和设计合理清晰

C.网络按访问控制策略划分成不同的安全域，将有相同安全需求的网络设备划分到一个安全域，采取相同或类似的安全策略，对重要网段进行重点保护

D.不用使用防火墙等安全设备、VLAN或其他访问控制方式与技术，将重要网段与其他网段隔离开，在不同安全域之间设置访问控制措施

52.将防火墙软件安装在路由器上就构成了简单的什么防火墙（C）

A.子网过滤B.包过滤C.代理服务器D.主机过滤

54.由于应用系统的复杂性和多样性。对于系统的安全问题，目前还没有统一的分类，某公司工程师从对应用系统的功击手段角度出发，归纳出常见的应用系统主要成胁，其中不符合出发点的是（D）

A.缓冲区溢出B.钓鱼攻击C.远程渗透D.隔离防护

55.以下哪个系统不属于关键信息基础设施？（D）

A.港口管理运营系统B.疾病控制系统C.电视播出管控系统D.教学管理系统

58.某汽车保险公司有庞大的信贷数据，基于这些可信的不可靠改的数据，公司希望利用区块链的技术，根据预先定义好的规则和条款，自动控制保险的理赔。这一功能主要利用了区块链的（D）技术特点。

A.分布式账本B.非对称加密和授权技术C.共识机制D.智能合约

59.攻击者可以使用ping、或某一个系统命令获得目标网络的信息。攻击者利用此命令能收集到目标之间经过的路由设备IP地址，选择其中存在安全防护相对薄弱的路由设备实施攻击或者控制路由设备对目标网络实施修探等其他攻击，这个命令为（D）

A.ipconfig B.ipconfig all C.show D.tracert

60.小张在微博上发布了对小李的不实言论，请问小张不可能面临以下哪一项民事违法处罚？（D）

A.删除不实言论B.赔偿损失C.赔礼道歉D.治安拘留

62.《网络安全法》于以下哪个日期正式实施？（D）

A.2014年2月27日 B.2015年6月26日

C.2016年11月7日 D.2017年6月1日

63.软件测试的目的是（B）。

A.证明软件的正确性

B.尽可能多地发现软件系统中的错误

C.找出软件系统存在的所有错误

D.证明软件系统中存在错误

64.S0L注入攻击是黑客对数据库进行攻击的常用手段之一。随着B/S模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多，但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。小李在对某asp网站进行测试时，采用经典的1=1，1=2测试法，测试发现1=1时网页显示正常，1=2时报错，于是小李得出了四条猜测，则下列说法错误的是（D）

A.该网站可能存在漏洞

B.攻击者可以根据报错信息获得的信息，从而进一步实施攻击

C.如果再往站前部署一台HSC的IPS设备，那么1=1，1=2测试时，URL请求将会被IPS设备阻断，攻击者得不到任何有效信息

D.该网站不可以进行SQL注入攻击

70、失效的验证和会话管理指b应用程序中与身份认证和会话管理相关的代码功能往往没有正确实现，导致政击者破坏口令、密钥、会话令牌或攻击其他的漏洞去冒充其他用户的身份，下列防范措施错误的是（B）

A、区分公共区域和受限区域

B、在网络上以纯文本形式发送密码、

C、对最终用户账户使用账户锁定策略

D、支持密码有效期

81、某公司软件开发实习生小李在开发过程中多次使用Session，他知道Session是用于解决http无协议缺乏状态和和跟踪的方式，但是也带来了相应的安全问题。对于已验证过的用户，攻击者如果能获取用户的有效会话session ID（服务器没有释放这个Session过的用户，攻击者如果能获取用户的有效会话session ID（服务器没有释放这个Session ID），无需用户名和密码，就能以此用户的身份去操纵Web应用。但他忘记这种攻击方式的名字，那么你知道吗（C）

