江苏省青少年网络信息安全知识竞赛试题

（小学组C卷）

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”网站的说法不正确的是\_\_\_\_\_\_

A、网站办公地址在美国五角大楼

B、网站没有公布办公邮箱

C、网站没有其总部地址

D、网站没有公开办公电话号码

2、关于Wikileaks的说法正确的是\_\_\_\_\_\_

A、是指维基搜索引擎

B、是指维基百科

C、是指“维基解密”网站

D、是国际性营利组织

3、日常生活中，我们可以享受云服务带来的哪些便捷？\_\_\_\_\_\_

A、上传、下载照片

B、备份通讯录

C、协作编辑文档

D、以上全部

4、黑客攻击苹果的\_\_\_\_\_\_，致使全球诸多当红女星的不雅照曝光，云安全问题值得关注。

A、Store

B、Watch

C、iCloud

D、Iphone

5、关于比特币敲诈者的说法不正确的是\_\_\_\_\_\_

A、流行于2015年初

B、受害者只要在规定时间内交纳一定数额的比特币，才可以解开被病毒加密的资料

C、病毒作者波格挈夫来自俄罗斯

D、主要通过网页传播

6、以下哪个后缀名用于重要数据文件，可以用于防范比特币敲诈者\_\_\_\_\_\_

A、.com

B、.zip

C、.doc

D、自定义后缀名

7、以下哪项不是电脑感染熊猫烧香后的特征\_\_\_\_\_\_

A、可执行文件图标均变为憨态可掬烧香膜拜的熊猫

B、蓝屏

C、计算机频繁重启

D、文件被复制

8、关于“心脏出血”漏洞的阐述错误的是\_\_\_\_\_\_

A、通过读取网络服务器内存，攻击者可以访问敏感数据

B、该病毒可使用户心脏出血

C、心脏出血漏洞是“灾难性的”

