**第5部分**

理论知识考试模拟试卷及答案

信息安全管理员（四级）理论知识试卷

注 意 事 项

1．考试时间：90min。

2．请首先按要求在试卷的标封处填写您的姓名、准考证号和所在单位的名称。

3．请仔细阅读各种题目的回答要求，在规定的位置填写您的答案。

4．不要在试卷上乱写乱画，不要在标封区填写无关的内容。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 一 | 二 | 总 分 |
| 得 分 |  |  |  |

|  |  |
| --- | --- |
| 得 分 |  |
| 评分人 |  |

一、判断题（第1题～第50题。将判断结果填入括号中。正确的填“√”，错误的填“×”。每题0.5分，满分25分）。

1．职业道德修养是指从业人员在职业活动中自觉按照职业道德要求约束自己的言行，不断提高职业道德品质的过程。（ ）

2．社会主义道德包含社会公德、职业道德、家庭美德、个人品德四个方面，简称四德。（ ）

3．职业守则只适用于特定的行业或职业群体，不适用于其他行业和职业。（ ）

4．信息安全管理员的职业守则特点主要包括遵纪守法、爱岗敬业、勤奋进取、忠于职守、认真负责、团结协作、爱护设备以及安全操作等。（ ）

5．冯·诺依曼结构的计算机硬件系统主要由控制器、存储器、输入设备和输出设备四大部件组成。（ ）

6．硬盘是计算机的核心部件，主要负责运算和控制计算机的各种操作。（ ）

7．用人单位与劳动者订立的劳动合同中，只要没有违反法律、行政法规的强制性规定，该劳动合同就一定是有效的。（ ）

8．劳动合同中约定的工作时间必须符合国家规定的标准工时制度。（ ）

9．OSI参考模型的全称是开放系统互连参考模型，是由国际标准化组织ISO在20世纪80年代初提出来的，它不受限于某个具体公司。（ ）

10．OSI模型的网络层负责处理数据链路层的错误检测和纠正。（ ）

11．TCP/IP是一组用于实现网络互连的通信协议 。（ ）

12．网络接口层的主要功能是负责路由的转发。（ ）

13． IP地址是互联网上每个设备唯一标识的地址，用于在网络中进行数据包的定向传输。（ ）

14．IP地址根据网络号和主机号的分配方式，被分为A、B、C、D、E、F、G七类。（ ）

15．交换机工作在OSI模型的数据链路层，它根据MAC地址进行数据帧的转发。（ ）

16．为确保交换机的物理安全，应将交换机放置在公共区域，以便于管理和维护。（ ）

17．路由器工作在OSI模型的网络层，它根据IP地址来决定数据包的转发路径。（ ）

18．路由器上的防火墙功能可以完全防止外部攻击。（ ）

19．无线网络安全的主要目的是保护无线网络免受未经授权的访问和数据泄露。（ ）

20．WEP是最安全的无线加密方法。（ ）

21．在Windows系统中，默认情况下，所有用户都可以更改系统时间（ ）

22．在Linux系统中，root用户拥有最高权限，可以执行任何操作。（ ）

23．操作系统的安全机制主要依赖于用户输入的验证和应用程序的安全性。（ ）

24．操作系统中的身份认证原理包括基于生物特征的身份认证。（ ）

25．恶意代码是指故意编写的，用于对计算机系统或网络造成损害的程序代码。（ ）

26．恶意代码可能会窃取用户的个人信息或敏感数据。（ ）

27．HTTP协议是基于TCP/IP协议族的，采用无连接的传输方式。（ ）

28．GET是HTTP协议的常用方法之一。（ ）

29．IIS 的配置只能通过图形用户界面完成，无法通过命令行进行。（ ）

30．Apache Web服务器的配置只能通过编辑httpd.conf文件来完成。（ ）

31．为了提高IIS的安全性，应禁用所有不必要的Web服务扩展。（ ）

32．Apache和Nginx都可以通过配置文件来禁用不必要的HTTP方法，以减少攻击面。（ ）

33．VLAN是虚拟局域网的缩写，它允许将一个物理网络划分为多个虚拟网络，从而隔离广播域。（ ）

34．静态VLAN和动态VLAN是VLAN配置中的两种主要类型，其中静态VLAN更安全。（ ）

35．交换机和路由器默认都允许所有用户访问其管理接口，无需进行任何访问控制配置。（ ）

36．使用SSH协议而不是Telnet可以为远程管理提供加密的通信，增强安全性。（ ）

