江苏省青少年网络信息安全知识竞赛试题

（中学组B）

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、“维基解密”网站已公布的资料不包括（ ）

A．有关阿富汗战争的文件

B．有关伊拉克战争的文件

C．美国外交部文件

D．有关火山爆发事件

2、“维基解密”网站已公布的资料不包括（ ）

A．有关阿富汗战争的文件

B．有关伊拉克战争的文件

C．有关日蚀月蚀事件

D．美国外交部文件

3、2014年9月苹果iCloud泄密事件，你认为攻击者采用了什么方式进行了攻击（ ）

A. 暴力破解口令

B. 社会工程攻击

C. 病毒

D. 木马

4、如何才能解密被比特币敲诈者CTB-Locker加密的文件（ ）

A. 在规定时间内支付一定数额的比特币作为赎金

B. 安装杀毒软件

C. 安装防火墙

D. 暴力破解

5、对于如何预防比特币敲诈者CTB-Locker，以下说法正确的是（ ）

A. 及时给操作系统打补丁

B. 安装主机监控系统，检测系统资源使用情况

C. 谨慎对待邮件附件，不轻易打开附件

D. 备份重要数据，并本地存储

6、感染熊猫烧香病毒后的症状不正确的是（ ）

A. 可执行的文件图标均变为憨态可掬烧香膜拜的熊猫

B. 出现蓝屏、死机

C. 出现文件破坏、电脑几乎无法使用

D. 运行程序错误

7、2006年底，一种新的蠕虫病毒肆虐互联网，最典型的特征就是计算机在感染该病毒后，所有的可执行文件的图标都变成了“熊猫烧香”的图案，根据资料，若某电脑感染“熊猫烧香”病毒， 以下文件中，图标肯定会变成“熊猫烧香”的是（ ）

