江苏省青少年网络信息安全知识竞赛试题

（中学组A）

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、Wilileaks是一个（ ）组织

A. 国内安全运营商

B. 国内多平台媒体联合

C. 国际性非营利媒体

D. 国际安全服务商

2、Wikileaks的目的是（ ）

A. 通过公开信息揭露存在暴政的政府和公司的不道德行为，起到监督的作用

B. 致力于维护各行业的运作

C. 致力于公开个人隐私

D. 揭露隐私、丑闻从而获利

3、2014年9月包括珍妮佛.劳伦斯，埃米莉等在内的多名好莱坞女明星不雅照外泄的来源是（ ）

A. 存储照片的硬盘维修时泄露

B. 黑客入侵电脑

C. 苹果云存储服务iCloud泄密

D. 存储在Iphone中的照片泄密

4、2014年9月苹果iCloud泄密事件暴露出服务器系统存在安全漏洞，容易被暴力破解，以下哪种方式不能弥补（A ）

A. 限制非法登陆次数

B. 设置强口令

C. 定期更新口令

D. 升级病毒库版本

5、比特币敲诈者CTB-Locker是一种（ ）

A. 木马

B. 病毒

C. 黑客

D. 以上都不对

1. 以下哪种文件后缀名不容易被比特币敲诈者CTB-Locker感染（ ）。

A. .exe

B. .zip

C. .doc

D. .bob

7、熊猫病毒在哪一年爆发（ ）

A. 2006年

B. 2007年

C. 2008年

D. 2009年

8、出现以下哪种症状说明你的电脑感染了熊猫烧香病毒（ ）

A. 可执行的文件图标均变为憨态可掬烧香膜拜的熊猫

B. word文档图标均变为憨态可掬烧香膜拜的熊猫

C. 程序源代码文件图标均变为憨态可掬烧香膜拜的熊猫

D. 以上都不对

9、主要用于加密机制的协议是（ ）

A. HTTP B. FTP C. TELNET D. SSL

10、 “心脏出血”漏洞的补救措施是（ ）

A. 系统打补丁

B. 更新已失效的X.509安全证书

C. 更换泄露的密钥

D. 以上都是

11、以下（ ）是Bash漏洞的危害。

A. 仅泄露用户敏感数据

B. 取得计算机控制权

C. 仅查看系统文件

D. 仅更改系统配置

12、Bash漏洞会导致以下哪种严重后果（ ）

A. 泄露用户敏感数据

B. 非正常关机

C. 破坏可执行文件

D. 取得计算机控制权

13、1991年海湾战争，美军将病毒注入伊拉克防空系统，这个事件属于（ ）

A. 网络盗窃战

B. 网络舆论战

C. 网络摧毁战

D. 以上都不是

14、xp靶场的主要目的是（ ）

A. 考验国内安全防护软件对windows xp的防护能力

B. 考验windows xp操作系统自身的安全防护能力

C. 为Windows xp安全测试提供靶机

D. 以上都不对

15、前两届 “XP靶场”比赛的主要任务是（ ）。

A. 任选一款安全软件保护的XP系统进行攻击，尝试删除电脑桌面上的一个文本文档

B. 任选一款安全软件保护的XP系统进行攻击，尝试在电脑桌面上新建一个文本文档

C. 任选一款安全软件保护的XP系统进行攻击，尝试盗取电脑桌面上的一个文本文档

D. 以上都不对

16、有关于病毒产业链的说法不正确的是（ ）

A. 在利益驱使下，编写和传播病毒已经演变成一个完整的行业

B. 黑客越来越喜欢炫耀自己的技术

C. 病毒产业链包括制作病毒、传播病毒、盗窃数据、销赃、洗钱等环节

D. 黑客培训也是病毒产业链中的一环

17、黑客hacker源于20世纪60年代末期的（B ）计算机科学中心。

A. 哈佛大学

B. 麻省理工学院

C. 伯克利分校

D. 清华大学

18、骇客cracker是指（ ）

A、比高级程序员能力更强的人

B、比黑客破坏能力稍差一些的人

C、处于恶意目的而破坏软件的人

D、和黑客是一类人

19、进入他人网站，以删除某些文字或图像，篡改网址、主页信息来显示自己的手段高超。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

