**第5部分**

理论知识考试模拟试卷及答案

信息安全管理员（三级）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 | 三 | 总 分 |
| 得 分 |  |  |  |  |

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

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．随着全球化的发展，职业道德也呈现出单一化的趋势，不同国家和地区的职业道德规范不存在差异。（ ）

2．职业道德仅涉及个人行为，与组织文化和行业规范无关。（ ）

3．职业守则是由国家或行业制定的，对从业人员不具有普遍约束力。（ ）

4．职业守则对于提高从业人员的专业素质和职业道德水平具有重要作用。（ ）

5．显卡的主要功能是处理文本。（ ）

6．计算机软件仅由一系列指令组成，不涉及任何数据。（ ）

7．用人单位在任何情况下都可以无条件地解雇员工。（ ）

8．劳动关系仅仅是一种经济关系，不涉及人身关系。（ ）

9．交换机默认情况下对所有端口进行广播传输。（ ）

10．交换机端口安全功能可以完全防止未经授权的设备连接到网络。（ ）

11．路由协议可以根据其工作原理分为距离矢量路由协议和链路状态路由协议。（ ）

12．路由协议的原理是通过交换网络拓扑信息和路由信息，使路由器能够动态地选择最佳路径。（ ）

13．防火墙可以分为静态防火墙和动态防火墙两类。（ ）

14．防火墙的主要功能是根据预设的安全策略，监控和控制网络之间的数据流，以防止未经授权的访问和攻击。（ ）

15．入侵检测系统IDS通常部署在网络的关键位置，如防火墙后面，以保护内部网络不受外部攻击。（ ）

16．IDS只能检测已知的攻击模式，无法发现新的攻击手段。（ ）

17．无线AC的安全配置方法包括设置强密码、启用MAC地址过滤和关闭SSID广播。（ ）

18．无线网络的加密方式只有WPA和WPA2两种。（ ）

19．网络安全审计的功能仅限于识别和记录网络中的安全事件。（ ）

20．安全审计系统仅根据审计对象的不同进行分类。（ ）

21．恶意代码是一种旨在破坏计算机系统或窃取用户信息的软件程序。（ ）

22．恶意代码的唯一危害是对计算机系统造成损坏。（ ）

23．文件系统是操作系统中负责管理和存取文件信息的软件。（ ）

24．加密文件系统EFS仅对存储在NTFS文件系统上的文件进行加密。（ ）

25．钓鱼攻击只能通过电子邮件进行。（ ）

26．计算机系统攻击信息收集方法包括病毒传播。（ ）

27．在Windows系统中，禁用管理员账户可以提高系统的安全性。（ ）

28．Windows 本地安全策略的功能仅限于管理用户账户权限和审计系统事件。（ ）

29．所有的应用安全威胁都必然导致数据泄露或系统崩溃。（ ）

30．Web应用攻击的产生往往是由于开发者在编写代码时未充分考虑安全性。（ ）

31．应用安全审计的目的是为了发现并修复应用程序中的所有安全漏洞。（ ）

32．应用系统若无任何日志审计功能，无法对用户的重要行为进行审计，可判定为中风险。（ ）

33．传输加密只应用于互联网通信，以保护数据在传输过程中的安全。（ ）

34．AES加密算法是一种分组密码算法，其密钥长度固定为128位。（ ）

35．WAF 对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，为Web应用提供防护。（ ）

36．Web应用防火墙WAF的工作原理主要是通过分析HTTP请求和响应的头部及内容，来检测和阻止针对Web应用程序的恶意攻击。（ ）

37．访问控制策略定义了用户可以访问的资源，以及在什么条件下可以访问，这通常基于安全和业务的要求。（ ）

38．身份验证是确定用户是否具有访问系统的权限的过程。（ ）

39．无线局域网接入技术中的WPA2协议比WPA协议更安全。（ ）