A. 风景.jpg

B. index.htm

C. 连连看.exe

D. 课表.xls

1. 以下哪些网站受“心脏出血”漏洞影响（ ）

A. 淘宝

B. 京东

C. 12306

D. 以上都是

9、 Https协议会受到（ ）漏洞的影响

A. bash漏洞

B. 肉鸡

C. 越狱

D. 心脏出血

10、以下说法错误的是（ ）。

A. 苹果操作系统存在Bash漏洞

B. Redhat操作系统存在Bash漏洞

C. Windows操作系统存在Bash漏洞

D. CentOS操作系统存在Bash漏洞

11、“XP靶场”活动每次比赛（ ）小时

A. 12

B. 2

C. 6

D. 24

1. 以下哪项不属于病毒产业链的从业者（ ）

A. 病毒开发者

B. 黑客教师

C. 病毒受害者

D. 利用病毒盗取信息者

13、白帽子（ ）

A. 是道德黑客

B. 获得国际资质的黑客

C. 获得国际资质的骇客

D. 获得国际资质的高级程序员

14、躲在暗处以匿名身份对网络发动攻击或者干脆冒充网络合法用户，侵入网络“行黑”，这类黑客属于：（ ）。

A. 恶作剧型

B. 隐蔽攻击型

C. 定时炸弹型

D. 矛盾制造型

15、按照计算机病毒的定义，下列属于计算机病毒的是（ ）。

A. 某Word 文档携带的宏代码，当打开此文档时宏代码会搜索并感染计算机上所有的 Word 文档

B. 某用户收到来自朋友的邮件附件中隐藏了恶意程序，该恶意程序运行后该用户的主机可以被别人远程控制

C. 某员工在公司内部使用的系统中加入一个逻辑炸弹，如果该员工在一年内被解雇则逻辑炸弹就会破坏系统

D. 黑客入侵了某服务器，并在其上安装了一个后门程序

16、关于计算机病毒，下列说法不正确的是（ ）

A．计算机病毒是一个程序

B．计算机病毒具有传染性

C．计算机病毒的运行不消耗CPU资源

D．病毒并不一定都具有破坏力

17、在下列4 项中，不属于计算机病毒特征的是\_\_\_\_\_\_\_\_。

A． 潜伏性

B．传染性

C．隐蔽性

D．规则性

18、以下哪一项不属于恶意代码？

A. 病毒

B. 蠕虫

C. 宏

D. 特洛伊木马

19、传入我国的第一例计算机病毒是（ ）。

A. 大麻病毒

B. 小球病毒

C. 1575病毒

D. 米开朗基罗病毒

20、发现同事电脑中毒该怎么办（ ）

A.  不关我事，继续办公

B.  协助同事查找问题

C.  及时报告给信息安全人员

D.  用U盘把同事电脑里面资料拷到自己电脑里面

21、下列有关计算机病毒的说法中，（ ）是错误的。

A.  游戏软件常常是计算机病毒的载体

B.   用消毒软件将一片软盘消毒之后，该软盘就没有病毒了

C.   尽量做到专机专用或安装正版软件，是预防计算机病毒的有效措施

D.   计算机病毒在某些条件下被激活之后，才开始起干扰和破坏作用

22、计算机病毒平时潜伏在\_\_\_\_。

A. 内存

B. 外存

C. CPU

D. I/O设备

23、针对计算机病毒的传染性，正确的说法是\_\_\_\_\_\_。

A. 计算机病毒能传染给未感染此类病毒的计算机

B. 计算机病毒能传染给使用该计算机的操作员

C. 计算机病毒也能传染给已感染此类病毒的计算机

D. 计算机病毒不能传染给安装了杀毒软件的计算机

24、以下关于计算机病毒说法正确的是\_\_\_\_\_\_。

A. 计算机病毒只有在发作的时候才能检查出来