A.数据嗅探B.重放攻击C.Session欺骗D.数据篡改

96.某公司为加强员工的信息安全意识，对公司员工进行相关的培训，在介绍相关第三方人员通过社会工程学入侵公司信息系统时，提到了以下几点要求，其中在日常工作中错误的是（D）

A.不轻易泄露敏感信息

B.在相信任何人之前先校验其真实的身份

C.不违背公司的安全策略

D.积极配合来自电话、有点的任何业务要求，即使是马上提供本人的口令信息

98.漏洞扫描是信息系统风险评估中的常用技术措施，定期的漏洞扫描有助于组织机构发现系统中存在的安全漏洞。漏洞扫描软件是实施漏洞扫描的工具，用于测试网络、操作系统、数据库及应用软件是否存在漏洞。某公司安全管理组成员小李对漏洞扫描技术和工具进行学习后有如下理解，其中错误的是（A）

A.主动扫描工作方式类似IDS（Instrusion Detection Systems）

B.CVE（Coummon Vulnerabilities&Exposures）为每个漏洞确定了唯一的名称和标准化的描述

C.X.Scanner采用多线程方式对指定IP地址进行安全漏洞扫描

D.ISS的Systerm Scanner通过依附于主机上的扫描器代理侦测主机内部漏洞

[解析]扫描分为被动和主动两种。被动扫描对网络上流量进行分析，不产生额外的流量，不会导致系统的崩溃，其工作方式类似于IDS。主动扫描则更多地带有入侵的意味，可能会影响网络系统的正常运行

102.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感胁，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 STKIDE中欺生兴的成助胁，以下威胁中哪个可以归入此类威胁？（D）

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

CISP复习题（四）

1.小李在检查公司对外服务网站的源代码时，发现程序在发生诸如没有找到资源、数据库连接错误、写临时文件错误等问题时，会将详细的错误原因在结果页面上显示出来。从安全角度考虑，小李决定修改代码将详细的错误原因都隐藏起来在页面上仅仅告知用户“抱歉，发生内部错误！”。请问，这种处理方法的主要目的是（D）。

A.避免缓冲区溢出

B.安全处理系统异常

C.安全使用临时文件

D.最小化反馈信息

3.你是单位安全主管，由于微软刚发布了数个系统漏洞补丁，安全运维人员给出了针对此纸漏修补的四个建议方案，请选择其中一个最优方案执行（C）。

A、由于本次发布的数个漏洞都属于高危漏洞，为了避免安全风险，应对单位所有的服务器和客户端尽快安装补丁

B、本次发布的漏洞目前尚未出现利用工作，因此不会对系统产生实质性危害，所以可以先不做处理

C、对于重要的服务，应在测试环境中安装并确认补丁兼容性问题后再在正式生产环境中部署

D、对于服务器等重要设备，立即使用系统更新功能安装这批补丁，用户终端计算机由于没有重要数据，由终端自行升级

5、在某信息系统的设计中，用户登录过程是这样的，（1）用户通过即TP协议访问信息系统；（2）用户在登录系统页面输入用户名和口令；（3）信息系统在服务器端检查用户名和密码的正确性，如果正确，则鉴别完成。可以看出，这个鉴别过程属于（A）

A.单项鉴别

B.双向鉴别

C.三向鉴别

D.第三方鉴别

6.关于ARP欺骗原理和防范措施，下面理解错误的是（D）

A、ARP欺骗是指攻击者直接向受害者主机发送错误的ARP应答报文，使得受害者主机将错误的硬件地址映射关系存入到ARP缓存中，从而起到冒充主机的目的

B、单纯利用ARP欺骗攻击时，ARP欺骗通常影响的是内部子网，不能跨越路由实施攻击

C、解决ARP欺骗的一个有效方法是采用“静态”的ARP缓存，如果发生硬件地址的更改，则需要人工更新缓存

D、彻底解决ARP欺骗的方法是避免使用ARP协议和ARP缓存，直接采用IP地址和其他主机进行连接

11.由于Internet的安全问题日益突出，基于TCP/IP协议，相关组织和专家在协议的不同层次设计了相应的安全通信协议，用来保障网络各层次的安全，其中，属于或依附于传输层的安全协议是（C）