40．WPA3是当前最安全的无线网络认证机制之一，它提供了比WPA2更强的安全保护。（ ）

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

二、单项选择（第1题～第140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70分。）

1．职业守则的制定过程中，（）原则不需要遵循。

A．公开 B．公正 C．公平 D．保密

2．在职业守则的监督过程中，（）是最基本的形式。

A．自我检查 B．上级审查 C．同事互评 D．客户反馈

3．（）软件类别主要用于创建和管理文档。

A．游戏软件 B．网络浏览器 C．文字处理软件 D．多媒体播放器

4．根据操作系统的分类，（）属于批处理系统。

A．Windows XP B．UNIX C．DOS D．Linux

5．在用户管理系统中，如果需要对某个用户进行权限调整，应该通过（）来实现。

A．用户编辑 B．角色管理 C．权限分配 D．用户分组

6．（）是关系数据库中最基本的数据单位。

A．记录 B．字段 C．表 D．视图

7．非关系型数据库主要解决（）问题。

A．安全 B．海量数据存储 C．复杂查询 D．事务处理

8．在SQL中，用于指定查询结果的排序顺序的子句是（）。

A．ORDER BY B．GROUP BY C．HAVING D．DISTINCT

9．女职工生育享受（）天的产假。

A．70 B．89 C．98 D．108

10．知识产权法的基本原则中，旨在保护创作者权益，确保其能从自己的智力劳动中获得合理回报的原则是（）。

A．合法性原则 B．合理性原则 C．公平性原则 D．激励创新原则

11．根据著作权法，（）不属于其保护对象。

A．文字作品 B．口述作品 C．商标设计 D．音乐作品

12．为了有效保护知识产权，权利人通常可以采取（）措施来防止他人未经许可使用其知识产权。

A．口头警告 B．公开发表声明 C．加密保护 D．行政救济

13．根据《中华人民共和国网络安全法》的实施要点，负责统筹协调网络安全工作和相关监督管理工作的是（）。

A．国家互联网信息办公室 B．公安部 C．工业和信息化部 D．国家安全部

14．根据《中华人民共和国网络安全法》的规定，（）不属于该法所规定的“网络运营者”范畴。

A．网络服务提供商 B．网络设备制造商 C．个人用户 D．互联网公司

15．恶意代码通常隐藏在正常文件中，以逃避安全软件的检测。这种特征被称为（）。

A．可变性 B．传播性 C．破坏性 D．隐蔽性

16．恶意代码通常隐藏在正常的软件或文件中，以逃避安全检测。这种隐藏方式属于（）。

A．混淆 B．伪装 C．嵌入 D．压缩

17．（）文件系统能支持4GB的单个文件大小。

A．FAT8 B．FAT16 C．FAT32 D．FAT64

18．NTFS文件系统与FAT文件系统相比，（）不是其优势。

A．更高的安全性 B．更好的性能 C．支持更大的文件和磁盘容量 D．兼容性好，可以在不同操作系统上使用

19．Ext3文件系统相对于Ext2文件系统的主要改进是（）。

A．支持更大的文件和文件系统容量 B．提高了文件系统的读写速度 C．引入了日志功能，提高了文件系统的稳定性和可靠性 D．支持数据压缩

20．网络文件系统NFS主要目的是（）。

A．实现本地文件系统的备份和恢复 B．允许用户通过网络访问远程文件系统 C．提高本地文件系统的读写速度 D．简化文件系统的管理和配置

21．关于DoS和DDoS攻击，（）最准确地反映了这两种攻击之间的主要区别。

A．DoS攻击是由一个攻击者发起的，而DDoS攻击是由多个攻击者协同发起的。 B．DoS攻击的目标是单个系统或服务，DDoS攻击则针对整个网络。 C．DoS攻击主要通过消耗带宽和资源来使服务不可用，DDoS攻击除此之外还利用大量合谋的机器来放大攻击效果。 D．两者在防御策略上没有显著差异，都需要更新安全补丁和部署防火墙等防护措施。