D、“心脏出血” 漏洞的危险性在于，它要比一般的漏洞潜伏得更深

9、OPENSSL存在什么漏洞\_\_\_\_\_\_

A、缓冲区溢出

B、格式化字符串

C、SQL注入漏洞

D、心脏出血漏洞

10、关于Bash漏洞的了解错误的是\_\_\_\_\_\_

A、Bash漏洞远不如心脏出血严重

B、Bash漏洞能取得用户计算机的控制权

C、Bash漏洞能影响到苹果操作系统和Linux

D、Bash漏洞的使用门槛非常低

1. 下列哪项不是信息化战争的“软打击”\_\_\_\_\_\_

A、精确导弹攻击

B、网络攻击

C、心理攻击

D、媒体攻击

12、第一次“XP靶场”活动于什么时候开展\_\_\_\_\_\_

A、2014年7月

B、2014年12月

C、2015年1月

D、2015年5月

1. xp靶场的打靶对象主要是\_\_\_\_\_\_

A、国内的安全防护软件

B、国际的安全防护软件

C、国内的数据库软件

D、国内的自动化办公软件

14、以下哪项不需要消耗流量\_\_\_\_\_\_

A、在线视频

B、小说下载

C、外挂下载

D、软件离线安装

15、哪一种是黑客中的分类\_\_\_\_\_\_

A、绿钢笔

B、黑鞋子

C、白手套

D、白帽子

16、黑客的主要攻击手段包括\_\_\_\_\_\_

A、社会工程攻击、蛮力攻击和技术攻击

B、人类工程攻击、武力攻击及技术攻击

C、社会工程攻击、系统攻击及技术攻击

17、下列不属于电脑病毒的特征的是\_\_\_\_\_\_

A、突发性

B、破坏性

C、繁殖性和传染性

D、潜伏性

18、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

19、《计算机病毒防治管理办法》是在哪一年颁布的\_\_\_\_\_\_

A、1994 B、1997 C、2000 D、1998

20、当软盘感染病毒，用各种清除病毒软件都不能清除病毒时，则应该对此软盘\_\_\_\_\_\_。

A、丢弃不用

B、删除所有文件

C、进行格式化

D、用酒精擦洗磁盘表面

21、以下关于计算机病毒说法错误的是\_\_\_\_\_\_。

A、计算机病毒没有文件名

B、计算机病毒的发作时有激发条件的，未必一旦感染，立即发作

C、计算机病毒也会破坏Word文档

D、计算机病毒无法破坏压缩文件

22、以下关于计算机病毒的特征说法正确的是\_\_\_\_\_\_。

A、计算机病毒只具有破坏性和传染性，没有其他特征

B、计算机病毒具有隐蔽性和潜伏性

C、计算机病毒具有传染性，但不能衍变

D、计算机病毒都具有寄生性，即所有计算机病毒都不是完整的程序

23、计算机病毒程序\_\_\_\_\_\_\_。

A、通常很大，可能达到几MB字节

B、通常不大，不会超过几十KB字节

C、一定很大，不会少于几十KB字节

D、有时会很大，有时会很小

24、下面，针对360安全卫士软件，说法错误的是\_\_\_\_\_。

A、360安全卫士可以检测出系统是否有漏洞

B、360安全卫士可以在下载时查出下载对象中是否有可疑的木马程序

C、360安全卫士可以通过“清理插件”来提高计算机的运行速度

D、360安全卫士可以自动进行磁盘碎片整理

1. 以下关于计算机病毒说法正确的是\_\_\_\_\_\_

A、计算机病毒是生物病毒在计算机上的变体

B、计算机病毒的某些特征与生物病毒的特征相似

C、计算机病毒也可以感染人类

D、计算机病毒是生物病原体和计算机程序的结合体

26、以下不属于木马检测方法的是\_\_\_\_\_\_。

A、检查端口及连接

B、检查系统进程

C、检查注册表

D、检查文件大小

27、有关木马的说法，正确的是\_\_\_\_\_\_

A、将表面看似正常的程序，实际上却隐含恶意意图的恶意代码

B、能够感染文件使之无法正常访问的恶意代码

C、利用系统漏洞进行传播的恶意代码

D、以上都不对

28、下列对于蠕虫病毒的描述错误的是：\_\_\_\_\_\_

A、蠕虫的传播无需用户操作

B、蠕虫会消耗内存或网络带宽，导致DOS

C、蠕虫的传播需要诱骗用户下载和执行

D、蠕虫程序一般由“传播模块”、“隐藏模块”和“目的功能模块”构成

29、计算机蠕虫是一种特殊的计算机病毒，要想防范计算机蠕虫就需要区别开其与一般的计算机病毒，下面说法正确的是\_\_\_\_\_\_

A、蠕虫不利用文件来寄生

B、蠕虫病毒的危害远远大于一般的计算机病毒

C、二者都是病毒，没有什么区别

D、计算机病毒的危害大于蠕虫病毒

30、关于计算机领域中的后门的说法，正确的是\_\_\_\_\_\_。

A、是系统管理员预留给少数特殊用户的

B、只有系统管理员知道后门的存在

C、可能是程序开发人员预留的

D、以上说法都不正确

31、计算机领域中后门的最主要危害是\_\_\_\_\_\_。

A、利用后门偷窥系统内信息

B、利用后门实施远程控制

C、利用后门注入病毒

D、以上说法都不对

32、关于如何判断电脑是否成为肉鸡，不正确的是凭\_\_\_\_\_\_

A、鼠标操作是否正常

B、系统开关机是否正常

C、电脑设备接口是否正常

D、网络状态是否正常

33、以下不是防范分布式拒绝服务攻击的是\_\_\_\_\_\_

A、关闭不必要的服务

B、定期更新补丁

C、限制每台服务器同时打开的链接数

D、停止下载任何文件

34、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

35、溢出攻击的核心是\_\_\_\_\_\_。

A、修改堆栈记录中进程的返回地址

B、利用Shellcode

C、提升用户进程权限

D、捕捉程序漏洞

36、许多黑客利用软件实现中的缓冲区溢出漏洞进行攻击，对于这一威胁，最可靠的解决方法是\_\_\_\_\_\_

A、安装相关的系统补丁软件

B、安装用户认证系统

C、安装防火墙

D、安装防病毒软件

37、APT的攻击目标一般不是\_\_\_\_\_\_

A、能源

B、金融

C、政府

D、个人

38、摆渡攻击通常不会用以下哪个途径来窃取资料\_\_\_\_\_\_

A、后门

B、U盘

C、移动硬盘”