B. 只要计算感染了病毒，该病毒会马上发作

C. DOS系统的病毒也可以攻击UNIX

D. 计算机病毒没有文件名

25、下面不可能感染计算机病毒的做法是\_\_\_\_\_\_。

A. 拷贝别人U盘上的一个文件

B. 把自己的一个文件拷贝给别人

C. 把有毒的U盘插入到未开机的计算机

D. 打开了一个陌生人的邮件

26、以下不是杀毒软件的是\_\_\_\_\_。

A. 瑞星

B. 碎片整理

C. 诺顿

D. 卡巴斯基

27、文件型病毒传染的对象主要是以下哪一种文件类型（ ）

1. .DBF B. .WPS C. .COM和.EXE D. .EXE和.DOC

28、有关如何防范木马的说法，正确的是（ ）

A．系统打补丁

B．安装杀毒软件并定期更新

C. 定期备份系统

D．以上都不对

29、木马不具有如下哪个特性？

A. 隐蔽性

B. 自启动性

C. 伪装性

D. 寄生性

30、张三丰同学说他的电脑“中了木马”，经常无缘无故地重启。这里的“木马”这和\_\_\_\_中记载的“木马记”有关联。

A．《吉尔伽美什》

B．《荷马史诗》

C．《哈姆雷特》

D．《圣经》

31、下列木马入侵步骤中，顺序正确的是\_\_\_\_\_\_\_。

A．传播木马-配置木马-运行木马

B．建立连接-配置木马-传播木马

C．配置木马-传播木马-运行木马

D．建立连接-运行木马-信息泄露

32、木马与病毒的最大区别是（ ）

A. 木马不破坏文件，而病毒会破坏文件

B. 木马无法自我复制，而病毒能够自我复制

C. 木马无法使数据丢失，而病毒会使数据丢失

D. 木马不具有潜伏性，而病毒具有潜伏性

33、以下哪个不是蠕虫（ ）

A. 红色代码

B. 熊猫烧香

C. 尼姆亚

D. CIH

34、针对操作系统安全漏洞的蠕虫病毒根治的技术措施是\_\_\_\_。

A.  防火墙隔离

B.  安装安全补丁程序

C.  专用病毒查杀工具

D.  部署网络入侵检测系统

35、以下哪一种方法中，无法防范蠕虫的入侵。（ ）

A. 及时安装操作系统和应用软件补丁程序

B. 将可疑邮件的附件下载等文件夹中，然后再双击打开

C. 设置文件夹选项，显示文件名的扩展名

D. 不要打开扩展名为VBS、SHS、PIF等邮件附件

36、网络后门的功能是（ ）。

A．保持对目标主机长期控制

B．防止管理员密码丢失

C．方便定期维护主机

D．为了防止主机被非法入侵

37、如何弥补漏洞带来的安全威胁（ ）

A. 安装杀毒软件

B. 安装防火墙

C. 及时给系统打补丁

D. 加密

38、为了解救已成为肉鸡的电脑，不可以（ ）

A. 断网

B. 断开鼠标与电脑的连接

C. 查杀病毒和木马

D. 恢复操作系统

39、以下关于DOS攻击的描述，哪句话是正确的？（ ）

A. 不需要侵入受攻击的系统

B. 以窃取目标系统上的机密信息为目的

C. 导致目标系统无法处理正常用户的请求

D. 如果目标系统没有漏洞，远程攻击就不可能成功

40、以下关于DOS攻击的描述，哪句话是正确的？

A.导致目标系统无法处理正常用户的请求

B.如果目标系统没有漏洞，远程攻击就不可能成功

C.以窃取目标系统上的机密信息为目的

D.不需要侵入受攻击的系统

41、关于摆渡攻击的错误的是（ ）

a. 摆渡攻击是百度的一种攻击方式

b. 摆渡攻击是一种专门针对移动存储设备的攻击方式

c. 摆渡攻击就是利用u盘作为“渡船”

