江苏省青少年网络信息安全知识竞赛试题

（中学组C）

参赛须知：

一、答题方法：本卷共100题,每题有ABCD四个答案，其中只有一个正确答案，请在答题卡上将你认为正确的选项涂黑。答题卡不得涂改，复印无效。试卷满分100分,每题1分。

二、参赛者须按规定在答题卡上填写姓名、班级、学校等信息。要求字迹清晰，填写项目完整，否则视为无效答题卡。

1、关于维基解密的说法错误的是（ ）

A．维基解密网站成立于2006年12月

B．是一个国际性非盈利媒体组织

C．专门公开来自匿名来源和网络泄露的文件

D．通过泄露私密文件来获取利润

2、熊猫烧香病毒是哪一类病毒（ ）

A. 蠕虫病毒

B. 脚本病毒

C. 木马病毒

D. 引导区病毒

3、关于如何预防熊猫烧香病毒，以下说法正确的是（ ）

A. 安装杀毒软件

B. 升级系统

C. 安装补丁

D. 以上说法都不对

4、“心脏出血”漏洞是以下哪个协议存在的安全漏洞（ ）

A. SSL

B. OPENSSL

C. HTTPS

D. FTP

5、受Bash漏洞影响的操作系统不包括（ ）

A. redhat

B. ubuntu

C. mac os

D. windows xp

6、微软结束对Windows XP的支持服务，以下哪项是最好的应对措施（ ）

A. 安装360安全卫士

B. 开启自动更新功能

C. 升级系统至Windows 7

D. 设置开机密码

7、黑帽子（ ）

A. 获得国际资质的黑客

B. 没有获得国际资质的骇客

C. 没有获得国际资质的高级程序员

D. 放弃道德信念而恶意攻击的黑客

8、下列哪种病毒能对计算机硬件产生破坏？（ ）

A．CIH

B．CODE RED

C．维金

D．熊猫烧香

9、计算机病毒的特点不包括（ ）

A．传染性

B．可移植性

C．破坏性

D．可触发性

10、不属于计算机病毒防治的策略的是（ ）

A．确认您手头常备一张真正“干净”的引导盘

B．及时、可靠升级反病毒产品

C．新购置的计算机软件也要进行病毒检测

D．整理磁盘

11、不属于预防病毒感染的方法是\_\_

A. 通过IE中的工具-〉Windows Update升级安装补丁程序

B. 定期升级杀毒软件

C. 不使用电子邮件

D. 将MS Word的安全级别设置为中级以上

12、计算机病毒在一定环境和条件下激活发作,该激活发作是指（ D ）。

A. 程序复制 B. 程序移动 C. 病毒繁殖 D. 程序运行

13、我国将计算机软件的知识产权列入（ ）权保护范畴。

A. 专利 B．技术 C．合同 D．著作

14、说法不正确的是\_\_\_\_\_\_\_。B

A. 计算机病毒程序可以通过链接到Word的宏命令上去执行

B. 计算机病毒程序可以链接到数据库文件上去执行

C. 木马程序可以通过打开一个图片文件去传播

D. 计算机病毒程序可以链接到可执行文件上去执行

15、在进行杀毒时应注意的事项不包括\_\_\_\_\_.

A. 在对系统进行杀毒之前，先备份重要的数据文件

B. 在对系统进行杀毒之前，先断开所有的I/O设备

C. 在对系统进行杀毒之前，先断开网络

D. 杀完毒后，应及时打补丁

16、计算机病毒不可能存在于\_\_\_\_\_\_。

A. 电子邮件

B. 应用程序

C. Word文档

D. 运算器中

17、下面专门用来防病毒的软件是\_\_\_\_\_.