D、移动载体

39、对于零日漏洞正确的是\_\_\_\_\_\_

A、零日漏洞又名零时差攻击

B、零日漏洞价格昂贵

C、零日漏洞几乎是无敌的

D、以上全部

40、下列避免社会工程攻击方法正确的是\_\_\_\_\_\_

A、小心来路不明的电话、访问或者电子邮件信息

B、不要在电子邮件中泄露个人的或者财务方面的信息

C、在检查某个网站的安全性之前不要在网络上发送机密信息

D、以上全部

41、2014年，互联网上爆出近几十万12306网站的用户信息，12306官方网站称是通过\_\_\_\_\_\_方式泄露的。

A、拖库

B、撞库

C、木马

D、信息明文存储

42、下列哪个不是QQ中毒后的处理办法\_\_\_\_\_\_

A、直接换一个新的QQ号

B、查杀病毒木马

C、检查系统，查看是否有漏洞

D、修改QQ密码

43、访问以下哪个网址将可能遭受钓鱼攻击\_\_\_\_\_\_

A、www.1cbc.com.cn

  B、www.qq.com

C、www.taobao.com

D、www.sina.com

44、以下\_\_\_\_\_\_是防范假冒热点攻击的措施？

A、尽量使用免费WIFI

B、不要打开WIFI的自动连接功能

C、在免费WIFI上购物

D、任何时候不使用WIFI联网

45、乱扫二维码，支付宝的钱被盗，主要是中了\_\_\_\_\_\_

A、僵尸网络

B、病毒

C、木马

D、蠕虫

46、越狱的好处\_\_\_\_\_\_

A、安全性降低

B、手机崩溃

C、稳定性低

D、安装免费软件

47、造成广泛影响的1988年Morris蠕虫事件，就是\_\_\_\_\_\_作为其入侵的最初突破点的。

A、利用操作系统脆弱性

B、利用系统后门

C、利用邮件系统的脆弱性

D、利用缓冲区溢出的脆弱性

48、邮件炸弹攻击是指\_\_\_\_\_\_

A、破坏被攻击者邮件服务器

B、添满被攻击者邮箱

C、破坏被攻击者邮件客户端

D、盗取被攻击者账号密码

49、破坏可用性的网络攻击是\_\_\_\_\_\_。

A、向网站发送大量垃圾信息，使网络超载或瘫痪

B、破译别人的密码

C、入侵者假冒合法用户进行通信

D、窃听

50、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\_\_\_\_\_\_。

A、保密性

B、不可抵赖性

C、可用性

D、可靠性

51、信息安全风险评估报告应当包括哪些？\_\_\_\_\_\_

A、评估范围

B、评估依据

C、评估结论和整改建议

D、以上全部

52、风险是\_\_\_\_\_\_和威胁的综合结果。

A、内部攻击

B、网络攻击

C、漏洞

D、管理不当

53、TCSEC共分为\_\_\_\_\_\_大类\_\_\_\_\_\_级。

A、4 7

B、3 7

C、4 5

D、4 6

54、黑客搭线窃听属于哪一类风险？\_\_\_\_\_\_

A、信息存储安全

B、信息传输安全

C、信息访问安全

D、以上都不正确

55、公钥体系中，用户乙从用户甲接收的数据要用\_\_\_\_\_\_进行解密

A、甲的公钥

B、甲的私钥

C、乙的公钥

D、乙的私钥

56、假设使用一种加密算法，它的加密方法很简单：在26个英文字母范围内，将每一个字母加5，即a加密成f，依次类推。这种算法的密钥就是5，那么用这种加密算法对消息“helloworld”加密后的密文是\_\_\_\_\_\_。