20、以下不属于计算机病毒特征的是（ ）

A. 破坏性

B. 传染性

C. 潜伏性

D. 自杀性

21、下列关于各类恶意代码说法错误的是：

A. 蠕虫的特点是其可以利用网络进行自行传播和复制

B. 木马可以对远程主机实施控制

C. 病毒具有传染性而木马不具有

D. 所有类型的病毒都只能破坏主机上的各类软件，而无法破坏计算机硬件

22、计算机病毒会对下列计算机服务造成威胁，除了：

A. 完整性

B. 有效性

C. 保密性

D. 可用性

23、下面为预防计算机病毒，正确的做法是\_\_\_\_\_。

A. 一旦计算机染上病毒，立即格式化磁盘

B. 如果是软盘染上病毒，就扔掉该磁盘

C. 一旦计算机染上病毒，则重装系统

D. 尽量用杀毒软件先杀毒，若还不能解决，再想其他办法

24、计算机杀毒时，说法不正确的是\_\_\_\_\_\_。

A. 应及时升级杀毒软件

B. 杀毒前应先对杀毒盘进行杀毒

C. 即使是在Windows系统下杀毒，也应制作一张DOS环境下的杀毒盘

D. 杀完毒后，应及时给系统打上补丁

25、下列四条叙述中，正确的一条是（ ）。

A. 微型计算机一般只具有定点运算功能

B. 微型计算机的内存容量不能超过32MB

C. 微型计算机CPU的主频在使用时是可以随时调整的

D. 不联网的微型计算机也会传染上病毒

26、下面说法正确的是\_\_\_\_。

A. 计算机病毒是计算机硬件设计的失误产生的

B. 计算机病毒是人为制造的

C. 计算机病毒必须清除掉后，计算机才能使用，否则会造成灾难性的后果

D. 计算机病毒是在编程时由于疏忽而造成的软件错误

27、下面能有效预防计算机病毒的方法是\_\_\_\_\_\_。

A. 尽可能地多做磁盘碎片整理

B. 及时升级防病毒软件

C. 尽可能地多做磁盘清理

D. 把重要文件压缩存放

28、下面为预防计算机病毒，正确的做法是\_\_\_\_\_。

A. 一旦计算机染上病毒，立即格式化磁盘

B. 如果是软盘染上病毒，就扔掉该磁盘

C. 一旦计算机染上病毒，则重装系统

D. 尽量用杀毒软件先杀毒，若还不能解决，再想其他办法

29、有关木马和病毒的说法，不正确的是（A ）

A. 木马以偷窃数据为主，而病毒以破坏数据为主

B. 木马和病毒都具有传染性

C. 木马是完整的程序和病毒是程序片段

D. 木马不具有潜伏性，而病毒具有潜伏性

30、以下哪个是计算机木马？（ ）

A. 震网

B. 冰河

C. REDCODE

D. 熊猫烧香

31、下面不属于计算机木马的是\_\_\_\_\_\_\_。

A. 冰河

B. CIH

C. 灰鸽子

D. PKZip

32、下面关于“木马”的说法错误的是\_\_\_\_\_\_\_。

A. “木马”不会主动传播

B. “木马”的传染速度没有病毒传播的快

C. “木马”更多的目的是“偷窃”

D. “木马”有特定的图标

33、Code Red爆发于2001年7月，利用微软的IIS漏洞在Web服务器之间传播。针对这一漏洞，微软早在2001年三月就发布了相关的补丁。如果今天服务器仍然感染Code Red，那么属于哪个阶段的问题?（ ）