22．（）不是对DoS攻击的防范方法。

A．网络流量过滤 B．限制连接数量 C．增加网络带宽 D．部署防火墙

23．口令攻击方法的前提是必须先得到该主机上的（）,然后再进行该用户口令的破译。

A．合法帐号 B．IP地址 C．使用日志 D．漏洞

24．在口令攻击中，攻击者往往采用中途截击的方法来获取用户帐户和密码。（）协议能有效防止这种攻击。

A．Telnet B．SMTP C．HTTPS D．HTTP

25．在Windows自带防火墙中，（）不是通过“高级设置”界面进行管理的功能。

A．入站规则配置 B．出站规则配置 C．连接安全规则配置 D．防火墙状态查看

26．关于Windows系统漏洞的修补方式，（）方法通常被认为是主动防御措施。

A．定期检查系统更新并安装补丁 B．安装第三方安全软件进行实时防护 C．对系统进行全面的安全扫描 D．进行系统级数据加密

27．了加固Linux账户安全，以（）密码策略是不推荐使用的。

A．强制用户定期更换密码 B．设置密码的最小长度要求 C．限制密码最大长度 D．要求用户输入复杂的密码组合

28．为了加固Linux SSH登录安全，不建议的措施是（）。

A．禁用root账户登录 B．启用公钥认证 C．保留默认的SSH端口22 D．使用强密码策略

29．（）不是常见Web应用攻击产生的直接危害。

A．数据篡改 B．系统资源耗尽 C．用户体验下降 D．病毒传播

30．（）不是防范常见Web应用攻击的有效措施。

A．输入验证和过滤 B．禁用JavaScript C．使用安全的会话管理技术 D．定期进行安全审计

31．（）最不可能导致缓冲区溢出。

A．输入数据超出预期长度 B．程序内部计算错误导致数组越界 C．使用未初始化的指针 D．程序正常处理边界条件

32．在防范缓冲区溢出的措施中，（）是通过编译器自动插入安全代码来实现的。

A．手动添加边界检查 B．使用安全的缓冲区操作函数 C．开启编译器的堆栈保护选项 D．限制用户输入的长度

33．（）不是应用安全审计的主要内容。

A．评估应用程序的安全性 B．修复应用程序中的安全漏洞 C．分析应用程序的日志文件 D．测试应用程序对常见攻击的防御能力

34．（）不属于代码审计的范畴。

A．对源代码进行静态分析 B．对编译后的二进制文件进行逆向工程 C．对应用程序进行动态测试 D．检查代码是否符合编码规范

35．代码审计中，（）不是主要关注点。

A．检测代码中的安全漏洞 B．评估代码的可维护性 C．检查代码的语法错误 D．分析代码的性能瓶颈

36．（）不属于应用安全审计的分类。

A．静态应用安全审计 B．动态应用安全审计 C．混合应用安全审计 D．实时应用安全审计

37．（）非对称加密算法基于大数分解问题。

A．RSA B．DSA C．ECC D．ElGamal

38．（）不是一种加密哈希函数。

A．MD5 B．SHA-1 C．SHA-256 D．CRC

39．关于数字签名的原理，（）的描述是错误的。

A．数字签名使用加密算法对消息进行加密，确保消息的机密性。 B．数字签名使用签名者的私钥对消息的哈希值进行加密，确保消息的完整性和来源。 C．数字签名可以防止消息篡改和身份冒充。 D．数字签名与消息一起传输，作为验证消息真实性的依据。

40．关于数字证书的功能，（）是不正确的。

A．数字证书用于验证网站的真实性，防止钓鱼攻击。 B．数字证书可以确保电子邮件的机密性和完整性。 C．数字证书仅用于验证公钥持有者的身份。 D．数字证书可以用于安全地存储和传输敏感信息。

41．关于Web应用防火墙WAF的安全策略，不正确的描述是（）

A．WAF的安全策略可以基于IP地址来限制访问。 B．WAF的安全策略可以基于URL路径来限制访问。 C．WAF的安全策略无法动态调整以适应变化的威胁环境。 D．WAF的安全策略可以基于用户代理字符串来识别和阻止特定类型的设备。

42．关于WAF日志记录与审计，不正确的描述是（）。

A．WAF日志记录了所有经过WAF的HTTP请求和响应。 B．WAF日志仅包含有关被阻止攻击的信息。 C．WAF日志可用于安全事件响应和取证分析。 D．WAF日志应定期备份，以防数据丢失。

43．关于WAF异常行为检测，不正确的描述是（）。

A．WAF通过分析HTTP请求的参数和头信息来进行异常行为检测。 B．WAF的异常行为检测功能无法应对零日攻击。 C．WAF可以根据历史数据和当前行为模式来检测异常行为。 D．WAF的异常行为检测功能可以提高对未知威胁的防御能力。

44．关于WAF性能优化与维护更新，不正确的描述是（）。

A．为了提高性能，WAF应该尽可能多地处理请求 B．定期更新WAF的规则集是维护其有效性的关键 C．WAF的性能优化通常涉及到调整缓存大小和请求处理线程数 D．WAF的维护更新应该在不影响业务连续性的前提下进行

45．在网络中实施基本访问控制时，（）方法是最常见的。

A．物理隔离 B．MAC地址过滤 C．端口安全 D．VPN使用

46．在网络访问权限的审核过程中，（）不是必须进行的步骤。

A．验证用户身份 B．检查用户请求的合理性 C．立即批准所有访问请求 D．定期审查权限设置

47．在无线网络中，（）加密技术能够提供端到端的加密服务。

A．WEP B．WPA C．WPA2 D．IPsec VPN

48．为了限制无线网络的接入，网络管理员应使用（）技术。

A．MAC地址过滤 B．端口转发 C．IP地址分配 D．路由选择

49．网络设备日志的主要作用是（）。

A．节省存储空间 B．记录设备运行状态 C．提高网络传输速度 D．优化网络拓扑结构

50．在网络设备日志中，（）最常用于安全事件响应。

A．错误日志 B．警告日志 C．信息日志 D．调试日志

51．关于网络设备日志的生成和配置，错误的描述是（）。

A．日志级别是可以自定义的，以满足不同场景的需求 B．日志格式通常由设备制造商预先定义，用户无法更改 C．日志轮询是减少日志文件大小的一种有效方法 D．日志存储位置应选择安全且可靠的地方，以防止数据丢失

