2020 年网络信息安全技术知识竞赛题库及答案
（共 120 题）

1. 软件驻留在用户计算机中　侦听目标计算机的操作　并可对目标计算机进行特定操作的

黑客攻击手段是____B_____。

a. 暴力破解

b. 木马

c. 拒绝服务

d. 缓冲区溢出

2. 以下哪一种方式是入侵检测系统所通常采用的　___A___。

a. 基于网络的入侵检测

b. 基于域名的入侵检测

c. 基于 IP 的入侵检测

d. 基于服务的入侵检测

3. 在各种防火墙结构中　就其本质而言　主要有以下四种　屏蔽路由器、双宿/多宿主机

模式、___A___和屏蔽子网模式

a. 屏蔽主机模式

b. 堡垒主机模式

c. 代理服务器模式

d. 应用级网关模式

4. 用于实现身份鉴别的安全机制是__B____。

a. 访问控制机制和路由控制机制

b. 加密机制和数字签名机制

c. 加密机制和访问控制机制

d. 数字签名机制和路由控制机制

5. 以下不属于代理服务技术优点的是___D_____

a. 可以实现身份认证

b. 可以实现访问控制

c. 内部地址的屏蔽和转换功能

d. 可以防范数据驱动侵袭

6. 未经授权的方式使用网络资源　称之为__A___

a. 非法访问

b. 窃取

c. 非法入侵

d. 冒充

7. 包过滤技术与代理服务技术相比较___C_____。

a. 包过滤技术安全性较弱、但会对网络性能产生明显影响

b. 代理服务技术安全性高　对应用和用户透明度也很

c. 包过滤技术对应用和用户是绝对透明的

d. 代理服务技术安全性较高、但不会对网络性能产生明显影

8. 下列不属于防火墙核心技术的是_C___。

a. 应用代理技术

b. NAT技术

c. 日志审计

d. (静态　动态)包过滤技术

9. 下列对计算机网络的攻击方式中　属于被动攻击的是____C___。

a. 拒绝服务

b. 物理破坏

c. 口令嗅探

d. 重放

10. 计算机网络安全的目标不包括_A____。

a. 免疫性

b. 不可否认性

c. 完整性

d. 保密性

11. 为了防御网络监听　最常用的方法是___C___。

a. 使用专线传输

b. 无线网

c. 数据加密

d. 采用物理传输　非网络

12. 应用代理防火墙的主要优点是__A__。

a. 安全控制更细化、更灵活

b. 服务对象更广

c. 安全服务的透明性更好

d. 加密强度更高

13. ISO安全体系结构中的对象认证服务　使用___B___完成。

a. 访问控制机制

b. 数字签名机制

c. 加密机制

d. 数据完整性机制

14. 下列关于网络防火墙说法错误的是____D___。

a. 网络防火墙不能防止策略配置不当或错误配置引起的安全威胁

b. 网络防火墙不能解决来自内部网络的攻击和安全问题

c. 网络防火墙不能防止本身安全漏洞的威胁

d. 网络防火墙能防止受病毒感染的文件的传输

15. 不属于计算机病毒防治的策略的是___C____。

a. 新购置的计算机软件也要进行病毒检测

b. 及时、可靠升级反病毒产品

c. 整理磁盘

d. 确认您手头常备一张真正 干净 的引导盘

16. ___B___情景属于审计　Audit　。

a. 用户在网络上共享了自己编写的一份 Office 文档　并设定哪些用户可以阅读　哪些用户可以修改

b. 某个人尝试登录到你的计算机中　但是口令输入的不对　系统提示口令错误　并将

这次失败的登录过程纪录在系统日志中　3 c. 用户依照系统提示输入用户名和口令

d. 用户使用加密软件对自己编写的 Office 文档进行加密　以阻止其他人得到这份拷贝

后看到文档中的内容

17. ISO 7498-2 从体系结构观点描述了 5 种安全服务　以下不属于这 5 种安全服务的是

___B____。

a. 授权控制

b. 数据报过滤

c. 数据完整性

d. 身份鉴别

18. 计算机病毒的危害性表现____B____。

a. 不影响计算机的运行速度

b. 影响程序的执行　破坏用户数据与程序

c. 能造成计算机器件永久性失效

d. 不影响计算机的运算结果　不必采取措施

19. 信息的完整性包含有信息来源的完整以及信息内容的完整　下列安全措施中能保证信息

来源的完整性是____C___。

a. 认证

b. 加密、访问控制

c. 数字签名、时间戳