A、mjqqtbtwqi

B、dlrowolleh

C、woeldhello

D、Ollehdleow

57、des加密的三个重要操作不包括\_\_\_\_\_\_

A、扩展置换

B、S盒变换

C、P盒变换

D、随机变换

58、下面哪一项是基于一个大的整数很难分解成两个素数因数？\_\_\_\_\_\_

A、ECC

B、RSA

C、DES

D、Diffie-Hellman

59、除了\_\_\_\_\_\_以外，下列都属于公钥的分配方法。

A、公用目录表

B、公钥管理机构

C、公钥证书

D、秘密传输

1. PKI是指什么\_\_\_\_\_\_

A、公钥基础设施

B、私钥基础设施

C、公钥部分设施

D、公钥高端设施

61、下列哪一项信息不包含在X.509规定的数字证书中？\_\_\_\_\_\_

A、证书有效期

B、证书持有者的公钥

C、证书颁发机构的签名

D、证书颁发机构的私钥

62、证书路径验证的目的是什么？\_\_\_\_\_\_

A、检查证书路径中的证书的合法性。

B、检查证书路径中的所有证书都指同一证书认证。

C、检查被吊销的证书存在外部认证路径。

D、检查证书路径中的名称都是相同的。

63、MD5产生的散列值是多少位？\_\_\_\_\_\_

A、56

B、64

C、128

D、160

64、对散列函数最好的攻击方式是\_\_\_\_\_\_。

A、穷举攻击

B、中间人攻击

C、字典攻击

D、生日攻击

65、以下哪一项鉴别机制不属于强鉴别机制？\_\_\_\_\_\_

A、令牌+口令

B、PIN码+口令

C、签名+指纹

D、签名+口令

66、身份认证的含义是\_\_\_\_。

A、注册一个用户       B、标识一个用户       C、验证一个用户       D、授权一个用户

67、关于防火墙的说法，以下错误的是\_\_\_\_\_\_。

A、防火墙提供可控的过滤网络通信

B、防火墙只允许授权的通信

C、防火墙只能管理内部用户访问外网的权限

D、防火墙可以分为硬件防火墙和软件防火墙

68、在防火墙技术中，内网这一概念通常指的是\_\_\_\_\_\_

A、受信网络

B、非受信网络

C、防火墙内的网络

D、互联网

69、防火墙主要可以分为\_\_\_\_\_\_

A、包过滤型、代理性、混合型

B、包过滤型、系统代理型、应用代理型

C、包过滤型、内容过滤型、混合型

70、误报的英文是\_\_\_\_\_\_

A、False Positives

B、False Negatives

C、Negatives

D、Positives

1. 以下哪一项不属于入侵检测系统的功能：

A、监视网络上的通信数据流

B、捕捉可疑的网络活动

C、提供安全审计报告

D、过滤非法的数据包

72、访问控制技术主要的目的是\_\_\_\_\_\_。

A、控制访问者能否进入指定的网络

B、控制访问系统时访问者的IP地址

C、控制访问者访问系统的时刻

D、谁能访问系统，能访问系统的何种资源以及访问这种资源时所具备的权限

73、信息系统实现访问控制有多种方式，其中以用户为中心建立起的描述访问权限的表格，这种方式指的是\_\_\_\_\_\_。

A、访问控制矩阵

B、访问控制表

C、访问控制能力表

D、授权关系表

74、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

75、渗透了解程度,以下哪个不正确\_\_\_\_\_\_

A、完全了解

B、部分了解

C、零了解

D、精确了解

1. 软件开发周期不包括\_\_\_\_\_\_

A、发布

B、开发

C、分析

D、需求收集

77、\_\_\_\_\_\_是在蜜罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个蜜罐，来构成一个黑客诱捕网络体系架构。