52．网络设备日志最佳的存储位置是（），以确保其完整性和可访问性。

A．本地硬盘 B．网络存储设备 C．云存储服务 D．远程服务器

53．远程访问是指通过网络从（）位置访问和操作计算机系统的能力。

A．相邻 B．远程 C．同一 D．本地

54．（）不是虚拟私人网络VPN的主要功能。

A．保证数据传输的安全性 B．加速数据在网络中的传输速度 C．允许用户通过公共网络安全地连接到远程网络资源 D．提供远程用户与本地网络之间的身份验证

55．在身份认证过程中，（）方法主要用于验证用户的身份。

A．加密 B．数字签名 C．身份验证令牌 D．安全套接字层

56．（）加密技术主要应用于对称密钥加密，并且在现代加密通信中仍然广泛使用。

A．RSA B．AES C．DES D．Diffie-Hellman

57．关于漏洞的定义，正确的描述是（）。

A．漏洞是软件或硬件中故意留下的后门，以便于攻击者进入系统 B．漏洞是软件或硬件的设计缺陷或实现错误，可能被攻击者利用来执行未授权的操作 C．漏洞是网络安全领域的专业术语，与系统安全无关 D．漏洞只存在于操作系统中，与其他软件无关

58．在漏洞利用原理中，"堆栈溢出"通常指的是（）。

A．攻击者向程序输入的数据超出了预期长度，导致内存区域被覆盖 B．攻击者利用程序中的逻辑错误，使得程序跳转到错误的地址执行 C．攻击者通过修改程序的内存布局，使得程序执行流程发生改变 D．攻击者利用程序中的权限检查漏洞，获取了更高的权限

59．在漏洞生命周期中，

A．漏洞刚被发现，尚未公开披露 B．漏洞已被公开披露，但未出现针对该漏洞的攻击 C．漏洞已被公开披露，且已有攻击者利用该漏洞发起攻击 D．漏洞已被修复，不再构成威胁

60．在漏洞检测技术中，（）技术通过模拟攻击者的行为来尝试利用漏洞。

A．静态代码分析 B．动态代码分析 C．渗透测试 D．漏洞扫描

61．备份的定义是（）。

A．将数据从原始位置复制到另一个位置的过程 B．将数据从原始位置移动到另一个位置的过程 C．将数据从原始位置删除，然后在另一个位置创建副本的过程 D．将数据从原始位置加密，然后在另一个位置解密的过程

62．在数据库备份策略中，增量备份和差异备份的主要区别是（）。

A．增量备份只备份自上次完全备份以来的更改，而差异备份备份自上次任何类型备份以来的更改。 B．差异备份只备份自上次完全备份以来的更改，而增量备份备份自上次任何类型备份以来的更改。 C．增量备份备份数据的频率高于差异备份。 D．差异备份恢复数据的速度比增量备份快。

63．数据完整性是指（）。

A．数据不会丢失 B．数据在多个副本之间保持一致 C．数据符合预定义的规则和约束条件 D．数据可以被所有授权用户访问

64．版本控制系统的主要目的是（）。

A．自动化软件开发过程中的构建和部署任务 B．提供一个集中的平台，用于存储和管理不同版本的软件代码和文档 C．跟踪软件开发过程中的变更历史，以便于回溯和协作 D．实现软件开发过程中的持续集成和持续交付