A.PPTP

B.L2TP

C.SSL

D.IPSec

13.一个密码系统至少由明文、密文、加密算法、解密算法和密钥5部分组成，而其安全性是由下列哪个选项决定的（D）。

A、加密算

B、解密算法

C、加密和解密算法

D、密钥

14.某集团公司根据业务需要，在各地分支机构部署前置机，为了保证安全，集团总部要求前置机开放日志共享，由总部服务器采集进行集中分析，在运行过程中发现攻击者也可通过共享从前置机中提取日志，从而导致部分敏感信息泄露，根据率低攻击面的原则，应采取以下哪项处理措施？（D）

A、由于共享导致了安全问题，应直接关闭日志井享，禁止总部提取日志进行分析

B、为配合总部的安全策略，会带来一定的安全问题，但不影响系统使用，因此接受此风险

C、日志的存在就是安全风险，最好的办法就是取消日志，通过设置让前置机不记录曰志

D、只允许特定的IP地址从前置机提取日志，对日志共享设置访问密码且限定访问的时间

16.金女士经常通过计算机网络购物，从安全角度看。下面需项是不好的操作习惯？（A）

A、使用专用上网购物用计算机。安教好软件后不要对该计算机上的系统教件应用获件进行升级

B、为计算机安装具有良好声断的安全防范软件，包括病毒查杀、安全检查和安全加围方面的软件

C、在IE的配置中，设置只能下载和安装经过签名的、安全的Activex控件

D、在使用网络浏览器时，设置不在计算机中保留网络历史记录和表单数据

23、以下哪项制度或标准被作为我国的一项基础制度加以推行，并且有一定强制性，其实施的主要目标是有效的提高我国信息和信息系统安全建设的整体水平，重点保障基础信息网络和重要信息系统的安全（B）

A.信息安全管理体系（ISMS）

B.信息安全等级保护

C.NIST SP800

D.ISO 270000系列

27.某网络安全公司基于网络的实时入侵检测技术，动态探测来自于外部网络和内部网络的所有访问行为。当检测到来自内外网络针对或通过防火墙的攻击行为。会及时响应，并通过防火墙实时阻断攻击源，从而进一步提高了系统的抗攻击能力，更有效地保护了网络资源提高了防翻体系，但入侵检测技术不能实现以下哪种功能（C）

A、检测并分析用户和系统的活动

B、核查系统的配置漏洞，评估系统关键和数据文件的完整性

C、防止IP地址欺骗

D、识别违反安全策略的用户活动

28.TCP/IP协议是Internet最基本的协议，也是Internet构成的基础，TCP/IP通常被认为是一个N层协议，每一层都使用它的下一层所提供的网络服务来完成自己的功能，这里N应等于（A）。

A.4B.5C.6D.7

29、目前，信息系统面临外部攻击者的恶意攻击威胁，从威胁能力和掌握资源分，这些威胁可以按照个人威胁、组织威胁和国家威胁三个层面划分，则下面选项中属于组织威胁的是（B）

A.喜欢恶作剧，实现自我挑战的娱乐型黑客

30.私有IP地址是一段保留的IP地址。只使用在局域网中，无法在Internet上使用。关于私有地址，下面描述正确的是（c）

A.A类和B类地址中没有私有地址，C类地址中可以设置私有地址

B.A类地址中没有私有地址，B类和类地址中可以设置私有地址

C.A类、B类和C类地址中都可以设置私有地址

D.A类、B类和C类地址中都没有私有地址

37.一个信息管理系统通常会对用户进行分组并实施访问控制。例如，在一个学校的教务系统中，教师能够录入学生的考试成绩学生只能查看自己的分数，而学校教务部门的管理人员能够对课程信息、学生的选课信息等内容进行修改。下列选项中，对访问控制的作用的理解错误的是（A）。