A. 微软公司软件的设计阶段的失误 B. 微软公司软件的实现阶段的失误

C. 系统管理员维护阶段的失误 D. 最终用户使用阶段的失误

34、蠕虫和从传统计算机病毒的区别主要体现在（ **B** ）上。

A. 存在形式 B. 传染机制

C. 传染目标 D. 破坏方式

35、应对计算机领域中后门的做法错误的是（ ）。

A. 预留的后门要及时删除

B. 系统及时打补丁或升级

C. 开发人员尽量不要预留后门

D. 系统定期杀毒并更新病毒库

1. 下面对后门特征和行为的描述正确的是（ ）

A. 为计算机系统秘密开启访问入口的程序

B. 大量占用计算机的系统资源，造成计算机瘫痪

C. 对互联网的目标主机进行攻击

D. 寻找电子邮件的地址进行发送垃圾邮件

37、哪一项不是防范漏洞的措施（ ）

A. 使用正版软件

B. 关注信息安全新闻

C. 利用补丁

D. 使用盗版软件

1. “肉鸡”的正确解释是（ ）

A.  比较慢的电脑

B.  被黑客控制的电脑

C.  肉食鸡

D.  烤鸡

39、攻击者用传输数据来冲击网络接口，使服务器过于繁忙以至于不能应答请求的攻击方式是（ ）。

A. 拒绝服务攻击

B. 地址欺骗攻击

C. 会话劫持

D. 信号包探测程序攻击

40、以下关于DOS攻击的描述，哪句话是正确的？（ C ）

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

41、摆渡攻击是（ ）

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. 摆渡攻击就是利用漏洞或后门作为“渡船”