65．在备份存储介质中，（）介质通常用于长期归档存储，因为它具有较好的成本效益和较长的数据保留周期。

A．固态硬盘 B．磁盘阵列 C．磁带库 D．云存储服务

66．在备份存储介质中，（）介质的特点是读写速度较快，但价格较高，且不适合长期归档存储。

A．磁盘驱动器 B．光盘驱动器 C．磁带驱动器 D．闪存驱动器

67．系统日志的主要目的是（）。

A．记录系统操作以进行故障排查和性能优化 B．存储用户登录信息和访问权限 C．跟踪网络流量和潜在的安全威胁 D．管理系统资源和分配内存

68．系统日志管理对于保持系统的完整性和可用性至关重要的原因是（）。

A．它可以加快系统启动速度 B．它有助于检测和预防恶意软件攻击 C．它可以释放磁盘空间 D．它确保所有用户都能访问系统资源

69．在系统日志中，（）主要记录系统的日常运行状态，如服务的启动和停止。

A．错误日志 B．访问日志 C．调试日志 D．信息日志

70．在日志采集过程中，（）方式能够实时地将日志数据从源系统传输到日志中心，且通常不需要修改源系统的配置。

A．Logstash B．Fluentd C．Syslog协议 D．Filebeat

71．日志采集技术中，基于流式处理的日志采集方法主要利用（）技术实现。

A．TCP/IP协议栈 B．HTTP/HTTPS协议 C．消息队列 D．正则表达式匹配

72．在系统日志分析中，（）方法是用来检测异常行为的最有效手段。

A．基于规则的匹配 B．基于统计的异常检测 C．人工审查 D．图像识别技术

73．在应用安全的风险识别过程中，（）是首要的任务。

A．彻底测试所有功能模块 B．确定潜在的威胁来源 C．分析历史安全事件报告 D．配置防火墙和入侵检测系统

74．在安全开发生命周期中，（）阶段专注于确保软件代码的安全性和质量。

A．需求分析 B．设计 C．编码 D．测试

75．在互联网应用中，OAuth 2.0主要用于（）类型的认证和授权。

A．用户登录 B．API访问 C．资源共享 D．邮件传输

76．在互联网应用中，（）加密技术主要用于保护数据的机密性，并且在两个通信方之间建立一个安全的通信通道。

A．SSL/TLS B．AES C．RSA D．SHA-256

77．在互联网应用中，输入验证的主要目的是（）。

A．提高用户体验 B．减少服务器负载 C．防止注入攻击 D．确保数据灵活性

78．在互联网应用中，会话管理的核心目的是（）。

A．节省服务器资源 B．提高用户体验 C．确保用户身份的安全性和会话的完整性 D．降低网络延迟

79．数据过滤的主要目的是（）。

A．增加数据量 B．减少数据量 C．提高数据质量 D．降低数据存储成本

80．在数据过滤技术中，（）主要用于根据数据的统计特性进行过滤。

A．基于规则的方法 B．基于机器学习的方法 C．基于统计的方法 D．基于专家知识的方法

81．包过滤防火墙主要工作的网络层次是（）。

A．物理层 B．数据链路层 C．网络层 D．传输层

82．内容过滤技术主要应用领域不包括（）。

A．网络防火墙 B．入侵检测系统 C．垃圾邮件过滤 D．MAC地址过滤

83．端点过滤通常用于（）场景。

A．服务器与服务器之间的数据传输 B．企业内部网络环境中的终端用户设备 C．互联网服务提供商级别 D．主数据中心的出入口

84．数据过滤规则在数据处理流程中起着至关重要的作用，（）的说法是不正确的。

A．数据过滤规则可以帮助去除重复或无效的数据。 B．数据过滤规则通常基于预设的条件和模式进行匹配。 C．数据过滤规则只能在数据收集阶段应用。 D．精确的数据过滤规则有助于提升数据分析的准确性。

85．在互联网访问日志记录中，（）信息最常用于追踪用户在网站上的行为路径。

A．用户代理字符串 B．服务器响应时间 C．会话ID D．引用页面

86．在互联网访问日志的收集过程中，通常使用（）协议来传输日志数据到日志服务器。

A．HTTP B．FTP C．Syslog D．SMTP

87．（）方式最常用于互联网访问日志的数据。

A．关系型数据库 B．非关系型数据库 C．列式存储 D．文件系统

88．对于互联网访问日志的分析，（）方法可以帮助我们快速定位到访问量突增的原因。

A．时序分析 B．关联规则分析 C．聚类分析 D．回归分析

89．（）加密技术最适合用于互联网访问日志的存储和传输。

A．对称加密 B．非对称加密 C．哈希加密 D．混合加密

90．在监控互联网访问日志时，（）方法最有效地检测到潜在的恶意活动。

A．实时分析日志条目，寻找异常模式。 B．定期检查日志摘要，忽略详细条目。 C．仅关注特定来源的流量，忽略其他来源。 D．使用简单的关键词搜索来识别已知攻击。

91．关于网络监控的定义，（）最准确地描述了其主要功能。

A．实时监测网络流量，确保网络带宽的充分利用。 B．追踪和记录网络活动，以便在发生问题时进行回溯分析。 C．对网络设备和系统的安全漏洞进行周期性扫描和修复。 D．自动调整网络配置，以适应不断变化的网络环境。