A.对经过身份鉴别后的合法用户提供所有服务

B.拒绝非法用户的非授权访问请求

C.在用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理

D.防止对信息的非授权篡改和滥用

38.以下关于灾难恢复和数据备份的理解，说法正确的是（C）

A、增量备份是备份从上次完全备份后更新的全部数据文件

B、依据具备的灾难恢复资源程度的不同，灾难恢复能力分为7个等级

C、数据备份按数据类型划分可以划分为系统数据备份和用户数据备份

D、如果系统在一段时间内没有出现问题，就可以不用再进行容灾演练了

42.数据库的安全很复杂，往往需要考虑多种安全策略，才可以更好地保护数据库的安全，以下关于数指床常用的安全策赔理解不正确的是（B）

A、最小特权原则，是让用户可以合法的存取或修改数据库的前提下，分配最小的特权使得这些信息恰好能够完成用户的工作

B、最大共享策略，在保证数据库的完整性。保密性和可用性的前提下，最大程度地共享数据库中的信息

C、粒度最小策略，将数据库中的数据项进行划分，粒度越小，安全级别越高，在实际中需要选择最小粒度

D、按内容存取控制策略，不同权限的用户访问数据库的不同部分

46、分布式拒绝服务（Distributed Donial of Service，DDoS）攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDos攻击，从而成倍地提高拒绝服务攻击的成力，一般来说，DDoS攻击的主要目的是破坏目标系统的（C）

A.保密性

B.完整性

C.可用性

D.真实性

47、关于信息安全管理体系的作用，下面理解错误的是（B）

A.对内而言，有助于建立起文档化的信息安全管理规范，实现有“法”可依，有章可循，有据可查

B.对内而言，是一个光花钱不挣钱的事情，需要组织通过其他方面收入来弥补投入

C.对外而言，有助于使各利益相关方对组织充满信心

D.对外而言，能起到规范外包工作流程和要求，帮助界定双方各自信息安全责任

52.老王是一名企业信息化负责人，由于企业员工在浏览网页时总导致病毒感染系统，为了解决这一问题，老王要求信息安全员给出解决措施，信息安全员给出了四条措施建议，老王根据多年的信息安全管理经验，认为其中一条不太适合推广，你认为是哪条措施（c）。

A、采购防病毒网关并部署在企业互联网出口中，实现对所以浏览网页进行检测，阻止网页中的病毒进入内网

B、采购并统一部署企业防病毒软件，信息化管理部门统一进行病毒库升级，确保每台计算机都具备有效的病毒检测和查杀能力

C、制定制度禁止使用微软的IE浏览器上网，统一要求使用Chrome 浏览器

D、组织对员工进行一次上网行为安全培训，提高企业员工在互联网浏览时的安全意识

53./etc/passwd 文件是UNIX/Linux安全的关键文件之一。该文件用于用户登录时校验用户的登录名、加密的口令数据项、用户ID（UID）、默认的用户分组ID（GID）、用户信息、用户登录目录以及登录后使用的shel1程序。某黑客设法窃取了银行账户管理系统的pasvd文件后，发现每个用户的加密的口令数据都显示为’x’。下列选项中，对此现象的

的解释正确的是（C）

A、黑客窃取的passwd文件是假的

B、用户的登录口令经过不可逆的加密算法加密结果为'x'