37．交换机、路由器通过实施多层次的用户角色和权限体系，以确保网络管理的安全性和有效性。（ ）

38．在Cisco设备中，通过设置命令级别访问可以限制用户执行特定命令，从而增强命令级别的安全性。（ ）

39．在操作系统中，用户账户和组账户是不同的概念。（ ）

40．在Linux系统中，用户和组的管理可以通过图形界面工具完成。（ ）

41．访问控制的三要素包括主体，客体，和访问权限。（ ）

42．基于角色的访问控制将用户分为不同的角色，每个角色具有特定的权限，用户可以根据其角色获得相应的访问权限。（ ）

43．补丁是指发布的软件更新，旨在修复安全漏洞，提高软件的稳定性和兼容性。（ ）

44．系统补丁可以分为安全补丁和功能补丁，其中安全补丁专门用于修复安全漏洞。（ ）

45．防病毒软件主要通过病毒特征码比对和危害结果来识别和清除病毒。（ ）

46．病毒特征码是由病毒编写者设定的，用于识别和清除病毒的程序代码。（ ）

47．域名是 IP地址的一种易于记忆的表示形式，主要用于在互联网上标识一个实体或组织的电子位置。（ ）

48．域名的基本结构包括顶级域名、二级域名和子域名，这种层次结构有助于清晰地组织和识别不同的网站。（ ）

49．域名备案的主要目的是为了管理和监控网站的运营。（ ）

50．只有企业法人可以进行域名备案。（ ）

|  |  |
| --- | --- |
| 得 分 |  |
| 评分人 |  |

二、单项选择（第1题～第150题。选择一个正确的答案，将相应的字母填入题内的括号中。每题0.5分，满分75分。）

1．（）属于职业道德的基本含义。

A．职业活动中应遵循的行为规范 B．职业活动中应遵循的约定俗成 C．职业活动中应遵循的法律规定 D．职业活动中应遵循的技术标准

2．职业道德的主要内容不仅包括对员工义务的要求，还包括对员工（）的要求。

A．权利 B．责任 C．薪酬 D．态度

3．职业守则对于个人而言，（）是其最重要的功能。

A．提高职业技能水平 B．实现个人价值 C．维护社会公共利益 D．促进社会和谐稳定

4．在职业守则的制定过程中，首要步骤是（）。

A．制定草案 B．调研分析 C．征求意见 D．正式发布

5．为了确保职业守则得到有效实施，措施（）是关键。

A．定期培训 B．绩效考核 C．员工激励 D．领导示范

6．职业技能的核心组成部分不包括（）。

A．专业知识 B．实践能力 C．心理素质 D．外貌形象

7．计算机软件主要分为两大类，其中一类直接面向用户，为用户提供各种特定功能和服务。这类软件被称为（）。

A．系统软件 B．应用软件 C．编程语言 D．数据库管理系统

8．按照软件的功能和用途，可以将计算机软件分为系统软件和应用软件两大类。（）属于系统软件。

A．文字处理软件 B．数据库管理系统 C．操作系统 D．多媒体播放软件

9．根据操作系统的设计和应用领域，将其分为不同类型，这种分类的依据是（）。

A．处理器架构 B．内存管理 C．操作系统分类 D．文件系统类型

10．在用户管理过程中，措施（）有助于提高安全性。

A．使用弱密码 B．共享账户 C．定期审查用户权限 D．禁用账户

11．权限管理的基本原则包括（）。

A．最小权限原则 B．最大权限原则 C．平均权限原则 D．随机权限原则

12．在信息服务管理中，流程（）负责确保服务正常运行并响应服务请求。

A．事件管理 B．问题管理 C．变更管理 D．发布管理

13．数据库是按照数据结构来组织、存储和管理数据的仓库，其中（）是数据库系统的核心和基础。

A．数据库管理系统 B．数据库模式 C．数据库视图 D．数据库索引

14．（）使用键值对Key-Value的形式存储数据。

A．关系型数据库 B．非关系型数据库 C．对象数据库 D．文档数据库

15．SQL语句中用于检索数据的常用命令是（）。

A．FROM B．SELECT C．GET D．QUERY

16．计算机网络是指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过（）连接起来，在网络操作系统，网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。