d. 摆渡木马隐蔽性、针对性很强，一般只感染特定的计算机

42、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

43、下面哪一项是缓冲溢出的危害？（ ）

A．可能导致shellcode的执行而非法获取权限，破坏系统的保密性

B．执行shellcode后可能进行非法控制，破坏系统的完整性

C．可能导致拒绝服务攻击，破坏系统的可用性

D．以上都是

44、以下（ ）不属于APT攻击的特点

A. 潜伏性

B. 针对性

C. 社会工程性

D. 传染性

45、关于零日漏洞以下哪种说法正确（ ）

A. 漏洞生存时间短

B. 已经修复的漏洞

C. 没有修复的漏洞

D. 漏洞比较脆弱

46、以下哪个不属于社会工程攻击（ ）

A. 免费软件中捆绑流氓插件

B. 中奖短信

C. 免费试听课程

D. 木马

47、以下不属于社会工程学技术的是（ ）

A.个人冒充

B.直接索取

C.钓鱼技术

D.木马攻击

48、以下关于拖库说法不正确的是（ ）

A. 原本是指从数据库中导出数据

B. 现在指网站遭到入侵后，黑客窃取其数据库

C. 拖库与撞库完全不同，没有任何关联

D. 2015年网易邮箱曾发生拖库事件

49、访问网址www.1cbc.com.cn，将可能遭受（ ）

A. 缓冲区溢出攻击

B. 钓鱼攻击

C. SQL注入攻击

D. 拒绝服务攻击

50、在使用公共WIFI时，以下不正确的是（ ）

A. 向WIFI提供方确认正确的WIFI名称和密码

B. 尽量不使用无密码的WIFI

C. 只要WIFI有密码，就可以进行网上银行转账和支付宝付款

D. 不要打开WIFI的自动连接功能

51、以下防范恶意二维码对策中不正确的是（ ）。

A．安装由安全厂商开发的安全二维码软件

B．不随意扫描不明确的二维码

C．可以扫描任意二维码，只要不进行网络支付或转账

D．制定法律政策，加强对二维码的审核、监管、追责等管理

52、以下关于苹果用户越狱的说法不正确的是（ ）

A. 越狱后，苹果不再提供保修服务

B. 越狱后，系统稳定性和安全性能降低

C. 相比越狱后带来的便捷和低费用，降低系统性能是完全可以接受的

D. 破解虽合法，但不意味后续效应不违反所有的法律

53、下列属于垃圾邮件过滤技术的是：

A. 黑名单技术

B. 贝叶斯过滤技术

C. 关键字过滤技术

D. 以上全部

54、以下（ ）方式阅读电子邮件可以防止电子邮件中的恶意代码。

A．纯文本

B．网页

C．程序

D．会话

55、为了防止邮箱邮件爆满而无法正常使用邮箱，您认为应该怎么做（ ）

A.  看完的邮件就立即删除

B.  定期删除邮箱的邮件

C.  定期备份邮件并删除

D.  发送附件时压缩附件

56、以下不属于网络安全特性的是\_\_\_\_\_。

A. 可控性

B. 完整性

C. 保密性

D. 信息的真实性

57、为了满足信息安全的可用性属性，应定期对系统和数据进行（ ），以备在发生灾难时进行恢复。

A. 加密

B. 备份

C. 数字签名

D. 更新

58、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\_\_\_\_。

A.  适度安全原则           B.  授权最小化原则           C.  分权原则           D.  木桶原则

59、在给用户授权时，应当遵循\_\_\_\_原则。

A. 适度          B. 分权           C. 最小化           D. 木桶

60、下列关于定性风险分析的说法中，错误的是（ ）

A. 风险概率分析指调查每项具体风险的发生可能性

B. 风险影响评估旨在分析风险对项目目标的潜在影响

C. 风险影响评估值只包括消极影响或威胁

D. 可以让专家通过召开会议或进行访谈的方式对风险进行评估

61、风险评估不包括以下哪项：

A．资产评估

B．脆弱性评估

C．威胁评估

D．业务稳定性评估

62、风险是丢失需要保护的资产的可能性，风险是（ ）

A. 攻击目标和威胁事件

B. 威胁和漏洞

C. 资产和漏洞

D. 上面3项都不是

63、风险评估的三个要素（ ）

A. 政策，结构和技术

B. 组织，技术和信息

C. 硬件，软件和人

D. 资产，威胁和脆弱性

64、信息网络安全（风险）评估的方法（ ）

A. 定性评估与定量评估相结合

B. 定性评估

C. 定量评估

D. 定点评估

65、关于资产价值的评估，\_\_\_\_说法是不正确的。

A.  资产的价值指采购成本

B.  资产的价值是可以进行估计

C.  资产价值的评估方法有定量评估和定性评估两种

D.  资产的价值与其重要性密切相关

66、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

67、1999年，我国发布第一个信息安全等级保护的国家标准GB17859-1999，提出将信息系统的安全等级划分为（ ）个等级。

A. 7

B. 8

C. 4

D. 5

68、在可信计算机系统评估准则中，计算机系统安全等级要求最低的是（ ）。

A. C 1级

B. D级

C. B 1级

D. A 1级

69、按TCSEC标准，WinNT的安全级别是（ ）。

A、C2 B、B2 C、C3 D、B1

70、对于散列函数的性质正确的是（ ）

A. 变异性

B. 递增性

C. 稳定性

D. 抗冲突性

71、现代密码系统的安全性取决于（ A）

A. 密钥的保护

B. 加密算法的保护

C. 明文的保护

D. 密文的保护

72、des加密的重要操作包括（ ）

A. 扩展置换

B. S盒变换

C. P盒变换

D. 以上全部

73、加密的优秀算法包括（ ）

A. MARS

B. RC6

C. CAST256

D. 以上全部

74、DES是一种block（块）密文的加密算法，是把数据加密成多大的块?