C、加密口令被转移带了另一个文件里

D、这些账户都被禁用了

54.随机进程名称是恶意代码迷惑管理员和系统安全检查人员的技术手段之一，以下对于随机进程名技术，描述正确的是（D）。

A、随机进程名技术虽然每次进程名都是随机的，但是只要找到了进和名称，就找到了恶意代码程序本身

B、恶意代码生成随机进程名称的目的是使进程名称不固定，因为杀毒软件是按照进程名称进行病毒进行查杀

C、恶意代码使用随机进程名是通过生成特定格式的进程名称，使进程管理器中看不到恶意代码的进程

D、随机进程名技术每次启动时随机生成恶意代码进程名称，通过不固定的进程名称使自己不容易被发现真实的恶意代码程序名称

58.由于频繁出现软件运行时被黑客远程攻击获取数据的现象，某软件公司准备加强软件安全开发管理，在下面做法中，对于解决问题没有直接帮助的是（A）

A、要求开发人员采用敏捷开发模型进行开发

B、要求所有的开发人员参加软件安全意识培训

C、要求规范软件编码，并制定公司的安全编码准则

D、要求增加软件安全测试环节，尽早发现软件安全问题

60.关于计算机取证描述不正确的是（C）

A.计算机取证是使用先进的技术和工具，按照标准规程全面地检查十算机系统，以提取和保护有关计算机犯罪的相关证据的活动

B.取证的目的包括：通过证据查找肇事者.通过证据推断犯罪过程.通过证据判断受害者损失程度及收集证据提供法律支持

C.电子证据是计算机系统运行过程中产生的各种信息记录及存储的电子化资料及物品。对于电子证据，取证工作主要围绕两方面进行：证据的获取和证据的保护

D.计算机取证的过程可以分为准备。保护.提取.分析和提交5个步骤

62.某社交网站的用户点击了该网站上的一个广告。该广告含有一个跨站脚本，会将他的测览器定向到旅游网站，旅游网站则获得了他的社交网络信息。虽然该用户没有主动访问该旅游网站，但旅游网站已经截获了他的社交网络信息（还有他的好友们的信息），于是犯罪分子便可以躲藏在社交网站的广告后面，截获用户的个人信息了，这种向Web页面插入恶意html代码的攻击方式称为（B）

A.分布式拒绝服务攻击B.跨站脚本攻击C.SQL注入攻击D.缓冲区溢出攻击

63.从Linux内核2.1版开始，实现了基于权能的特权管理机制，实现了超级用户的特极分部制，打破了UNIX/LINUX操作系统中超级用户/普通用户的概念，提高了操作系统的安全性。下列选项中，对特权管理机制的理解错误的是（B）

.普通用户及其s由el1没有任何权能，而超级用户及其shel1在系统启动之初拥有全部权能

B.系统管理员可以剥夺和恢复超级用户的某些权能

C.进程可以放弃自己的某些权能

D.当普通用户的某些操作设计特权操作时，仍然通过setuid实现

65.部署互联网协议安全虚拟专用网（Internet Protocol Security Virtual Private65.部署互联网协议安全虚拟专用网（Internet Protocol Security Virtual PrivateNetwork，IPsec VN）时，以下说法正确的是（C）

A、配置MD5安全算法可以提供可靠地数据加密

B、配置AES算法可以提供可靠的数据完整性验证

C、部署IPsecVPN网络时，需要考虑IP地址的规划，尽量在分支节点使用可以聚合的IP地址段，来减少IPsec 安全关联（Security Authentication，SA）资源的消耗

D、报文验证头协议（Authentication Header，AH）可以提供数据机密性

66.数据在进行传输前，需要由协议栈自上而下对数据进行封装，TCP/IP协议中，数据封装的顺序是（B）

A、传输层、网络接口层、互联网络层

B、传输层、互联网络层、网络接口层

C、互联网络层、传输层、网络接口层

D、互联网络层、网络接口层、传输层

68.Winors系统中，安全标识符（SID）是标识用户、组和计算机账户的唯一编码，在操作系统内部使用。当授权用户、组、服务或者其他安全主体对象的权眼时，操作系统会把SID和权限写入对象的ALC中。小刘在学习了SID的组成后，为了巩固所学知识，在自己计算机的Windows 操作系统中使用whoami/users 操作查看当前用户的SID。得到的SID为S-1-5-21-1534169462-1651380828-111620651-500。下列选项中，关于此STD的理解错误