A．通信线路 B．电线 C．无线信号 D．光纤

17．（）协议不是TCP/IP协议簇的核心协议。

A．TCP B．IP C．UDP D．ZigBee

18．在构建局域网时，用于连接多台计算机并提供网络交换功能的设备是（）。

A．路由器 B．集线器 C．交换机 D．调制解调器

19．根据《劳动合同法》第三十八条，如果用人单位的规章制度违反法律、法规的规定并损害了劳动者权益，劳动者可以（）。

A．忍受并继续工作 B．要求用人单位修改规章制度 C．直接解除劳动合同 D．向法院提起诉讼但不能解除劳动合同

20．根据劳动法规定，用人单位在某些特定情况下不得随意行使解雇权，这些情况通常被称为（）。

A．解雇许可 B．解雇限制 C．解雇条件 D．解雇程序

21．劳动关系是指用人单位与劳动者之间基于劳动合同建立的社会关系。（）不是劳动关系的特征。

A．平等性 B．从属性 C．经济性 D．永久性

22．劳动合同的订立应当遵循（）、协商一致的原则。

A．平等自愿 B．互惠互利 C．以劳动者为主 D．用人单位为主

23．根据《中华人民共和国劳动法》的规定，劳动合同应当以书面形式订立，但（）的除外。

A．非全日制用工 B．固定期限用工 C．无固定期限用工 D．劳务派遣用工

24．根据《中华人民共和国工伤保险条例》的规定，职工因工作遭受事故伤害或者患职业病需要暂停工作接受工伤医疗的，在停工留薪期内，原工资福利待遇不变，由所在单位按月支付。停工留薪期一般不超过（）个月。

A．6 B．12 C．18 D．24

25．根据知识产权法的基本原则，以（）行为不属于侵权行为。

A．未经许可擅自使用他人的作品 B．在公共场合大声朗读他人的诗歌 C．未经允许将他人的发明申请专利 D．在社交媒体上分享他人的照片

26．（）不受著作权法的保护。

A．一部已经发表的小说 B．一幅未发表的个人画作 C．一个商业软件 D．一篇未发表的新闻报道

27．实用新型专利权的期限为（）。

A．10年 B．20年 C．30年 D．50年

28．为了保护知识产权，企业可以采取（）的措施。

A．申请专利保护 B．公开技术细节 C．签订保密协议 D．加强内部管理

29．网络安全法规定，网络运营者应当制定网络安全事件应急预案，并定期组织演练。这一规定的目的是确保（）的实现。

A．保护公民个人信息安全 B．打击网络犯罪活动 C．保障网络安全稳定运行 D．促进网络技术创新和应用

30．根据网络安全法的规定，国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行相应的（）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。