D. 摆渡木马隐蔽性、针对性很强，会感染网络中的所有计算机

42、向有限的空间输入超长的字符串是哪一种攻击手段？（ ）

A. 网络监听 B. 缓冲区溢出 C. 拒绝服务 D. IP欺骗

43、下面哪一项不是缓冲溢出的危害？（ ）

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. 资源过度消耗

44、APT的攻击目标一般包括（ ）

A. 能源

B. 金融

C. 政府

D. 以上全部

45、对于零日攻击正确的是（ ）

A. 零日攻击几乎攻无不克

B. 零日攻击越来越常见

C. 零日攻击可以多次利用

D. 零日漏洞具有间断性

1. 以下哪个于社会工程攻击（ ）

A. 后门

B. 病毒

C. 免费试听课程

D. 木马

47、以下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. 以上全部

48、以下不是拖库事件的是（ D）

A. 2011年的CSDN用户数据泄露事件

B. 2015年的网易邮箱信息泄露事件

C. 2011金山毒霸网站用户数据泄露事件

D. 2014年互联网上流传12306网站用户信息

49、以下不能防止拖库的方法是（D ）

A. 重要帐号单独管理，其他的帐号无所谓

B. 可以电脑允许自动“保存密码”，但定期修改密码

C．分级管理密码，把密码记录在本地磁盘的某个特定的文档中

D. 以上全部

50、QQ中毒是指（ ）。

A. QQ号码被盗号

B. QQ号码中毒

C. QQ服务器中毒

D. 安装QQ程序的电脑中毒

51、在windows操作系统的（ ）模式下，病毒无法发作和传播。

A. 安全

B. 网络

C. 离线

D. 命令

52.下面哪项不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. 利用计算机木马

53、防范网络钓鱼，以下说法不正确的是（ ）

A. 仔细查看网站域名是否正确

B. 微信、QQ、邮件中的链接要谨慎点击，短信中的链接都是安全的

C. 钓鱼网站的链接多数不可用

D. 钓鱼网站的配色、内容等制作比较粗糙

54、用户使用无密码的公共WIFI过程中，黑客利用一定的软件系统和技术可以获得（ D ）信息。

A. 用户使用的终端和应用

B. 用户发送的即时通信消息

C. 用户浏览的网页和登录的账户信息

D. 以上全部

55、恶意二维码容易在以下哪种场合出现（ ）。

A. 信息获取

B. 广告推送

C. 优惠促销

D. 网络支付

E. 以上全部

56、以下哪项是从源头防止手机病毒和木马（ ）。

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

57、以下哪项操作可能会威胁到智能手机的安全性（ ）

A、越狱

B、Root

C、安装盗版软件

D、以上都是

58、手机越狱带来的负面影响包括（ ）

A. 可能安装恶意应用，威胁用户的数据安全

B. 设备稳定性下降

C. 设备性能下降

D. 以上都是

59、下列不属于垃圾邮件过滤技术的是：A

A. 软件模拟技术

B. 贝叶斯过滤技术

C. 关键字过滤技术

D. 黑名单技术

60、为了防止电子邮件中的恶意代码，应该用（ ）  方式阅读电子邮件。

A. 纯文本

B. 网页

C. 程序

D. 会话

61、以下措施对降低垃圾数量没有帮助的是（ ）。

A. 举报收到垃圾

B. 使用垃圾邮件筛选器

C. 安装邮件分发系统

D. 谨慎共享电子邮件地址

62、 可以从哪些方面增强接收邮件的安全性（ ）

A. 不断优化垃圾邮件设置、查看邮件数字签名，确认发件人信息、定期更新防病毒软件

B. 不断优化垃圾邮件设置、查看邮件数字签名，确认发件人信息、定期更新防病毒软件、邮件传输加密

C.  查看邮件数字签名，确认发件人信息、定期更新防病毒软件、邮件传输加密

D. 全部不是

63、信息安全的属性不包括\_\_\_\_。

A. 保密性

B. 可用性

C. 可控性

D. 合理性

64、得到授权的实体需要时就能得到资源和获得相应的服务，这一属性指的是\_\_\_\_。B

A. 保密性

B. 可用性

C. 完整性

D. 可靠性

65、下列情况中，破坏了数据的保密性的攻击是\_\_\_\_\_\_。

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

66、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

67、风险评估包括以下哪些部分：

A．资产评估

B．脆弱性评估

C．威胁评估

D．以上都是

68、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

69、下列关于风险的说法，\_\_\_\_是错误的。

A.  风险是客观存在的

B.  导致风险的外因是普遍存在的安全威胁

C.  导致风险的外因是普遍存在的安全脆弱性

D.  风险是指一种可能性

70、 风险管理的任务包括\_\_\_\_。

A. 风险识别和评估           B. 风险控制和转移

C. 接受风险           D. 以上全部

71、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由两个定级要素决定，两个要素分别是受侵害的客体和（ ）。