的是（D）

A、前三位S-1-5表示此SID是由Windows NT颁发的

B、第一个子颁发机构是21

C、Windows NT的SID的三个子颁发机构是1534169462、1651380828、111620651

D、此SID以500结尾，表示内置guest账户

69.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？（D）

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

70.某信息安全公司的团队对某款名为“红包快抢”的外挂进行分析发现此外挂是一个典型的木马后门，使黑客能够获得受害者电脑的访问权，该后门程序为了达到长期驻留在受害者的计算机中，通过修改注册表启动项来达到后门程序随受害者计算机系统启动而启动为防范此类木马的攻击，以下做法无用的是（C）

A.不下载、不执行、不接收来历不明的软件和文件

B.不随意打开来历不明的邮件，不浏览不健康不正规的网站

C.使用共享文件夹

D.安装反病毒软件和防火墙，安装专门的木马防范软件

74.超文本传输协议（HyperText Transfer Protoco1，HTTP）是互联网上广泛使用的一种网协议，下面哪种协议基于HTTP并结合SSL协议，具备用户鉴别和通信数据加密等功能（C协议，下面哪种协议基于HTTP并结合SSL协议，具备用户鉴别和通信数据加密等功能（C）

A.HTTP1.0协议B.HTTP1.1协议C.HTTPS协议D.HTTPO协议

81.来现易公司的0A系统由于存在系统部词，被功击者上传了木马病毒并删除了系统中的数据，由于系统备份是每周六进行一次事件发生时间为周三因此导致该公司三个工作目的数据丢失并使得0A系统在随后两天内无法访问。影响到了与公司有业务往来部分公司业务。在事故处理报告中，根据6B/Z20986-207《信息安全事件分级分类指南》，该时间段准确分类和定级应该是（C）。

A、有害程序事件特别重大事件（I级）

B、信息破坏事件重大事件（Ⅱ级）

C、有害程序事件较大事件（Ⅲ级）

D、信息破坏事件一般事件（IV级）

86.关于密钥管理，下列说法错误的是（B）

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-Hellman 协议协商出会话秘钥

87.某单位在一次信息安全风险管理活动中，风险评估报告提出服务器A的FTP服务存在高风险漏洞。随后该单位在风险处理时选择了关闭FTP服务的处理措施。请问该措施属于哪种风险处理方式（B）

A、风险降低

B、风险规避

C、风险转移

D、风险接受

88.防火墙是网络信息系统建设中常常采用的一类产品，他在内外网隔离方面的作用是（C）

A.既能物理隔离，又能逻辑隔离

B.能物理隔离，不能逻辑隔离

C.不能物理隔离，能逻辑隔离

D.不能物理隔离也不能逻辑隔离

92Linux系统的安全设量主要从磁盘上分区、账户安全设置、禁用危险服务，远程登录安全、用户级别安全、审计策感、保护root账户、使用网结防火墙和文件权限操作共10个方面来完成。小张在学习了Linux系统安全的相关知识后，尝试为自己计算机上的Linux方面来完成。小张在学习了Linux系统安全的相关知识后，尝试为自己计算机上的Linux系统进行安全配置。下列选项是他的部分操作。其中不合理的是（A）