A．安全防护 B．安全管理 C．安全防护和安全管理 D．安全审计

31．网络运营者在发生网络安全事件时，应当按照规定及时告知用户并向有关主管部门报告。其中（）不属于网络运营者需要报告的主管部门。

A．公安机关 B．国家安全机关 C．工业和信息化部门 D．文化部门

32．（）不属于网络接入中的规范要求。

A．定期更新操作系统和软件 B．使用防火墙和安全软件 C．避免在公共网络接入个人设备 D．不在公共网络上进行敏感操作

33．小明正在用手机微信与他人聊天，请问微信app位于OSI模型的第（）层。

A．5 B．6 C．7 D．8

34．在网络层，（）负责为每个数据包分配唯一的IP地址。

A．IP协议 B．ICMP协议 C．ARP协议 D．RARP协议

35．在网络层，（）负责为每个数据包分配唯一的IP地址。

A．IP协议 B．ICMP协议 C．ARP协议 D．RARP协议

36．在传输层，（）负责提供可靠的、面向连接的数据传输服务。

A．TCP协议 B．UDP协议 C．HTTP协议 D．FTP协议

37．在子网划分中，子网掩码的作用是（）。

A．区分网络号和主机号 B．增加IP地址的数量 C．减少路由表的大小 D．提高网络传输速度

38．IP协议报文中的字段（）用于标识数据包的优先级。

A．版本 B．服务类型 C．总长度 D．标识

39．交换机的端口安全功能主要用于防止（）的安全威胁。

A．IP地址冲突 B．MAC地址泛洪攻击 C．VLAN跳跃攻击 D．ARP欺骗攻击

40．交换机以（）方式学习MAC地址。

A．通过ARP协议 B．通过ICMP协议 C．通过监听到的数据帧 D．通过手工配置

41．路由协议的主要作用是（）。

A．发现和维护网络中的路由信息 B．加密网络数据 C．分配IP地址 D．管理网络流量

42．静态路由与动态路由相比，（）的优点是静态路由所不具备的。

A．自动适应网络变化 B．减少带宽消耗 C．更少的配置工作 D．更高的安全性

43．WEP加密方法在（）被IEEE正式批准为802.11标准的一部分。

A．1997年 B．1999年 C．2001年 D．2003年

44．在无线网络中（）链路认证方式是开放系统认证和共享密钥认证的混合体。

A．EAP B．SAP C．WEP D．WPA

45．操作系统中（）命令不能用于查看当前运行的进程。

A．ps B．top C．tasklist D．process

46．在Linux系统中，shell （） 提供了自动补全功能和命令历史记录。

A．bash B．sh C．csh D．tcsh

47．在Linux系统中，用于列出目录内容的命令是（）。

A．ls B．cd C．pwd D．mkdir

48．在Windows系统中，（）程序用于管理文件和文件夹。

A．文件管理器 B．资源管理器 C．文件浏览器 D．文件查看器

49．在操作系统中，（）账户类型具有最高权限。

A．管理员账户 B．普通用户账户 C．来宾账户 D．系统账户

50．确保操作系统提供的服务安全性的过程，包括配置安全策略、监控和审计等，这一过程被称为（）。

A．系统加固 B．安全审计 C．服务安全管理 D．防御策略

51．操作系统通过设定特定规则来限制用户对文件和目录的访问，这种机制被称为（）。

A．权限分配 B．身份验证 C．文件访问控制 D．资源管理

52．操作系统内置的一种安全功能，用于监控和控制网络通信，防止未授权访问和数据泄露，这一功能通常被称为（）。

A．网络安全协议 B．系统安全性设置 C．自带防火墙管理 D．数据加密服务

53．病毒是一种（）的恶意代码。

A．自我复制 B．远程控制 C．窃取数据 D．破坏系统

54．计算机病毒是一种恶意软件，它能够在计算机系统中自我复制并将自身传播到其他计算机或系统中，通常具有（）的特征。

A．可预见性 B．破坏性 C．不可清除性 D．无关性

55．网络蠕虫攻击的目标通常是（）。

A．计算机 B．集线器 C．交换机 D．路由器

56．木马病毒通过伪装成合法软件诱导用户下载和执行，从而在用户不知情的情况下执行恶意操作，其核心攻击方式是（）。

A．缓冲区溢出 B．代码注入 C．拒绝服务 D．钓鱼攻击

57．HTTP状态码200表示（）。

A．请求已成功 B．服务器遇到错误，无法完成请求 C．请求的资源不存在 D．客户端必须采取进一步行动

58．HTTPS协议的主要功能是（）。

A．提高网页加载速度 B．对电子邮件进行加密 C．保护Web通信的机密性和完整性 D．防止恶意软件通过网络传播

59．FTP协议中，用于建立数据连接的默认端口号是（）。

A．20 B．21 C．22 D．23

60．在DNS查询过程中，（）负责最终返回所请求的记录。

A．根DNS服务器 B．顶级域TLD服务器 C．权威DNS服务器 D．本地DNS服务器

61．在配置FTP服务器时，（）不是必须配置的。

A．匿名访问设置 B．传输模式设置 C．防火墙规则 D．数据库连接信息

62．在Web服务中，SSL/TLS证书的主要作用是（）。

A．提高网站的加载速度 B．验证服务器的身份 C．压缩传输的数据 D．防止恶意软件感染

63．在配置证书服务时，（）不是必须的操作。

A．生成私钥和公钥对 B．向证书颁发机构申请证书 C．安装和配置证书颁发机构服务 D．编辑服务器的hosts文件

64．在配置MySQL数据库服务时，（）操作不是必须的。

A．设置root用户的密码 B．创建数据库和用户 C．配置数据存储路径 D．安装MySQL客户端工具