92．在网络监控中，基于网络流量进行详细分析以识别潜在威胁的监控方式被称为（）。

A．性能监控 B．安全监控 C．协议分析 D．应用层监控

93．在金融交易环境中，网络监控主要用于（）。

A．提升系统性能 B．用户行为分析 C．保障交易安全 D．优化用户体验

94．分布式网络监控的优点是（）。

A．集中资源进行高效的监控处理 B．减轻单点故障的风险 C．只需在一个地点部署监控设备 D．不需要考虑数据隐私保护

95．关于攻击流量的特征，不准确的描述是（）。

A．攻击流量通常具有突发性和高流量特点。 B．攻击流量往往针对特定的目标系统或服务。 C．攻击流量的目的是正常的数据传输和通信。 D．攻击流量可能由自动化脚本或僵尸网络发起。

96．（）属于常见的网络攻击流量。

A．由大量用户同时访问网站产生的正常HTTP流量 B．使用伪造源地址发送的大量TCP连接请求流量 C．公司内部员工在工作时间进行的文件传输流量 D．家庭用户在家中观看在线视频的流量

97．SYN Flood 攻击是一种拒绝服务DoS攻击，它的主要原理是（）。

A．通过发送大量完整的TCP连接请求，使服务器处理不过来。 B．通过发送大量伪造的SYN请求，使服务器在等待确认的过程中资源耗尽。 C．通过发送大量错误的IP地址，使服务器无法找到正确的连接。 D．通过发送大量不完整的TCP连接请求，使服务器无法完成连接建立。

98．UDP Flood攻击主要是通过（）方式对目标系统造成影响的。

A．通过发送大量伪造的UDP数据包，使目标系统忙于处理这些无效的数据包。 B．通过发送大量真实的UDP数据包，消耗目标系统的带宽和处理器资源。 C．通过发送特定类型的UDP数据包，触发目标系统的漏洞。 D．通过利用UDP协议的缺陷，直接攻击目标系统的网络栈。

99．在网络安全领域中，（）方法或工具最常用于网络安全事件的发现。

A．安全日志分析 B．入侵检测系统 C．防火墙 D．安全扫描器

100．（）不属于网络安全事件评估的主要内容。

A．事件性质 B．事件发生的频率 C．事件造成的损失 D．事件的发展趋势

101．（）隔离措施适用于处理具有高度传染性的网络病毒。

A．关闭受影响的系统 B．限制网络访问 C．防止病毒传播到其他系统 D．对受影响的系统进行全面消毒

102．（）不属于网络安全事件信息收集的原则。

A．及时性原则 B．完整性原则 C．准确性原则 D．保密性原则

103．计算机病毒的主要目的是（）。

A．破坏硬件 B．改善计算机性能 C．降低计算机使用成本 D．破坏数据和干扰计算机操作

104．按照依附的媒体类型分类，计算机病毒主要可以分为（）。

A．引导型病毒、文件型病毒、混合型病毒 B．蠕虫病毒、木马病毒、脚本病毒 C．良性病毒、恶性病毒 D．附件型病毒、嵌入型病毒、外壳型病毒

105．计算机病毒的主要传播途径通常不包括（）。

A．通过U盘/移动硬盘传播 B．通过正规软件商店下载的软件传播 C．通过电子邮件传播 D．通过网页传播

106．（）是计算机病毒最显著的特征。

A．寄生性 B．传染性 C．潜伏性 D．破坏性

107．系统后门通常被用于（）。

A．提高系统的安全性 B．允许开发人员远程调试系统 C．使攻击者能够未经授权的访问系统 D．限制用户对系统资源的访问

108．（）是系统后门类型中隐蔽性最低的。

A．Rhosts ++后门 B．嗅探欺骗后门 C．校验和及时间戳后门 D．Rootkit

109．在检测系统后门时，（）方法主要用于查找和分析系统的源代码中是否存在后门。

A．网络流量监控 B．漏洞扫描 C．代码审查 D．敏感词检测

110．在清除系统后门时，（）方法通常被视为最有效和彻底的解决方案。

A．使用杀毒软件进行全面扫描 B．进入安全模式并手动删除相关文件 C．定期更新系统和软件补丁 D．备份数据并重新安装操作系统

111．（）不是获取计算机病毒样本的主要目的。

A．分析病毒的感染和传播机理 B．了解病毒对系统和数据的危害程度 C．快速清除用户计算机中的病毒 D．为研发新的防病毒产品提供基础数据支持

112．在留存计算机病毒样本时，（）方法被普遍认为是安全且有效的。

A．直接存储在电脑硬盘的常规文件夹中 B．使用虚拟机并在虚拟机中存储病毒样本 C．将病毒样本存储在U盘中，便于携带和分享 D．通过电子邮件将病毒样本发送给自己，以便日后下载