A. 瑞星

B. 天网防火墙

C. Debug

D. 整理磁盘

18、以下不是感染计算机木马后的症状（ ）

A．系统中开放了不明端口

B．系统中有不明来源的进程在执行

C．系统文件被篡改

D．系统注册表添加了启动项

19、哪一项不是特洛伊木马所窃取的信息？

A．计算机名字

B．硬件信息

C．QQ用户密码

D．系统文件

20、关于蠕虫以下哪种说法正确（ ）

A.  具有寄生性

B.  主要攻击本地文件

C.  利用系统存在的漏洞传染

D.  由计算机使用者触发其运行

21、为什么说蠕虫是独立式的？

A．蠕虫不进行复制

B．蠕虫不向其他计算机进行传播

C．蠕虫不需要宿主计算机传播

D．蠕虫不携带有效负载

22、关于计算机领域的后门，错误的是（ ）

A. 有可能是开发人员预留的

B. 可能是系统设计的漏洞

C. 黑客发现后门可以利用它自由进出

D. 后门是开发人员特地预留给用户的

23、肉鸡交易已经形成了黑色产业链，以下不是其中原因的是（ ）

A. 很多人愿意成为黑客攻击的打手

B. 肉鸡的需求非常旺盛

C. 捕获肉鸡的门槛很低

D. 普通网民防范措施不够

24、哪一项不是蠕虫病毒的传播方式及特性。

A．通过电子邮件进行传播

B．通过光盘、软盘等介质进行传播

C．通过共享文件进行传播

D．不需要在用户的参与下进行传播

25、摆渡攻击的主要目的是？（ ）

A. 间接从内部网络中窃取文件资料

B. 从外部直接破坏内部网络

C. 从内部直接破坏外部网络

D. 以上都不对

26、向有限的空间输入超长的字符串是哪一种攻击手段？（ ）

A. 拒绝服务 B. 网络监听 C. 缓冲区溢出 D. IP欺骗

27、许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么？（ ）

A. 安装防火墙

B. 给系统安装最新的补丁

C. 安装入侵检测系统

D. 安装防病毒软件

28、以下（ ）不属于APT攻击的特点

A.  潜伏性

B. 传染性

C.  社会工程性

D.  针对性

29、关于零日漏洞以下哪种说法不正确（ ）

A.  漏洞长期存在

B.  已经修复部分漏洞

C.  漏洞比较脆弱

D.  以上全部

30、以下可以防止拖库的方法是（ ）

A. 分级管理密码，重要帐号单独管理

B. 定期修改密码

C. 不让电脑自动“保存密码”

D. 以上全部

31、下面哪项是网络钓鱼常用手段（ ）

A.  利用假冒网上银行、网上证券网站

B.  利用虚假的电子商务网站

C.  利用垃圾邮件

D.  以上全部

32、网络钓鱼主要是利用（ ）达到目的。

A. 黑客利用人们贪小便宜的心理

B. 黑客利用普通网民缺乏安全防范意识

C. 黑客利用普通网民缺乏对网站真假鉴别的能力

D. 以上都对

33、在我国，构建假冒热点是违反（ ）的行为。

A. 道德

B. 行政管理

C. 法律

D. 以上都不对

34、以下（ ）方式阅读电子邮件不能防止电子邮件中的恶意代码。

A．会话

B．网页

C．程序

D．以上全部

35、计算机信息安全属性不包括\_\_A\_\_。

A. 语意正确性

B. 完整性

C. 可用性服务和可审性

D. 保密性

36、下列情况中，破坏了数据的完整性的攻击是\_\_\_\_\_\_\_。

A. 假冒他人地址发送数据

B. 不承认做过信息的递交行为

C. 数据在传输中途被篡改

D. 数据在传输中途被窃听

37、安全保障阶段中将信息安全体系归结为四个主要环节，下列\_\_\_\_是正确的。

A.  策略、保护、响应、恢复           B. 加密、认证、保护、检测

C.  策略、网络攻防、密码学、备份           D. 保护、检测、响应、恢复

38、下面哪一项最好地描述了风险分析的目的？

A. 识别用于保护资产的责任义务和规章制度

B. 识别资产以及保护资产所使用的技术控制措施

C. 识别资产、脆弱性并计算潜在的风险

D. 识别同责任义务有直接关系的威胁

39、在信息系统安全中，风险由以下哪两种因素共同构成的？ C

A．攻击和脆弱性

B．威胁和攻击

C．威胁和脆弱性