65．在配置FTP服务器时，为了提高稳定性，应该（）。

A．允许匿名访问 B．禁用SSL/TLS加密 C．限制用户的并发连接数 D．允许所有用户写入

66．在DNS服务器中，为了防止缓存污染攻击，应该（）。

A．禁用DNS缓存 B．启用DNSSEC C．关闭DNS服务器 D．禁用递归查询

67．在MySQL数据库中，（）可以提高安全性。

A．禁止远程服务 B．禁用SQL注入防护 C．定期备份数据库 D．关闭审计功能

68．在数据管理中，为确保数据安全，采取的一种重要措施是进行（）。

A．数据加密 B．数据压缩 C．数据备份与恢复 D．数据分析

69．在VLAN中，用于在帧头中标识VLAN信息的字段是（）。

A．VLAN源地址 B．VLAN标签 C．VLAN协议 D．VLAN标记

70．在VLAN间路由中，（）负责在不同VLAN之间转发数据包。

A．交换机 B．路由器 C．集线器 D．网桥

71．在网络中，用于远程管理交换机和路由器的常用协议是（）。

A．HTTP B．FTP C．SNMP D．DNS

72．在配置交换机或路由器时，（）有助于防止未经授权的访问。

A．使用默认的用户名和密码 B．定期更改密码 C．禁用所有接口 D．关闭SNMP服务

73．在交换机或路由器的配置视图中，（）的方法可以有效地限制特定用户对设备配置的访问。

A．通过设置不同的用户名和密码 B．通过设置设备访问时间段 C．通过启用认证、授权和计费AAA服务 D．通过物理隔离

74．（）为身份验证方法提供了最高级别的安全性。

A．密码认证 B．多因素认证 C．生物识别 D．MAC地址过滤

75．操作系统中的访问控制列表ACL的主要作用是（）。

A．限制网络流量 B．控制用户访问文件和目录 C．监视系统活动 D．加密数据传输

76．（）身份验证机制提供了比传统密码更高的安全性。

A．单一密码认证 B．双因素认证 C．生物识别技术 D．密码加密存储

77．在文件系统中，用于详细列出特定用户或用户组对文件或目录具有的访问权限的数据结构被称为（）。

A．身份认证服务器 B．加密密钥 C．访问控制列表 D．访问控制策略

78．在身份验证方法中，（）是通过用户所知道的信息如密码或PIN码来验证用户身份的。

A．知识因素 B．拥有因素 C．是因素 D．生物因素

79．在自动化补丁管理中，（）不是补丁管理工具的核心功能。

A．自动检测系统漏洞 B．自动下载和安装补丁 C．自动重启服务 D．自动审批流程

80．补丁管理流程的第一步是（）。

A．评估补丁 B．测试补丁 C．下载补丁 D．确定补丁需求

81．（）是常见的补丁管理工具。

A．Microsoft SCCM B．Adobe Photoshop C．Microsoft Word D．Mozilla Firefox

82．补丁的优先级通常是根据（）来确定的。

A．补丁的大小 B．补丁的复杂性 C．补丁影响的系统范围 D．补丁修复的安全漏洞的严重性

83．防病毒软件在进行文件扫描时（）。

A．仅依赖病毒特征码 B．主要依赖病毒特征码，但也结合其他技术 C．不依赖病毒特征码，而是依赖人工智能 D．完全不依赖病毒特征码

84．防病毒软件的启发式检测是基于（）的原理。

A．对病毒进行完全解密 B．检测文件是否与用户常用文件相似 C．分析程序的行为，寻找类似病毒行为模式 D．仅通过文件大小判断

85．沙盒技术通过创建一个隔离的环境来测试和验证软件，确保其在实际部署前不会对系统造成损害，这种技术的核心是（）。

A．隔离性 B．完整性 C．透明性 D．可控性

86．（）不是常见的系统恢复与备份方式。

A．全盘备份 B．增量备份 C．手动复制文件 D．在线同步备份

87．域名注册通常需要通过（）机构进行。

A．互联网服务提供商ISP B．域名注册商 C．网络管理员 D．操作系统供应商

88．DNS解析过程中，最后一步是（）。

A．缓存查询 B．本地Hosts文件查询 C．向根域名服务器发起查询请求 D．返回IP地址给客户端

89．域名到期前的（）天，系统会开始提醒用户续费。

A．30 B．15 C．7 D．3

90．域名隐私保护的主要目的是（）。

A．隐藏域名的注册信息，防止垃圾邮件 B．增加域名的SEO排名 C．保护网站免受黑客攻击 D．节省域名注册费用

91．在中国进行域名备案，（）是不必要的材料。

A．域名证书 B．网站负责人的身份证复印件 C．企业的税务登记证 D．网站的应急联系方式

92．域名备案的第一步通常是（）。

A．支付备案费用 B．准备备案材料 C．提交备案申请 D．等待审核结果

93．域名备案成功后，网站运营者需要定期更新备案信息，（）不是必须更新的内容。

A．联系人信息 B．联系电话 C．网站名称 D．服务器IP地址

94．如果一个备案的网站被发现传播违法信息，（）不是备案服务商通常会采取的措施。

A．立即关闭网站 B．通知网站负责人进行修改 C．向有关部门报告 D．对网站负责人罚款

95．数据备份的主要目的是为了在数据丢失或损坏时能够迅速恢复，其（）体现在多个方面，如业务连续性保障、法律责任遵从等。

A．安全性 B．可靠性 C．重要性 D．完整性

96．完全备份和增量备份的主要区别是（）。

A．完全备份备份所有数据，而增量备份仅备份自上次备份以来变化的数据 B．完全备份恢复速度快，而增量备份恢复速度慢 C．完全备份占用存储空间少，而增量备份占用存储空间多 D．完全备份安全性高，而增量备份安全性低