113．在计算机安全领域，对于计算机病毒样本的加密隐藏存储，（）方法更为有效和安全。

A．将病毒样本直接存储在电脑硬盘的隐藏文件夹中 B．使用专门的加密软件对病毒样本进行加密后存储在硬盘中 C．将病毒样本存储在U盘中，并对U盘进行物理隐藏 D．将病毒样本存储在网络云盘中，并设置复杂的访问密码

114．在计算机病毒研究中，使用沙盘或沙箱技术留存病毒样本的主要优势是（）。

A．沙盘技术可以模拟真实环境，便于病毒样本的激活和分析 B．沙盘技术能够彻底隔离病毒样本，保护真实系统免受威胁 C．沙盘技术能够增加病毒样本的可见性，便于检测和识别 D．沙盘技术可以提高病毒样本的复制速度，加速研究进程

115．系统安全事件处置流程中，通常第一步应该执行的是（）。

A．确定事件性质和严重程度 B．启动应急预案并通知所有相关人员 C．收集并分析受影响系统的日志数据 D．尝试恢复受损的系统或服务

116．（）不属于常见的系统安全事件类别。

A．拒绝服务攻击 B．数据泄露事件 C．软件升级导致的系统崩溃 D．未经授权的物理访问

117．在处理复杂的恶意软件感染时，为了确保清除工作的彻底性，（）措施是不恰当的。

A．遵循由防病毒软件供应商提供的清除指南 B．结合使用多种扫描工具以覆盖更多种类的恶意软件 C．删除系统上所有可疑的文件和程序 D．在清除过程中持续监控系统行为以防意外情况发生

118．在数据泄露事件发生后，为了迅速响应并减轻损失，应当首先（）。

A．分析泄露数据的内容和类型以确定影响范围 B．通知受影响的客户并告知可能受到的风险 C．切换到备用系统以维持业务的持续性 D．立即停止所有可能涉及到数据泄露的系统服务