D．威胁和破坏

40、下列对“信息安全风险”的描述正确的是：

A．是来自外部的威胁利用了系统自身存在的脆弱性作用于资产形成风险

B．是系统自身存在的威胁利用了来自外部的脆弱性作用于资产形成风险

C．是来自外部的威胁利用了系统自身存在的脆弱性作用于网络形成风险

D．是系统自身存在的威胁利用了来自外部的脆弱性作用于网络形成风险

41、关于资产价值的评估，\_\_\_\_说法是正确的。

A.  资产的价值指采购费用

B.  资产的价值无法估计

C. 资产价值的定量评估要比定性评估简单容易

D.  资产的价值与其重要性密切相关

42、根据定量风险评估的方法，下列表达式正确的是\_\_\_\_。

A.  SLE=AV x EF           B.  ALE=AV x EF           C.  ALE=SLE x EF           D.  ALE=SLE x AV

43、TCSEC的中文全称是什么

A. 《计算机安全评估准则》

B. 《可信计算机系统评估准则》即橘皮书

C. 计算机防火墙标准

44、GB l7859借鉴了TCSEC标准，这个TCSEC是\_\_\_\_国家标准。

A. 英国           B. . 意大利           C.  美国           D.  俄罗斯

45、在公钥密码体系中，不可以公开的是 C

A．公钥

B．公钥和加密算法

C．私钥

D．私钥和加密算法

46、数字签名通常使用（ ）方式

A. 私钥对数据进行加密

B. 私钥对数字摘要进行加密

C. 公钥对数据进行加密

D. 公钥对数字摘要进行加密

47、关于散列函数的说法不正确的是（ ）

A. 下载软件的用户可以利用散列值验证软件的正确性

B. 散列函数是绝对安全的

C. 用户可以利用散列值检查文件是否染毒

D. 一般数字签名都是利用私钥对数据的散列值进行计算

48、香农提出的密码思想核心是（ ）

A. 扩散

B. 扩展

C. 扩张

D. 扩大

49、加密的优秀算法不包括（ ）

A. MARS

B. RC6

C. CAST256

D. GPS

50、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？

A. 对称的公钥算法

B. 非对称私钥算法

C. 对称密钥算法

D. 非对称密钥算法

51、数字证书将用户与（ ）相联系。

A. 私钥

B. 公钥

C. 护照

D. 驾照

52、RA( )签发数字证书。

A. 可以

B. 不必

C. 必须

D. 不能

53、（ ）可以签发数字证书。

A. CA

B. 政府

C. 店主

D. 银行

54、CA使用( )签发数字证书。

A. 用户的公钥

B. 用户的私钥

C. 自己的公钥

D. 自己的私钥

55、X.509证书不包含以下哪个信息（ ）。

A. 序列号

B. 算法表示

C. 发行机构名称

D. 密钥

56、PKI模型中，不包括哪个部件？（ ）。

A. PKI用户

B. CA

C. 机构

D. 资料库

57、PKI中，哪些信息不能公开？（ ）。

A. 最新的CRL

B. 过期的订户证书

C. 交叉证书

D. 订户的私钥

58、\_\_\_最好地描述了数字证书。

A.  等同于在网络上证明个人和公司身份的身份证

B.  浏览器的一标准特性，它使得黑客不能得知用户的身份

C. 网站要求用户使用用户名和密码登陆的安全机制

D. 伴随在线交易证明购买的收据

59、以下哪个算法不是散列函数（ ）。

A．SHA-256

B．MD4

C．SM3

D．MD6

60、作为最安全，你会否考虑下列哪一项？

A. 密码

B. 一次性密码

C. 登录短语

D. 登录 ID

61、下列哪些措施可以增加穷举攻击的成本？

A. 增加口令的使用年限

B. 增加口令的长度

C. 增加口令的使用历史

D. 以上都不对

62、身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（ ）。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