97．制定合理的数据备份策略对于确保数据安全至关重要，其中（）是一种常见的备份策略，可以最大限度地减少数据丢失的风险。

A．3-2-1备份规则 B．全量备份 C．增量备份 D．差异备份

98．在企业级数据备份策略中，常用于长期存储和离线备份的介质是（）。

A．硬盘 B．固态硬盘 C．磁带 D．网络附加存储

99．在选择数据备份的位置时，考虑地理冗余的原因是（）。

A．降低备份成本 B．减少数据传输延迟 C．以防自然灾害影响备份数据 D．提高数据访问速度

100．当发生数据丢失或损坏时，可以通过之前备份的数据进行（），以恢复至数据丢失前的状态。

A．数据恢复 B．数据复制 C．数据迁移 D．数据同步

101．（）不是计算机网络的主要功能。

A．资源共享 B．数据传输 C．通信 D．能源共享

102．当需要测试网络连接的质量，包括丢包率和往返时间等参数时，应该选择工具（）。

A．Ping B．Tracert C．Ipconfig D．Nslookup

103．使用（）可以追踪数据包从源到目的地经过的路由，并显示每个跳点的延迟。

A．ping B．traceroute C．nslookup D．route

104．网关的主要功能包括（）、路由选择和流量控制等。

A．协议转换 B．网络信号放大 C．网络攻击防御 D．病毒检测

105．ARP协议是一种用于（）的协议。

A．IP地址到MAC地址的转换 B．IP地址到端口号的转换 C．MAC地址到IP地址的转换 D．端口号到IP地址的转换

106．ARP请求报文是由需要发送数据的（）发出的。

A．主机 B．路由器 C．交换机 D．网关

107．（）不属于防范ARP欺骗攻击的方法。

A．MAC地址绑定 B．使用防火墙和入侵检测系统 C．配置静态ARP表 D．不实施网络分段

108．当网络中出现ARP欺骗时，用户可能会遇到（）的症状。

A．网络连接不稳定 B．电脑无法关机 C．电脑无法开机 D．硬盘空间不足

109．在进行网络诊断时，第一步骤是（）。

A．分析网络流量 B．检查网络连接 C．定位问题原因 D．修复网络故障

110．在使用ping命令进行网络诊断时，（）能够让你持续不断地向目标主机发送ICMP数据包，直到你手动停止。

A．ping目标主机 B．ping -c10目标主机 C．ping -t目标主机 D．ping -i2目标主机

111．在进行网络诊断时，常见网络诊断工具通常具有（）特点。

A．仅能检测硬件故障 B．仅能提供静态的网络状态信息 C．可以发送测试数据包并实时更新网络状态 D．需要用户手动分析每个数据包的详细内容

112．要查看本地计算机上所有TCP和UDP端口的详细信息，可以使用（）工具。

A．Ping命令 B．Tracert命令 C．Netstat命令 D．Ipconfig命令

113．在使用ping命令进行网络诊断时，（）选项能够让你持续不断地向目标主机发送ICMP数据包，直到你手动停止。

A．ping 目标主机 B．ping -c10目标主机 C．ping -t目标主机 D．ping -i2目标主机

114．在Windows系统的命令提示符中，使用arp命令来查看本地ARP缓存表时，应输入（）命令。

A．arp -a B．arp -d C．arp -s D．arp -n

115．在Windows系统的命令提示符中，使用tracert命令来跟踪数据包从源主机到目标主机之间的路由路径时，应输入（）命令。

A．tracert 目标主机 B．tracert -d 目标主机 C．tracert -h 10目标主机 D．tracert -p 80目标主机

116．在使用traceroute命令时，（）选项将使得命令只显示IP地址而不进行主机名解析。

A．traceroute -d 主机名 B．traceroute -n 主机名 C．traceroute -i 接口名主机名 D．traceroute -m 数值主机名

117．当遭受拒绝服务攻击时，网络系统的（）症状可能最显著。

A．系统显示正常，但运行速度变慢 B．用户收到大量垃圾邮件 C．网络连接异常，服务不稳定 D．应用程序界面显示异常

118．（）攻击属于拒绝服务攻击DoS的一种。

A．SQL注入攻击 B．分布式拒绝服务攻击DDoS C．跨站脚本攻击XSS D．钓鱼攻击

119．拒绝服务攻击的原理是通过向目标系统发送大量的无效或伪造的请求，使目标系统无法处理正常用户的请求，从而达到（）的目的。

A．消耗目标系统的网络带宽 B．破坏目标系统的硬件设备 C．窃取目标系统的敏感信息 D．硬盘空间减少

120．在应对拒绝服务攻击DoS时，防御手段通常可以分为（）这几类。

A．攻击检测和防御、访问控制、入侵检测 B．加密通信、防火墙配置、内容过滤 C．访问控制、数据备份、系统升级 D．流量清洗、网络隔离、带宽限制

121．防御拒绝服务攻击时很难确切地识别攻击源头的主要原因是（）。

A．源头在国外 B．攻击者技术很强 C．攻击源一般是大量受感染的普通电脑 D．攻击源一般是性能强悍的电脑

122．（）设备不属于传统的拒绝服务攻击防御设备。

A．防火墙 B．入侵检测系统IDS C．负载均衡器 D．数据泄露防护系统DLP

123．防火墙的特点中，（）的描述是正确的。

A．防火墙无法检测和阻止内部网络的攻击。 B．防火墙仅能过滤基于IP地址的攻击。 C．防火墙可以配置为允许特定类型的流量通过。 D．防火墙会增加网络延迟，影响性能。