119．在日志分类中，（）是按照日志的来源进行划分的。

A．系统日志 B．安全日志 C．应用日志 D．审计日志

120．在应用程序日志中，（）最可能包含关于用户操作行为的信息。

A．错误日志 B．警告日志 C．信息日志 D．调试日志

121．在提取日志时，（）通常适用于需要对日志数据进行复杂处理和实时分析的场景。

A．使用文本编辑器手动查找 B．利用日志分析工具 C．编写自定义脚本来提取日志 D．直接查看日志文件

122．在提取数据库日志时，（）通常被认为是最直接且高效的方式，尤其适用于大型数据库环境。

A．手动导出日志文件 B．使用数据库管理工具的日志导出功能 C．编写SQL查询语句来提取日志 D．利用操作系统命令行工具

123．日志分析中，基于规则的分析方法通常依赖于预先定义的规则集来识别特定的安全事件。（）不是基于规则的日志分析方法的主要特点。

A．高效性 B．准确性 C．灵活性 D．易于实现

124．在日志规范化的过程中，（）是用来确保日志数据在不同系统和平台间具有一致性的。

A．格式转换 B．时间戳标准化 C．数据脱敏 D．关键字段定义

125．在日志分析中，如果采用基于访问频率的分析方法来检测异常行为，（）不是该方法的主要优点。

A．实时性强 B．准确性高 C．不能预判未知攻击 D．易于实现

126．在基于特征的日志分析方法中，（）不是特征提取的关键步骤。

A．数据预处理 B．特征选择 C．特征构造 D．模型训练

127．基于统计的日志分析方法中，（）统计量通常用于衡量日志数据中某事件发生的频率。

A．均值 B．中位数 C．众数 D．方差

128．在基于关联的日志分析方法中，（）最常用于在多个日志源之间建立事件之间的关联。

A．时间戳匹配 B．IP地址关联 C．用户身份认证 D．事务ID跟踪

129．违法有害信息的主要特点之一是具有（）。

A．煽动性 B．真实性 C．灵活性 D．合法性

130．根据违法有害信息识别方法的分类，（）是通过对网络信息进行语义理解来识别违法有害信息的。

A．内容分析法 B．关键词过滤法 C．社交网络分析法 D．用户行为分析法

131．在识别违法有害信息时，对待来源不明的信息，应当（）。

A．轻信并传播 B．不轻信，要求核实 C．忽略这些信息 D．举报所有来源不明的信息

132．在进行违法有害信息举报时，最重要的是（）。

A．提供详细的信息 B．选择合适的举报平台 C．确保举报内容真实可靠 D．快速提交举报

133．基于规则的违法有害信息识别方法通常采用（）规则来识别信息。

A．关键词过滤 B．语义分析 C．机器学习模型 D．人工审核

134．在利用机器学习识别违法有害信息时，数据量不足可能导致（）问题。

A．模型过拟合 B．模型欠拟合 C．模型超拟合 D．模型可解释性差

135．在应用安全事件的处置流程中，隔离受影响的系统是为了（）。

A．防止事件扩大 B．保护数据安全 C．追踪事件原因 D．恢复系统功能

136．制定应急响应计划的主要目的是（）。

A．快速恢复系统正常运行 B．减少事件造成的损失 C．预防类似事件再次发生 D．提升团队的安全意识

137．为了防止网页内嵌恶意代码，用户应该安装并定期更新（）。

A．杀毒软件 B．浏览器 C．视频播放器 D．文档编辑器

138．（）措施可以有效预防SQL注入攻击。

A．使用参数化查询 B．关闭所有网络连接 C．使用强密码策略 D．定期更新操作系统

139．在处理非授权访问事件时，（）步骤是错误的。

A．确认非授权访问的事实 B．确定受影响的数据和资源 C．立即删除所有受影响的数据 D．通知相关利益方

140．使用HttpOnly标志设置Cookie的主要目的是（）。

A．为了提高Cookie的安全性 B．为了增加Cookie的存储空间 C．为了减少Cookie的传输速度 D．为了降低Cookie的消耗

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

三、多项选择（第1题～第10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1分，满分10分。）

1．职业道德基本知识中，关于奉献社会的要求，正确的是（）。

A．树立正确的义利观 B．认真履行岗位职责 C．正确处理个人利益和集体利益的关系 D．增强社会责任感 E．以我为主

2．（）属于职业守则主要包括的道德规范。

A．诚实守信 B．尊重他人 C．保护环境 D．遵守行业规定 E．追求个人利益最大化

3．计算机的输入设备有（）。

A．键盘 B．鼠标 C．手写板 D．打印机 E．显示器

4．（）原则是劳动合同订立时应当遵循的。

A．长期合作 B．最低工资 C．平等 D．自愿 E．互利共赢

5．关于交换机的功能，说法正确的是（）。

A．交换机可以增加网络中广播帧的数量 B．交换机可以根据MAC地址表进行数据帧的转发 C．三层交换机可以实现不同VLAN之间的通信 D．交换机无法识别IP地址 E．工作在OSI模型的网络层

6．关于路由器的安全管理方式，正确的包括（）。

A．访问控制列表ACL可以限制特定IP地址或端口的网络访问 B．路由器可以通过配置防火墙规则来阻止外部攻击 C．路由器支持SSH远程安全登录，以增强管理安全性 D．路由器无法进行病毒扫描和防护 E．路由器可以配置VPN以提供安全的远程访问

7．关于边界防护设备的概念，（）这些描述是正确的。

A．边界防护设备可以部署在网络边缘，保护内部网络免受外部威胁 B．边界防护设备可以实时监控网络流量，检测并阻止恶意攻击 C．边界防护设备可以提高网络的安全性和保密性 D．边界防护设备无法防止内部用户的恶意行为 E．边界防护设备可以记录网络活动，便于事后审计和溯源

8．关于入侵检测系统IDS的概念，正确的包括（）。

A．IDS是一种主动防御技术，能够实时监控网络流量并检测潜在的攻击。 B．IDS通常部署在网络边缘，作为第一道防线来阻止外部威胁。 C．IDS可以分析网络流量中的异常行为，如恶意软件传播、拒绝服务攻击等。 D．IDS在检测到攻击时，会自动采取相应的措施来阻止攻击。 E．IDS主要依赖于已知的攻击特征库来进行攻击检测。

9．无线网络安全面临的威胁包括（）。

A．恶意软件 B．黑客攻击 C．无线电干扰 D．信号覆盖不足 E．数据泄露

10．网络安全审计通常包括（）。

A．身份验证和授权机制 B．数据保护和隐私政策 C．系统和应用程序的安全性 D．应急响应计划 E．网络带宽

信息安全管理员（三级）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．√

二、单项选择(第1题～第140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70分。)

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

三、多项选择(第1题～第10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1分，满分10分。)

1．ABCD 2．ABCD 3．ABC 4．CD 5．BCD 6．ABCE 7．ABCE 8．ACE 9．ABCE 10．ABCD