河北省第二届网络安全知识竞赛 [退出]

一、单选题

每题 1 分，共 60 题，总分 60 分

1、灾难恢复是指将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到（D）而设计的活动和流程。

A.理想状态

B.稳定状态

C.正常状态

D.可接受状态

2、灾难恢复规划是一个周而复始、持续改进的过程，最后个阶段是（D）。

A.灾难恢复需求的确定

B.灾难恢复策略的制定

C.灾难恢复策略的实现

D.灾难恢复预案的制定、落实和管理

3、（D）是网络安全防护的重中之重，要在网络安全等级保护制度的基础上，实行重点保护。

A.政府网站

B.个人信息

C.办公系统

D.关键信息基础设施

4、《儿童个人信息网络保护规定》已经国家互联网信息办公室室务会议审议通过，将于（D ）开始实施。

A.2019/6/1

B.2012/6/1

C.2018/10/1

D.2019/10/1

5、业务连续性管理框架中，（B）是指了解组织的产品和服务，识别关键活动，搞清楚其供应链上的依赖关系。

A.BCM 管理程序

B.理解组织

C.演练、维护和评审

D.开发并实施 BCM 响应

6、（A）应该周期性地保存起来，以消除可能出现的信息丢失并让数据恢复过程更快完成。

A.备份记录

B.备份设备

C.恢复记录

D.恢复设备

7、根据《网络安全法》的规定，（B）负责统筹协调网络安全工作和相关监督管理工作。

A.公安部

B.国家网信部门

C.工信部

D.国家电信主管部门

8、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（B ）至少进行一次检测评估，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。

A.每两年

B.每年

C.每半年

D.每季度

9、关于检测与入侵检测，下面说法错误的是（A）

A.应急响应而言，检测和我们常说的入侵检测是相同的

B.检测的目的首先是确认事件是否真的发生

C.在肯定有安全事件发生后判定问题所发生的领域，其当前造成的危害和影响范围有多大，以及其发展的速度与其进一步的威胁是什么

D.入侵检测最常见的定义是确定对系统的非授权访问和滥用是否发生

10、业务连续性管理框架中，理解组织是指了解组织的产品和服务，识别关键活动，搞清楚其供应链上的（B）。

A.对应规则

B.依赖关系

C.作用机理

D.上下游单位

11、发生网络安全事件时，运营单位应当采取的措施不包括（C）

A.立即启动网络安全事件应急预案

B.向上级部门和当地网信部门报告

C.向社会公众发布警示信息

D.采取必要措施消除安全隐患、防止危害扩大

12、各地各部门各单位要认真执行网络安全重大事项报告制度，在出台涉及网络安全的地方法规、部门规章、重大规划、重要政策文件、举办涉及网络安全的重要会议和活动，要及时向（D）报告。

A.党委办公厅

B.政府办公厅

C.上级部门

D.网信部门

13、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（C）

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

14、当发生安全事件时，初步动作和响应的步骤不包括（C）

A.激活和增强审计功能

B.迅速备份完整系统

C.按照组织的报告程序(应急响应策略)向安全负责人报告任何可疑的现象

D.记录所发生事件

15、暴力破解，是指通过穷举所有口令组合的方式来破解口令。对抗暴力破解的最佳方法是? C

A.设置复杂口令

B.设置多个密码

C.设置一个较长的口令以扩大口令的破解难度

D.经常换口令

16、密码体制被定义为（A）数据变换

A.一对

B.两对

C.三对

D.四对

17、首先需要将信息系统及其中的信息资产进行（C），才能在此基础上进行下一步的风险评估工作。

A.资产赋值

B.保密性赋值

C.资产分类

D.完整性赋值

18、网络安全预警的分级主要考虑两个要素：（A）与网络安全保护对象可能受到损害的程度

A.网络安全保护对象的重要程度

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

19、首次提出了非对称密码体制的假想的是（D）

A.《密码起源》

B.《密码简史》

C.《密码安全》

D.《密码学新方》

20、计算机安全的核心元素是（A）。

A.访问控制

B.隐私保护

C.资源清单

D.防御攻击

21、安全风险计算模型包含（A）、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

22、（D）通常是由被评估信息系统的拥有者的上级主管机关或业务主管机关发起的，旨在依据已经颁布的法规或标准进行的，具有强制意味的检查活动，是通过行政手段 加强信息安全的重要措施。

A.基线评估

B.自评估

C.详细评估

D.他评估

23、在互联网信息内容管理中，市场环境信息属于（C）

A.国家外部信息

B.国家内部信息

C.组织外部信息

D.组织内部信息

24、在互联网信息内容安全管理中，产业界动向和竞争态势等信息资源属于（C）

A.国家外部信息

B.国家内部信息

C.组织外部信息

D.组织内部信息

25、计算机病毒防治体系的核心技术机制包括，（B）以及事发检测和响应的网络版病毒查杀系统。

A.防火墙

B.事先预防的安全补丁管理平台

C.网络入侵检测

D.系统和数据备份

26、风险评估要素关系模型中，（A）依赖于资产去完成

A.业务战略

B.残余风险

C.脆弱性

D.风险

27、信息安全管理旨在实现信息的完整性、机密性和可用性。网络信息被非正当的修改或破坏，这是破坏了信息的（B）

A.机密性

B.完整性

C.可控性

D.可用性

28、（A）侧重于打击违法有害信息，对信息的合法有效性进行控制管理

A.信息安全管理

B.信息内容安全管理

C.人员管理

D.系统管理

29、网络出版物可以含有以下（B）内容

A.危害社会公德或者民族优秀文化传统的

B.宣传宗教信仰的

C.宣扬淫秽、色情、赌博、暴力或者教唆犯罪的

D.侵害民族风俗、习惯的

30、互联网信息内容安全管理的保护对象包括国家、公共和个人安全。侵犯知识产权的信息属于危害(C)