124．Web 服务溢出攻击指的是（）。

A．利用漏洞获取服务器权限 B．向目标服务器发送大量请求导致其无法处理正常用户请求 C．向目标服务器提交恶意数据，使其执行非预期操作 D．通过社交工程手段诱使用户泄露敏感信息

125．（）不属于常见的系统安全事件分类。

A．未经授权的访问 B．数据泄露 C．系统性能下降 D．恶意软件感染

126．在信息系统安全管理中，常见系统安全事件记录的触发时机通常是（）。

A．系统管理员定期手动触发 B．安全事件发生时自动触发 C．系统升级或维护时触发 D．用户报告安全问题后触发

127．关于系统日志，描述最准确的是（）。

A．系统日志是用户自行创建的记录系统活动的文件。 B．系统日志仅记录操作系统层面的重要事件。 C．系统日志是自动记录计算机或系统活动信息的文件集合。 D．系统日志主要用于记录用户操作，与系统安全无关。

128．关于应用程序日志，描述正确的是（）。

A．应用程序日志是用户手动创建的文档，用于记录应用程序的使用情况 B．应用程序日志仅记录程序运行成功的记录 C．应用程序日志是自动记录应用程序运行、错误和警告等信息的文件 D．应用程序日志主要用于娱乐目的，记录用户与应用程序的有趣互动

129．关于安全日志，描述正确的是（）。

A．安全日志是用户自行编写的安全事件记录 B．安全日志仅记录系统启动和关闭的信息 C．安全日志是自动记录系统、应用程序和网络设备安全事件和行为的文件集合 D．安全日志主要记录用户日常操作，与系统安全无直接关联

130．在日志记录中，日志级别通常用于表示（）。

A．日志的存储位置 B．日志的生成时间 C．日志的重要性和详细程度 D．日志的编写人员

131．在常用的日志采集工具中，（）工具属于Java应用程序中常用的日志框架，并支持多种输出方式。

A．Logstash B．ELKStack C．Filebeat D．Log4j

132．（）工具不是用于日志分析的。

A．Kibana B．Graylog C．Prometheus D．Splunk

133．关于恶意代码的定义中，描述正确的是（）。

A．恶意代码是任何未经用户许可就运行的程序 B．恶意代码是故意设计来破坏、窃取信息或扰乱计算机系统正常运行的软件 C．恶意代码仅指那些包含广告或间谍行为的软件 D．恶意代码是计算机系统中不必要的代码

134．关于恶意代码的特征中，描述正确的是（）。

A．恶意代码通常会在计算机屏幕上显示彩色的广告 B．恶意代码都是个人或小团体秘密编写和散播的 C．恶意代码具有恶意的目的，本身是计算机程序，通过执行发生作用 D．恶意代码只会影响安装了特定操作系统的计算机

135．关于恶意代码的传播手段，描述正确的是（）。

A．恶意代码主要通过电子邮件附件的形式传播 B．恶意代码只会在移动存储设备上进行传播 C．恶意代码的传播方式多种多样，包括但不限于电子邮件附件、恶意网站链接、移动存储设备等 D．恶意代码只会在互联网上传播，不会通过其他途径

136．恶意代码在渗透过程中可能会利用（）技术。

A．脱敏 B．缓冲区溢出 C．分布式拒绝服务攻击 D．病毒扫描

137．关于恶意代码的自启动方法，（）描述最全面。

A．恶意代码主要利用Windows启动菜单启动 B．恶意代码通过修改系统文件配置实现自启动 C．恶意代码通过添加注册表启动项启动 D．恶意代码的自启动方法多种多样，包括但不限于通过服务启动、文件关联启动、修改系统配置文件启动等

138．（）不是恶意代码用来隐蔽自身的常用手段。

A．伪装成系统文件 B．修改为常见文件名 C．使用加密技术 D．存入数据库表中

139．恶意代码在感染系统后，为了不被立即发现，通常会选择（）策略进行潜伏。

A．立即执行破坏操作 B．保持静默，不进行任何活动 C．定期检查系统状态，等待时机 D．尝试自我修复和升级

140．（）技术可以帮助恶意代码在内存中隐藏自己，从而避免被安全软件发现。

A．进程注入技术 B．代码混淆技术 C．文件隐藏技术 D．加密技术

141．关于数据恢复，描述最准确的是（）。

A．数据恢复是通过正常途径恢复已丢失或损坏的数据 B．数据恢复是预防数据丢失的技术 C．数据恢复是当计算机存储介质损坏，导致部分或全部数据不能访问读出时，通过一定的方法和手段将数据重新找回，使信息得以再生的技术 D．数据恢复是一种备份技术，用于在数据丢失时快速恢复