A、蜜网

B、鸟饵

C、鸟巢

D、玻璃鱼缸

78、密码分析的目的是什么？\_\_\_\_\_\_

A、确定加密算法的强度

B、增加加密算法的代替功能

C、减少加密算法的换位功能

D、确定所使用的换位

79、以下哪个不是密码分析的方法\_\_\_\_\_\_

A、穷举

B、拦截攻击

C、分析法

D、边信道攻击

1. 棱镜门的主要曝光了对互联网的什么活动\_\_\_\_\_\_

A、监听

B、看管

C、羁押

D、受贿

81、棱镜门事件的发起者是谁\_\_\_\_\_\_

A、俄罗斯克格勃

B、美国国家安全局

C、英国军情六处

D、中国红客

82、逻辑炸弹和病毒相比，没有什么特点\_\_\_\_\_\_

A、破坏性

B、传染性

C、隐蔽性

D、攻击性

83、Windows 操作系统提供的完成注册表操作的工具是：\_\_\_\_\_\_。

A 、syskey

B 、msconfig

C 、ipconfig

D 、regedit

84、对于新购买的电脑，不建议的行为是：\_\_\_\_\_\_

A、设置开机密码

B、安装QQ软件

C、让电脑公司重装XP系统

D、启用Windows Update

85、以下关于“最小特权”安全管理原则理解正确的是：\_\_\_\_\_\_

A、组织机构内的敏感岗位不能由一个人长期负责

B、对重要的工作进行分解，分配给不同人员完成

C、一个人有且仅有其执行岗位所足够的许可和权限

D、防止员工由一个岗位变动到另一个岗位，累积越来越多的权限

86、\_\_\_\_\_\_属于Web中使用的安全协议。

A、PEM、SSL

B、S-HTTP、S/MIME

C、SSL、S-HTTP

D、S/MIME、SSL

87、网站的安全协议是https时，该网站浏览时会进行\_\_\_\_\_\_处理。

A、增加访问标记

B、身份验证

C、加密

D、口令验证

88、数字签名技术不能解决的安全问题是\_\_\_\_\_\_。

A、第三方冒充

B、接收方篡改

C、信息窃取

D、接收方伪造

89、主要用于加密机制的协议是\_\_\_\_\_\_

A、HTTP

B、FTP

C、TELNET

D、SSL

90、FTP(文件传输协议，File Transfer Protocol，简称FFP)服务、SMTP(简单邮件传输协议，Simple Mail Transfer Protocol，简称SMTP)服务、HTTP(超文本传输协议，Hyper Text Transport Protocol，简称HTTP)、HTTPS(加密并通过安全端口传输的另一种HTTP)服务分别对应的端口是\_\_\_\_。

A 、25 21 80 554 B、 21 25 80 443

C 、21 110 80 554 D、 21 25 443 554

91、下面不能防范电子邮件攻击的是\_\_\_\_\_\_。

A、采用FoxMail

B、采用电子邮件安全加密软件

C、采用Outlook Express

D、安装入侵检测工具

92、全球著名云计算典型应用产品及解决方案中，亚马逊云计算服务名称叫\_\_\_\_\_\_。

A、Google App

B、SCE

C、Azure

D、AWS

93、主要的电子邮件协议有\_\_\_\_\_\_。

A、TCP/IP

B、SMTP、POP3和IMAP4

C、IP、TCP

D、SSL、SET

94、下列哪项不是口令攻击的常用方法\_\_\_\_\_\_

A、随机猜测

B、猜测攻击

C、穷举攻击

D、字典攻击

95、小学生上网设置密码最安全的是\_\_\_\_\_\_

A、跟用户名相同的密码

B、使用生日作为密码

C 、10位的综合型密码

D 、爸爸妈妈的电话号码

1. 网吧不能对哪种人群开放？\_\_\_\_\_\_

　　A、18岁以上

　　B、20岁以上

　　C、18岁以下

D、20岁以下

97、\_\_\_\_\_\_是世界上首个强制推行网络实名制的国家。

A、美国    B、日本    C、韩国    D、德国

98、5月12日，有人出于恶作剧或为提高个人网上空间点击率等目的，编造“北京将有比较强的地震”、 “汶川地震系人为”等谣言，并在在互联网相关贴吧里发帖，造成了不良影响，触犯了有关法律。公安机关对相关造谣人员分别处以治安处罚。这表明\_\_\_\_\_\_。

①公民在网络虚拟世界的行为是不自由的

②公民的自由总是在法律规范内的自由

③公民是现实社会的权利主体，但不是网络世界的权利主体

④公民有使用网络的权利，也有维护网络安全的义务

A、①④

B、②③

C、②④

D、③④

99、下面对计算机“日志”文件，说法错误的是\_\_\_\_\_\_。

A、日志文件通常不是.TXT类型的文件

B、用户可以任意修改日志文件

C、日志文件是由系统管理的

D、系统通常对日志文件有特殊的保护措施

100、恶意代码是\_\_\_\_\_\_。

A、被损坏的程序

B、硬件故障

C、一段特制的程序或代码片段

D、芯片霉变

答案：

ACDCD DDBDA

AAADD AABCC

DDBDB DACAC

BCDCA ADADD

AAABC DCBAC

DCABD ADBDA

DACDB CCAAA

DDCAD CAABA

BBDCB CCCDB

DDBAC CCCBC