A、编辑文件/etc/passxd.，检查文件中用户1D，禁用所有1D=0的用户

B、编辑文件/etcf/ssh/shd config.将PermitRootLogin 设置为no

C、编辑文件/etc/pan.d/systerauth，设置authrequire pan tally，so onerr-fail

D、编辑文件/etc/profile，设置TMOUT-600

93.由于密码技术都依赖于密码，因此密钥的安全管理是密码技术应用中非常重要的环节，下列关于密钥管理说法，错误的是（B）。

A、科克霍夫在《军事密码学》中指出系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥

B、在保密通信过程中，通信双方可以一直使用之前用过的会话密钥，不影响安全性

C、密钥管理需要在安全策略的指导下处理密钥生命周期的整个过程，包括产生、存储、备份、分配、更新、撤销等

D、在保密通信过程中，通信双方也可利用Diffie-Hellman协议协商出会话密钥进行保密通信

94.操作系统用于管理计算机资源，控制整个系统运行，是计算机软件的基础。操作系统安全是计算、网络及信息系统安全的基础。一般操作系统都提供了相应的安全配置接口。小王新买了一台计算机，开机后首先对自带的Windows操作系统进行配置。他的主要操作有：1）关闭不必要的服务和端口；2）在“在本地安全策略”重配置账号策略、本地策略、公钥策略和IP安全策略；3）备份敏感文件，禁止建立空连接，下载最新补丁；4）关闭审核策略，开启口令策略，开启账号策略。这些操作中错误的是（D）

A.操作（1），应该关闭不必要的服务和所有端口

B.操作（2），在“本地安全策略”中不应该配置公钥策略，而应该配置私钥策略

C.操作（3），备份敏感文件会导致这些文件遭到窃取的几率增加

D.操作（4），应该开启审核策略

95.某单位门户网站开发完成后，测试人员使用模糊测试进行安全性测试，以下关于模糊测试过程的说法正确的是（D）

A.模拟正常用户输入行为，生成大量数据包作为测试用例

B.数据处理点.数据通道的入口点和可信边界点往往不是测试对象

C.监测和记录输入数据后程序正常运行的情况

D.深入分析网站测试过程中产生崩溃或异常的原因，必要时需要测试人员手工重现并分析

96.Apache HP Server（简称Apache）是一个开放源码的Web服务运行平台，在使用过程中，该软件默认会将自己的软件名和版本号发送给客户端。从安全角度出发，为隐藏这些信息，应当采取以下哪种措施（B）

A.不选择Windows平台，应选择在Linux平台下安装使用

B.安装后，修改配置文件httpd.conf中的有关参数

C.安装后，删除Apache HTTP Server码

D.从正确的官方网站下载Apeche HTTP Server，并安装使用

98.王工是某某单位的系统管理员，他在某次参加了单位组织的风险管理工作时，发现当前案例中共有两个重要资产：资产Al和资产A2；其中资产A1面临两个主要威胁，威胁T1和威胁T2；而资产A2面临一个主要威胁，威胁T3；威胁T1可以利用的资产A1存在的两个脆弱性；脆弱性V1和脆弱性V2；威胁T2可以利用的资产A1存在的三个脆弱性，脆弱性V3、脆弱性V4和脆弱性V5；威胁T3可以利用的资产A2存在的两个脆弱性；脆弱性V6和脆弱性V7。根据上述条件，请问：使用相乘去时，应该为资产A1计算几个风险值（c）

A、2

B、3

C、5

D、6

101.随着即时通讯软件的普及使用，即时通讯软件也被恶意代码利用进行传播，以下哪项功能不是恶意代码利用即时通讯进行传播的方式（D）

A.利用即时通讯软件的文件传送功能发送带恶意代码的可执行文件

B.利用即时通讯软件发送指向恶意网页的URL

C.利用即时通讯软件发送指向恶意地址的二维码

D.利用即时通讯发送携带恶意代码的TXT文档

102.数字签名不能实现的安全特征为（D）

A.防抵赖B.防伪造C.防冒充D.保密通信

104.以下关于数字签名说法正确的是（D）。

A.数字签名是在所传输的数据后附加上一段和传输数据毫无关联的数字信息

B.数字签名能够解决数据的加密传输，即安全传输问题

C.数字签名一般采用对称加密机制

D.数字签名能够解决篡改、伪造等安全性问题

106.关于《网络安全法》域外适用效力的理解，以下哪项是错误的（A）

A.当前对于境外的网络攻击，我国只能通过向来源国家采取抗议

B.对于来自境外的网络安全威胁我国可以组织技术力量进行监测、防御和处置

C.对于来自境外的违法信息我国可以加以阻断传播

D.对于来自境外的网络攻击我国可以追究其法律责任