A. 32位;

B. 64位;

C. 128位;

D. 256位

75、关于密钥的安全保护下列说法不正确的是\_\_\_\_\_\_

A．私钥送给CA

B．公钥送给CA

C．密钥加密后存人计算机的文件中

D．定期更换密钥

76、如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的系统为（ ）

A. 常规加密系统

B. 单密钥加密系统

C. 公钥加密系统

D. 对称加密系统

77、公开密钥加密又叫做（ ）

A. 单一密钥

B. 非对称密钥

C. 完整密钥

D. 对称密钥

78、用户的（ ）不能出现在数字证书中。

A. 私钥

B. 公钥

C. 组织名

D. 人名

79、关于CA和数字证书的关系，以下说法不正确的是（ ）。

A．数字证书是保证双方之间的通讯安全的电子信任关系，他由CA签发

B．数字证书一般依靠CA中心的对称密钥机制来实现

C．在电子交易中，数字证书可以用于表明参与方的身份

D．数字证书能以一种不能被假冒的方式证明证书持有人身份

80、（ ）标准定义数字证书结构。

A. X.500

B. TCP/IP

C. ASN.1

D. X.509

81、要解决信任问题，需要使用（ ）。

A. 公钥

B. 自签名证书

C. 数字证书

D. 数字签名

82、关于PKI技术所能解决的问题，以下错误的是（ ）。

A. 通过加密技术来解决信息的保密性问题

B. 通过签名技术来解决信息的不可抵赖问题

C. 能解决信息的完整性不被破坏

D.能提高大并发下的web服务器性能

83、X.509证书不包含以下哪个信息（ ）。

A. 序列号

B. 有效期

C. 版本号

D. 密钥

84、PKI中，哪些信息不能公开？（ ）。

A. 最新的CRL

B. 过期的订户证书

C. CA的公钥

D. 订户的私钥

85、以下说法正确的是（ ）。

A. 证书需要签发者进行数字签名，CRL不需要签发者进行数字签名

B. CA必须公开自己的公钥，用户才能验证其他用户证书的真伪

C. 检查证书撤消状态时，要同时进行OCSP和CRL检查，才是足够安全的

D. IE浏览器不支持PKI

86、关于HASH算法说法不正确的是（ ）。

A．输入的数据长度是固定的

B．固定长度输出

C．单向不可逆

D. HASH算法是一个从明文到密文的不可逆的映射

87、中国哪位学者在美国召开的国际密码会议中报告破译了MD4,MD5?（ ）。

A. 张天云

B. 王小云

C. 李庆

D. 赵冰兴

88、商用加密系统的相对安全性可由什么测量？

A. 由使用该系统的政府机构进行评分。

B. 系统所需的最低加密迭代数。

C. 密钥空间的大小和可用的计算能力。

D. 密码系统中采用的密钥变更方法。

89、下列哪一项不适用于系统生成的密码？

A. 密码不易为用户记住

B. 如果密码生成算法被获取，整个系统将处于危险之中

C. 密码是更容易受到暴力攻击和字典攻击

D. 对于攻击者来说，密码很难猜测

90、基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（ ）。

A. 公钥认证

B. 零知识认证

C. 共享密钥认证

D. 口令认证

91、身份认证中的证书由\_\_\_\_\_\_\_\_\_

A. 政府机构发行

B. 银行发行

C. 企业团体或行业协会发行

D. 认证授权机构发行

92、用于实现身份鉴别的安全机制是（ ）。

A. 加密机制和数字签名机制 B. 加密机制和访问控制机制

C. 数字签名机制和路由控制机制 D. 访问控制机制和路由控制机制

93、关于防火墙的功能，以下哪一种描述是错误的？（ ）

A. 防火墙可以检查进出内部网的通信量

B. 防火墙可以使用应用网关技术在应用层上建立协议过滤和转发功能

C. 防火墙可以使用过滤技术在网络层对数据包进行选择

D. 防火墙可以阻止来自内部的威胁和攻击

94、一般而言，Internet防火墙建立在一个网络的（ ）。

A. 内部子网之间传送信息的中枢

B. 每个子网的内部

C. 内部网络与外部网络的交叉点

D. 部分内部网络与外部网络的结合处

95、防火墙对数据包进行状态检测包过滤，不可以进行过滤的是（ ）？

A. 源和目的IP地址

B. 源和目的端口

C. IP协议号

D. 数据包中的内容

96、防火墙对要保护的服务器做端口映射好处是（ ）？

A. 便于管理

B. 提高防火墙的性能

C. 提高服务器的利用率

D. 隐藏服务器

97、以下说法正确的是（ ）？

A. 防火墙对内部网络起到了很好的保护作用，并且它是坚不可摧的

B. 包过滤防火墙通常工作在osi的三层及三层以上

C. 双重宿主主机体系中，双重宿主主机至少有三个网络接口

D. 包过滤又称为报文过滤，是防火墙最传统最基本的过滤技术

98、某种技术被用来转换对外真正ip地址与局域网内部的ip地址，这种技术是（ ）

A. 地址过滤

B. NAT

C. 反转

D. 认证

99、某种防火墙的缺点是没有办法从细微之处分析数据包，但这种防火墙速度很快，这种技术是（ ）

A. 代理技术

B. 包过滤技术

C. 核检测技术

D. NAT

100、渗透测试步骤不包括（ ）

A. 枚举

B. 脆弱性映射

C. 利用

D. 研究

答案：

DCABC DCDDC

ACAAA CDCBC

BBADC BCADB

CBDBB ACBCA

ACDDC DDCBC

CCAAC DBBCC

DADAA ADBAD

ADDBA CBABD

CDDDB ACCCC

AADCD DDBBD