A.个人安全

B.公司安全

C.公共安全

D.国家安全

31、信息安全的属性有很多，最核心的是保持信息的(A)、完整性和可用性。

A.稳定性

B.保密性

C.新鲜性

D.兼容性

32、关于漏洞扫描技术，下面说法不正确的是（D）

A.漏洞扫描技术的重要性在于把极为繁琐的安全检测通过程序来自动完成

B.一般而言，漏洞扫描技术可以快速、深入地对网络或目标主机进行评估

C.漏洞扫描技术是对系统脆弱性的分析评估，能够检查、分析网络范围内的设备、网络服务、操作系统、数据库系统等的安全性

D.采用网络漏洞扫描技术，漏洞知识库一旦建立就不能再做改变

33、从根本上讲，信息安全问题由信息技术引发，解决信息安全问题要通过（A）

A.发展信息安全高科技

B.加大处罚力度

C.加强信息安全管理

D.增加网络安全监管员

34、随着大数据和云计算技术的发展，网络的匿名性将（C）。

A.不再凸显

B.彻底消失

C.更加凸显

D.没有变化

35、信息是（A）的结果

A.数据处理

B.事件处理

C.材料加工

D.计算机运算

36、信息安全的保护对象主要是计算机硬件，软件和(D)。

A.操作系统

B.开发语言

C.文件系统

D.数据

37、针对网上制售传播淫秽色情等有害信息的行为，网络平台提供者（B）承担责任。

A.不需要

B.需要

C.视情况而定

D.视执法者决定

38、利用网络传授制作计算机病毒属于（A）。

A.教唆犯罪

B.传授犯罪方法

C.侵犯著作权

D.危害国家安全罪

39、系统管理员的主要职责不包括（D）

A.负责系统的运行管理，实施系统安全运行细则

B.负责设置和管理用户权限，维护系统安全正常运行

C.对操作网络管理功能的其他人员进行安全监督

D.对进行系统操作的其他人员予以安全监督

40、应用开发管理员的主要职责不包括（D）

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

41、访问控制功能可能由（D）模块协作完成

A.一个

B.两个

C.三个

D.多个

42、计算机安全的主要目标不包括以下哪个选项 （B）

A.防止未经授权的用户获取资源

B.防止已经授权的用户获取资源

C.防止合法用户以未授权的方式访问

D.使合法用户经过授权后可以访问资源

43、阻止潜在的攻击进入用户的网络系统指的是 （B）。

A.过滤互联网请求

B.过滤流入的内容

C.过滤流出的内容

D.过滤不良信息

44、基于源的过滤技术通过内容的来源进行过滤， 以下属于基于源的过滤技术的有（A）

A.IP 包过滤

B.内容分级审查

C.关键字过滤

D.启发式内容过

45、通过各种线路传导出去，可以将计算机系统的电源线，机房内的电话线、地线等作为媒介的数据信息泄露方式称为（B）。

A.辐射泄漏

B.传导泄漏

C.电信号泄漏

D.媒介泄漏

46、380V 电力电缆，容量大于 5kVA，与信号线缆平行敷设，最小净距为（D）/mm

A.150

B.200

C.300

D.600

47、数字水印可以用来实现所有权保护、版权证明和数据可靠性保护、数字拷贝追踪以及访问控制等。数字水印的特征没有？C

A.不需要带外传输

B.透明性

C.稳定性

D.安全性

48、阻止用户浏览不适当的内容或站点指的是（A）。

A.过滤互联网请求

B.过滤流入的内容

C.过滤流出的内容

D.过滤不良信息

49、380V 电力电缆，容量 2~5kVA，与信号线缆平行敷设，最小净距为（C）/mm

A.150

B.70

C.300

D.80

50、入侵防御系统是一种智能化的网络安全产品，不但能检测入侵行为的发生，而且能通过一定的响应方式，实时中止入侵行为的发生和发 展，实时保护信息系统不受实质性的攻击。入侵防御系统使得入侵检测系统和防火墙走向了统一。下列不属于入侵防御系统种类的是（D）

A.基于主机的入侵防御系统

B.基于应用的入侵防御系统

C.基于网络的入侵防御系统

D.基于协议的入侵防御系统

51、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 提供的核心服务不包括了哪些信息安全的要求（A）

A.访问安全性

B.真实性

C.完整性

D.保密性

52、数字版权保护系统中的密码技术没有？D

A.对称与非对称加密

B.数字签名和单向散列

C.数字证书

D.访问控制

53、入侵防御系统倾向于提供主动防御，其设计宗旨是预先对入侵活动和攻击性网络通信进行拦截，避免其造成损失，而不是在检测到网络入侵的同时或之后进行报警。基于网络的入侵防御系统所基于的硬件平台不包括（C）

A.专用的 FPGA 编程芯片

B.网络处理器

C.专用的单片机芯片

D.专用的 ASIC 芯片

54、随着计算机技术和互联网的迅速发展，来自网络的攻击每年呈几何级数增长。这些攻击中的大多数是利用计算机操作系统或其他软件系统的漏洞实施的。以下关于漏洞的说法错误的是（C）

A.漏洞的分类方法很多，也没有统一的标准

B.漏洞具有时间与空间特性

C.系统的环境变量发生变化时产生的漏洞为开放式

D.程序在实现逻辑中没有考虑一些意外情况为异常

55、（A）身份鉴别技术依赖于特殊的硬件设备来提取生物特征信息，且其准确性和稳定性与传统的认证技术相比相对较低，因此，并没有得到全面普及。通常用于安全级别较高的场所

A.基于生物特征

B.主流的身份鉴别

C.基于用户知识的身份鉴别技术