142．关于数据恢复的技术分类，最正确的描述是（）。

A．数据恢复技术只包括逻辑数据恢复 B．数据恢复技术只包括物理数据恢复 C．数据恢复技术包括逻辑数据恢复和物理数据恢复 D．数据恢复技术包括软件恢复、物理恢复和固件恢复

143．数据恢复的应用场景不包括（）。

A．硬盘损坏 B．文件丢失 C．系统奔溃 D．数据加密

144．在数据恢复过程中，数据恢复软件的工作方式是（）。

A．数据恢复软件直接访问硬件并恢复物理损坏的数据 B．数据恢复软件通过修改操作系统的文件系统来恢复数据 C．数据恢复软件扫描存储介质，查找并恢复被删除但尚未被覆盖的文件 D．数据恢复软件能够预测未来可能丢失的数据并提前备份

145．（）是Windows操作系统中常用的文件系统。

A．EXT1 B．NTFS C．HFS+ D．EXT4

146．NTFS文件系统中的（）组件负责提供文件级别的安全性。

A．主文件表 B．访问控制列表 C．Boot扇区 D．文件记录

147．EXT文件系统是Linux操作系统中广泛采用的（）文件系统的扩展。

A．FAT B．HLS C．MBR D．EXT2

148．在计算机硬盘上，（）类型用于定义多个分区的布局和大小。

A．文件系统 B．引导扇区 C．分区表 D．主引导记录

149．（）软件专门针对Mac用户提供数据恢复服务，且支持多种Mac操作系统版本。

A．Disk Drill B．EaseUS Data Recovery Wizardfor Mac C．Stellar Data Recovery for Mac D．Paragon Backup&Recovery

150．相对于传统机械硬盘，固态硬盘的数据恢复面临的特殊挑战不包括（）。

A．擦除特性 B．不同的固件和控制器技术 C．NAND闪存单元的编程 D．缺乏专门的修复设备

信息安全管理员（四级）理论知识试卷答案

一、判断题(第1题～第40题。将判断结果填入括号中。正确的填“√”，错误的填“×”。每题0.5分，满分20分。)

1．√ 2．√ 3．× 4．√ 5．× 6．× 7．× 8．√ 9．√ 10．× 11．√ 12．× 13．√ 14．× 15．√ 16．× 17．√ 18．× 19．√ 20．× 21．× 22．√ 23．× 24．√ 25．√ 26．√ 27．× 28．√ 29．× 30．× 31．√ 32．√ 33．√ 34．√ 35．× 36．√ 37．√ 38．√ 39．√ 40．√ 41．√ 42．√ 43．√ 44．√ 45．× 46．× 47．√ 48．√ 49．√ 50．×

二、单项选择(第1题～第160题。选择一个正确的答案，将相应的字母填入题内的括号中。每题0.5分，满分80分。)

1．A 2．B 3．B 4．B 5．A 6．D 7．B 8．C 9．C 10．C 11．A 12．A 13．A 14．B 15．B 16．A 17．D 18．C 19．C 20．B 21．D 22．A 23．A 24．B 25．B 26．B 27．A 28．A 29．C 30．C 31．D 32．C 33．C 34．A 35．A 36．A 37．A 38．B 39．B 40．C 41．A 42．A 43．B 44．D 45．D 46．A 47．A 48．B 49．A 50．C 51．C 52．C 53．A 54．B 55．A 56．B 57．A 58．C 59．A 60．C 61．D 62．B 63．D 64．D 65．C 66．B 67．A 68．C 69．B 70．B 71．C 72．B 73．C 74．B 75．B 76．B 77．C 78．A 79．D 80．D 81．A 82．D 83．B 84．C 85．A 86．C 87．B 88．D 89．A 90．A 91．C 92．B 93．C 94．D 95．C 96．A 97．A 98．C 99．C 100．A 101．D 102．A 103．B 104．A 105．A 106．A 107．D 108．A 109．B 110．C 111．C 112．C 113．C 114．A 115．A 116．B 117．C 118．B 119．A 120．D 121．C 122．D 123．C 124．C 125．C 126．B 127．C 128．C 129．C 130．C 131．D 132．C 133．B 134．C 135．C 136．B 137．D 138．D 139．B 140．A 141．C 142．C 143．D 144．C 145．B 146．B 147．D 148．C 149．C 150．D