A. 客体的脆弱性

B. 客体业务存在的风险

C. 客体业务信息安全

D. 对客体造成侵害的程度

72、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高的是（ ）。

A. C 1级

B. D级

C. B 1级

D. A 1级

73、橘皮书主要是针对（ ）

A. 操作系统

B. 数据库

C. 信息系统

D. web应用

74、在公钥密码体系中，可以公开的是（ ）

A．密钥对

B．公钥和加密算法

C．私钥

D．私钥和加密算法

75、在加密技术中，把密文变为明文的过程称为\_\_\_\_\_\_。

A. 明文

B. 密文

C. 加密

D. 解密

答案：D

76、最著名的对称密码是（A ）

A. 数据加密标准DES

B. 解密标准

C. 数据标准

D. 加速标准

77、数据加密标准DES采用的密码类型是（ B ）。

A. 序列密码

B. 分组密码

C. 散列码

D. 随机码

1. 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不同的密钥？

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

79、甲和乙采用公钥密码体制对数据文件进行加密传送，甲用乙的公钥加密数据文件，乙使用（ ）来对数据文件进行解密。

A. 甲的公钥

B. 甲的私钥

C. 乙的公钥

D. 乙的私钥

80、公钥密码思想以什么为基础的的（ ）

A. 单向陷门函数

B. 双向陷门函数

C. 单向平门函数

D. 双向平门函数

81、数据保密性安全服务的基础是（ ）。

A. 数据完整性机制 B. 数字签名机制

C. 访问控制机制 D. 加密机制

82、证书授权中心（CA）的主要职责是（ ）。

A. 颁发和管理数字证书以及进行用户身份认证

B. 进行用户身份认证

C. 以上答案都不对

D. 颁发和管理数字证书

83、 PKI体系不包括（ ）。

A. CA

B. KM

C. RA

D. DB

84、哪些证书的序列号应出现在CRL上（ ）。

A. 有效期内的正常证书

B. 过期的证书

C. 尚未生效的证书

D. 相应私钥泄漏的，有效期内的CA证书

85、以下说法正确的是（ ）。

A. 用户要将自己的私钥和公钥都同时交给CA，CA才能签发数字证书

B. 用户证书对应的密钥对，只能由用户自己来生成

C. 按照证书主题的不同，可以将数字证书分为2种：CA证书和用户证书

D. 按照目前的计算机处理能力，256 bit的RSA密钥算法是安全的

86、关于散列函数，叙述不正确的是（ ）。

A. 散列函数具有单向性

B. 输入消息中的任何变动都不会对输出摘要产生影响

C. 散列函数具有抗冲突性

D. 可以防止消息被篡改

1. 针对目标计算机系统执行一次手动尝试和错误攻击获取访问权限，影响此次攻击所需时间的最重要因素是什么？（ ）

A. 口令的密钥空间

B. 攻击者的专业知识

C. 执行该次攻击的系统处理速度

D. 用于口令转换的加密算法

88、可以用来签发证书的介质，以下错误的是（ ） 。

A. 智能卡

B. USB-KEY

C. 微软的CSP容器

D. U盘

89、包过滤型防火墙原理上是基于（ ） 进行分析的技术。

A. 物理层

B. 数据链路层

C. 网络层

D. 应用层

90、关于网络安全，下列哪一项是正确的？（ ）

A. 在当今这个互联世界中，防火墙并不是必要的

B. 在当今这个互联世界中，防火墙是必要的

C. 在当今这个互联世界中，whitewall是必要的

D. 在当今这个互联世界中，black firewall是必要的

91、当用户网络有多个公网出口时，需要用到防火墙的（ ）功能？

A. OSPF

B. H.323

C. DHCP

D. PBR

92、小红的学校申请到5个ip地址，要使学校的20台主机都能连接到互联网上，她需要防火墙的什么功能？（ ）

A. 假冒ip地址的侦测

B. 网络地址转换技术

C. 内容检查技术

D. 基于地址的身份认证

1. 下面说法错误的是\_\_\_\_。

A. 由于基于主机的入侵检测系统可以监视一个主机上发生的全部事件，它们能够检测基于网络的入侵检测系统不能检测的攻击

B. 基于主机的入侵检测可以运行在交换网络中

C. 基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描

D. 基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击，因为应用程序日志并不像操作系统审计追踪日志那样被很好地保护

94、下面入侵检测技术当中，哪一种是基于模式匹配技术的（B ）

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

95、下列对访问控制影响不大的是（ D）。

A. 主体身份

B. 客体身份

C. 访问类型

D. 主体与客体的类型

96、标准的访问控制列表数字标识范围是（ ）。

A.1-50

B. 1-99

C.1-100

D.1-199

97、对于渗透团队，了解测试目标的本质，是哪种测试？（A ）

A. 白盒测试

B. 黑盒测试

C. 灰盒测试

D. 红盒测试

98、以下哪种方法可以使得一个加密密钥更能抵抗穷举攻击？（B ）

A. 没有任何选择。

B. 增加密钥的长度。

C. 增加密钥的时限。

D. 增加密钥保留时间。

1. 超链接欺骗攻击通常成功的原因是（ ）

A. 大多数用户请求 DNS 名称服务而不转向超链接。

B. 攻击者使用审核日志执行用户身份验证。

C. 攻击依赖于服务器软件的修改。

D. 大多数用户不需要连接到 DNS 名称请求，他们转向超链接。

100、 以下哪种口令不属于弱口令（ ）

A. 1.2345678E7

B.  abcdefg

C.  AAAAAAA

D.  qw！bydp00dwz1.

答案：

CACAB DBADD

BDCAA BBCBD

DCDBD BBDAB

BDCBD ADBAC

BBDDA CDDDD

ADBDE ADDAA

CADBD ADCCA

DDABD ABDDA

DADDC BADCB

CBCBD BABDD