63、（ ）以密码理论为基础，证实主体的真实身份与其所声称的身份是否相符的技术。

A. 数字签名

B. 消息摘要

C. 身份认证

D. 数据加密

64、防火墙用于将Internet和内部网络隔离，（ ）。

A. 是防止Internet火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

1. 防火墙会过滤传入的流量，其根据是

A. 数据包组成

B. 安全策略

C. 状态数据包规则

D. 安全过程

66、在保护组织的内部网络的同时，以下哪个数据包不应被防火墙丢弃？

A. 入站数据包的源路由选项集

B.  路由器信息交换协议

C. 入站数据包与内部来源 IP 地址

D. 出站数据包与外部目标 IP 地址

67、防止盗用ip行为是利用防火墙的（ ）功能？

A. 防御攻击的功能

B. 访问控制功能

C. IP和 MAC地址绑定功能

D. URL过滤功能

68、如果内部网络的地址段为192.168.1.0、24，需要用到防火墙的（ ）功能，才能使用户上网？

A. 地址映射

B. 地址转换

C. IP和 MAC地址绑定功能

D. URL过滤功能

69、防火墙是一种（ ）技术，是在内部网络和不安全的网络之间设置障碍，阻止对信息资源的非法访问 A

A. 访问控制

B. 信息管理

C. 病毒防御

D. 主动防御

70、有些攻击比如smurf攻击，会使用ip欺骗和icmp回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务，管理员可以在源站点使用的解决办法是？（ ）

A. 通过使用防火墙阻止这些分组进入自己的网络

B. 关闭这些分组的url链接

C. 使用防火墙的包过滤功能，保证网络中的所有传输信息都具有合法的源地址

D. 安装可清除客户端木马程序的防病毒软件模块

71、使用漏洞库匹配的扫描方法，能发现\_\_\_\_。

A. 未知的漏洞

B. 已知的漏洞

C. 自行设计的软件中的漏洞

D. 所有漏洞

72、访问控制模型使资源的所有者可以指定哪些科目可以访问特定的资源?