d. 预防、检测、跟踪

20. 由计算机及其相关的好配套设备、设施　含网络　构成的　按照一定的应用目标和规则

对信息进行采集加工、存储、传输、检索等处理的人机系统是___C_____。

a. 计算机工作系统

b. 计算机操作系统

c. 计算机信息系统

d. 计算机联机系统

21. 假设使用一种加密算法　它的加密方法很简单　将每一个字母加 5　即 a 加密成 f。这种算法的密钥就是 5　那么它属于　B　　。

a. 分组密码技术

b. 古典密码技术

c. 对称加密技术

d. 公钥加密技术

22. 以下关于计算机病毒的特征说法正确的是　___B____。

a. 计算机病毒只具有传染性　不具有破坏性

b. 破坏性和传染性是计算机病毒的两大主要特征

c. 计算机病毒具有破坏性　不具有传染

d. 计算机病毒只具有破坏性　没有其他特征

23. 下列计算机病毒检测手段中　主要用于检测已知病毒的是____B____。

a. 校验和法

b. 特征代码法

c. 行为监测法

d. 软件模拟法

24. 确保授权用户或者实体对于信息及资源的正常使用不会被异常拒绝　允许其可靠而且及时地访问信息及资源的特性是__A__。　4 a. 可用性

b. 可靠性

c. 完整性

d. 保密性

25. 在被屏蔽的主机体系中　堡垒主机位于___A____中　所有的外部连接都经过滤路由器到它上面去。

a. 内部网络

b. 周边网络

c. 自由连接

d. 外部网络

26. 社会发展三要素是指　物质、能源和__B___。

a. 计算机网络

b. 信息

c. 互联网

d. 数据

27. 网络信息未经授权不能进行改变的特性是__B__。

a. 可用性

b. 完整性

c. 可靠性

d. 保密性

28. 对口令进行安全性管理和使用　最终是为了__A__。

a. 防止攻击者非法获得访问和操作权限

b. 规范用户操作行为

c. 口令不被攻击者非法获得

d. 保证用户帐户的安全性

29. 信息安全问题是一个___D___问题

a. 硬件

b. 软件

c. 综合

d. 系统

30. 数据在存储过程中发生了非法访问行为　这破坏了信息安全的__C__属性。

a. 完整性

b. 不可否认性

c. 保密性

d. 可用性

31. 防火墙能够__D__。

a. 防范恶意的知情者

b. 防备新的网络安全问题

c. 完全防止传送已被病毒感染的软件和文件

d. 防范通过它的恶意连接

32. 编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据

影响计算机使用　并能

自我复制的一组计算机指令或者程序代码是__D_____.。

a. 计算机游戏

b. 计算机系统　5 c. 计算机程序

d. 计算机病毒

33. 以下哪一项不属于入侵检测系统的功能　___A_____。

a. 过滤非法的数据包

b. 监视网络上的通信数据流

c. 提供安全审计报告

d. 捕捉可疑的网络活动

34. Internet 的影响越来越大　人们常把它与报纸、广播、电视等传统

媒体相比较　称之为

___B___。

b. 第四媒体

c. 交互媒体

d. 全新媒体

35. 以下哪一项不在证书数据的组成中__D_____。

a. 有效使用期限

b. 版本信息

c. 签名算法

d. 版权信息

36. 保证用户和进程完成自己的工作而又没有从事其他操作可能

这样能够使失误出错或蓄

意袭击造成的危害降低　这通常被称为__D__。

a. 适度安全原则

b. 分权原则

c. 木桶原则

d. 授权最小化原则

37. ___C___是目前信息处理的主要环境和信息传输的主要载体

a. WAN

b. 信息网络

c. 计算机网络

d. 互联网

在发生灾难时进行恢复。该机制是为了满足信息安全的__C__属性。

a. 不可否认

b. 完整性

c. 可用性

d. 真实性

39. 针对操作系统安全漏洞的蠕虫病毒根治的技术措施是__A__。

a. 安装安全补丁程序

b. 专用病毒查杀工具

c. 防火墙隔离

d. 部署网络入侵检测系统

40. 机房中的三度不包括_C____。

a. 湿度

b. 温度

c. 可控度　　6 d. 洁净度

41. 以下哪一项属于基于主机的入侵检测方式的优势　___A____。

a. 不要求在大量的主机上安装和管理软件

b. 适应交换和加密

c. 具有更好的实时性

d. 监视整个网段的通信

42. 关于双钥密码体制的正确描述是____A___。

从一个很难计算出另一个

b. 双钥密码体制中加密密钥与解密密钥相同　或是实质上等同

c. 双钥密码体制中加解密密钥虽不相同　但是可以从一个推导出另一个

d. 双钥密码体制中加解密密钥是否相同可以根据用户要求决定

43. 统计数据表明　网络和信息系统最大的人为安全威胁来自于__A___。

a. 内部人员

b. 互联网黑客

c. 第三方人

d. 恶意竞争对手

44. 关于审计跟踪技术的描述　___B____是错误的。

a. 操作系统必须能生成、维护和保护审计过程。

b. 所有用户都能开启和关闭审计跟踪服务。

c. 审计过程一般是一个独立的过程　它应与系统其他功能隔离开。

d. 好的审计跟踪系统可以进行实时监控和报警。

45. PKI是__A__。

a. Public Key lnstitute

b. Private Key lnfrastructure

c. Public Key lnfrastructure

d. Private Key lnstitute

46. 计算机病毒的结构不包括____A_____部分。

b. 激发部分

c. 传染部

d. 引导部分

47. __D__是最常用的公钥密码算法。

a. DSA

b. 椭圆曲线

c. 量子密码

d. RSA

48. 向有限的空间输入超长的字符串是一种__B____攻击手段。

a. 拒绝服务

b. 缓冲区溢出

c. IP欺骗

d. 网络监

49. 20世纪70年代后期　特别是进入90年代以来　美国、德国、英国、加拿大、澳大利亚、法国等西方发达国家为了解决计算机系统及产品的安全评估问题　纷纷制订并实施了一系列安全标准。如　美国国防部制订的 彩虹 系列标准　其中最具影响力的是 可信计算机 7 系统标准评估准则　简称 TCSEC　__B___

a. 白皮书

c. 黄皮书

d. 黑皮书

50. 包过滤的基本思想是　对所接收的每个数据包进行检查　根据__A_____　然后决定转

发或者丢弃该包

a. 过滤规则

b. 用户需要

c. 安全策略

d. 数据流向

51. 黑客在程序中设置了后门　这体现了黑客的___C_____目的。

a. 利用有关资源

b. 窃取信息

c. 非法获取系统的访问权限

d. 篡改数据

52. 使网络服务器中充斥着大量要求回复的信息　消耗带宽　导致

网络或系统停止正常服务

这属于___C__攻击类型。

a. BIND漏洞

b. 远程过程调用

c. 拒绝服务

d. 文件共享

其基本特征是___B____。

a. 文件长度变短

b. 文件长度加长

c. 文件照常能执行

d. 文件不能被执行

54. 以下方法中　不适用于检测计算机病毒的是___D____

a. 软件模拟法

b. 特征代码法

c. 校验和法

d. 加密

55. 以下哪项技术不属于预防病毒技术的范畴____A___。

a. 加密可执行程序

b. 校验文件

c. 引导区保护

d. 系统监控与读写控制

56. 我国正式公布了电子签名法　数字签名机制用于实现__A__需求。

a. 不可抵赖性

b. 保密性

c. 完整性

d. 可用性

57. 关于 A 类机房应符合的要求　以下选项不正确的是___C_____。

a. 供电电源设备的容量应具有一定的余量　8 b. .计算站应设专用

可靠的供电线路

c. 计算机系统应选用铜芯电缆

d. 计算站场地宜采用开放式蓄电池

58. ____D___功能属于操作系统中的日志记录功能。

a. 以合理的方式处理错误事件　而不至于影响其他程序的正常运行

b. 保护系统程序和作业　禁止不合要求的对程序和数据的访问

c. 控制用户的作业排序和运行

d. 对计算机用户访问系统和资源的情况进行记录

59. 关于安全审计目的描述错误的是__A__。

a. 实现对安全事件的应急响应

b. 识别和分析未经授权的动作或攻击

c. 将动作归结到为其负责的实体

d. 记录用户活动和系统管理

60. PKI所管理的基本元素是_B___。

a. 用户身份

b. 数字证书

c. 数字签名

d. 密钥

61. 拒绝服务攻击造成的后果是___D___。

a. 硬盘被格式化

b. 硬件损坏

c. 文件被删除