A. 自主访问控制

B. 强制访问控制

C. 敏感的访问控制

D. 基于角色的访问控制

73、BLP 模型定义访问权限是通过：

A. 筛选规则

B. 安全标签

C. 访问控制矩阵

D. 配置文件

74、（ ）定义成一张表，描述主体对客体的访问权限？

A.  容量表

B.  访问控制列表

C.  访问控制矩阵

D.  能力表

75、访问控制模型是什么？

A. 正式描述访问控制 ID 规范。

B. 正式安全策略的说明。

C. 正式描述敏感标签。

D. 没有任何选择。

76、下列描述不正确的是（ ）

A. 访问控制列表能决定数据是否可以到达某处

B. 访问控制列表可以用来定义某些过滤器

C. 一旦定义了访问控制列表，则其所规范的某些数据包就会严格被允许或拒绝

D. 访问控制列表可以用于路由更新的过程中

77、以下情况可以使用访问控制列表，描述正确的是（ ）

A. 禁止有CIH病毒的文件到我的主机

B. 只允许系统管理员可以访问我的主机

C. 禁止所有使用telnet 的用户访问我的主机

D. 禁止使用unix系统的用户访问我的主机

78、NAT技术将一个IP地址作用于另一个IP地址代替，它在防火墙上的作用是：（ ）

A. 隐藏内部网络地址，保证内部主机信息不泄露

B. 由于ip地址匮乏而使用无效的ip地址

C. 使外网攻击者不能攻击到内网主机

D. 使内网主机受网络安全管理规则的限制

79、下面入侵检测技术当中，哪一种是基于模式匹配技术的（ ）

A. 异常检测 B. 误用检测

C. 基于统计的检测 D. 基于数据挖掘的检测

80、为了简化管理，通常对访问者（ ），以避免访问控制表过于庞大。

A. 分类组织成组

B. 严格限制数量

C. 按访问时间排序，删除长期没有访问的用户

D. 不作任何限制

81、下面哪个操作可以使访问控制列表真正生效（ ）

A. 访问控制列表应用到接口上

B. 定义扩展访问控制列表

C. 定义多条访问控制列表的组合

D. 用ACCEE-LIST命令配置访问控制列表

82、在配置访问控制列表的规则时，关键字any代表的通配符掩码是（ ）

A. 0.0.0.0

B. 所使用的子网掩码的反码

C. 255.255.255.255

D. 无此命令关键字

83、下列对于基于角色的访问控制模型的说法错误的是？

A. 它将若干特定的用户集合与权限联系在一起

B. 角色一般可以按照部门、岗位、工种等与实际业务紧密相关的类别来划分

C. 因为角色的变动往往远远低于个体的变动，所以基于角色的访问控制维护起来比较便利

D. 对于数据库系统的适应性不强，是其在实际使用中的主要弱点

84、什么访问权限控制方法便于数据权限的频繁更改？

A. 基于角色 B. 基于列表

C. 基于规则 D. 基于票证

85、软件开发的”收官之战”是（ ）

A. 测试

B. 设计

C. 开发

D. 需求

86、设置蜜罐管理员需要注意的问题，以下错误说法的是（ ）

A．涉陷技术

B．病毒攻击

C．隐私

D、责任

87、设置蜜罐管理员需要注意的问题，以下错误说法的是（ ）

A．涉陷技术

B．病毒攻击

C．隐私

D、责任

88、保证发送的消息是收到的消息，该消息不是有意或无意改变的是？

A. 完整性

B. 保密

C. 可用性

D. 身份

89、对于密码分析防范，错误的是？ A

A. 增加密钥保留时间。

B. 设计强壮的密码算法。

C. 增加密钥的长度。

D. 注意密钥的分发与存储。

90、以下关于无线网络相对于有线网络的优势不正确的是（ ）。

A. 可扩展性好

B. 灵活度高

C. 维护费用低

D. 安全性更高

91、从安全属性对各种网络攻击进行分类，截获攻击是针对（ ）的攻击。

A. 机密性 B. 可用性

C. 完整性 D. 真实性

92、WLAN主要适合应用在以下哪些场合？（ ）

A. 难以使用传统的布线网络的场所

B. 使用无线网络成本比较低的场所

C. 人员流动性大的场所

D. 以上都是

93、 IP地址不用于什么设备？（ ）

A. 网络设备

B. 网络上的服务器

C. 移动硬盘

D. 上网的计算机

94、哪个不是统一资源定位符中常用的协议？（ ）

A. http

B. https

C. ftp

D. ddos

95、下列关于ADSL拨号攻击的说法，正确的是（ ）。

A. 能用ADSL设备打电话进行骚扰

B. 能损坏ADSL物理设备

C. 能用ADSL设备免费打电话

D. 能获取ADSL设备的系统管理密码

96、无线局域网的覆盖半径大约是（ ）。

A. 10m~100m

B. 5m~50m

C. 15m~150m

D. 8m~80m

97、通过寻找目标的安全漏洞，盗窃存放系统口令的文件，破译加密的口令，是哪种对策（ ）

A. 直接破解系统口令文件

B. 网络嗅探

C. 键盘记录

D. 中间人攻击

98、哪个不是国内著名的互联网内容提供商？（ ）

A. 百度

B. 网易

C. 新浪

D. 谷歌

99、以下关于盗版软件的说法，错误的是（ ）。

A. 若出现问题可以找开发商负责赔偿损失

B. 使用盗版软件是违法的

C. 成为计算机病毒的重要来源和传播途径之一

D. 可能会包含不健康的内容

100、恶意代码传播速度最快、最广的途径是（ ）。

A. 安装系统软件时

B. 通过U盘复制来传播文件时

C. 通过光盘复制来传播文件时

D. 通过网络来传播文件时

答案：

DAABD CDABD

CDDBB DACDC

CDABD CBBCD

DDDAA CDCCA

DABCC BBADC

BAADD CDADB

BBCBB DCBAC

BACCB CCABA

ACDAA BBAAD

ADCDD AADAD