**全国大学生网络安全知识竞赛试题及答案**

1. **单选题**

**1。大学生小吴在网上以一个知名作家的名义写博客，但事先没有征得该作家同意。小吴应当承担 （A)**

**A.侵权责任**

**B.违约责任**

**C.刑事责任**

**D。行政责任**

**2.绿色上网软件可以安装在家庭和学校的 （B)**

**A。电视机上**

**B。个人电脑上**

**C.电话上**

**D.幻灯机上**

**3。以下有关秘钥的表述,错误的是 （A）**

**A。密钥是一种硬件**

**B.密钥分为对称密钥与非对称密钥**

**C.对称密钥加密是指信息的发送方和接收方使用同一个密钥去加密和解密数据**

**D。非对称密钥加密需要使用不同的密钥来分别完成加密和解密操作**

**4.浏览网页时,遇到的最常见的网络广告形式是 （B）**

**A。飘移广告**

**B。旗帜广告**

**C.竞价广告**

**D.邮件列表**

**5.下列选项中，不属于个人隐私信息的是 (B）**

**A。恋爱经历**

**B。工作单位**

**C。日记**

**D。身体健康状况**

**6。根据《互联网上网服务营业场所管理条例》，网吧每日营业时间限于 （C）**

**A.6时至24时**

**B。7时至24时**

**C。8时至24时**

**D.9时至24时**

**7.李某将同学张某的小说擅自发表在网络上，该行为 (B）**

**A。不影响张某在出版社出版该小说,因此合法**

**B.侵犯了张某的著作权**

**C.并未给张某造成直接财产损失,因此合法**

**D。扩大了张某的知名度，应该鼓励**

**8.在设定网上交易流程方面，一个好的电子商务网站必须做到 （B)**

**A.对客户有所保留**

**B.不论购物流程在网站的内部操作多么复杂,其面对用户的界面必须是简单和操作方便的**

**C.使客户购物操作繁复但安全**

**D.让客户感到在网上购物与在现实世界中的购物流程是有区别的**

**9。我国出现第一例计算机病毒的时间是 (C）**

**A。1968年**

**B。1978年**

**C。1988年**

**D.1998年**

**10.表演者对其表演享有许可他人通过网络向公众传播其表演并获得报酬的权利。该权利的保护期限是 (A）**

**A。50年**

**B.60年**

**C.30年**

**D.没有期限**

**11.国际电信联盟将每年的5月17日确立为世界电信日.2014年已经是第46届,其世界电信日的主题为 （D)**

**A。“让全球网络更安全"**

**B。“信息通信技术:实现可持续发展的途径”**

**C。“行动起来创建公平的信息社会”**

**D.“宽带促进可持续发展”**

**12.下列有关隐私权的表述，错误的是 (C）**

**A。网络时代,隐私权的保护受到较大冲击**

**B.虽然网络世界不同于现实世界，但也需要保护个人隐私**

**C.由于网络是虚拟世界，所以在网上不需要保护个人的隐私**

**D.可以借助法律来保护网络隐私权**

**13.在原告起诉被告抢注域名案件中，以下不能判定被告对其域名的注册、使用具有恶意的是 （D）**

**A。为商业目的将他人驰名商标注册为域名的**

**B.为商业目的注册与原告的域名近似的域名，故意造成与原告网站的混淆,误导网络用户访问其网站的**

**C.曾要约高价出售其域名获取不正当利益的**

**D.注册域名后自己准备使用的**

1. **根据《治安管理处罚法》的规定，煽动民族仇恨、民族歧视，或者在出版物、计算机信息网络中刊载民族歧视、侮辱内容的,处10日以上15日以下拘留,可以并处(B）以下罚款。**

**A。500元**

**B。1000元**

**C.3000元**

**D.5000元**

**15。关于网络游戏的经营规则，下列说法错误的是 (D）**

**A。网络游戏运营企业应当要求网络游戏用户使用有效身份证件进行实名注册**

**B。网络游戏运营企业终止运营网络游戏应当提前60日予以公告**

**C.我国对国产网络游戏实行备案制**

**D。我国对进口网络游戏实行备案制**

**二、多选题**

**1.“三网合一”的“三网”是指 (ABC)**

**A。电信网**

**B。有线电视网**

**C。计算机网**

**D。交换网**

**2。未经权利人许可,不得将其作品或录音制品上传到网上和在网上传播.这里的权利人包括 (ABC）**

**A。版权所有人**

**B.表演者**

**C。录音制品制作者**

**D。网站管理者**

**3.下列有关局域网的说法，正确的是 （ACD）**

**A。局域网是一种通信网**

**B.连入局域网的数据通信设备只包括计算机**

**C.局域网覆盖有限的地理范围**

**D。局域网具有高数据传输率**

**4。用户可设置的文件的属性有 （BCD）**

**A.只写**

**B.隐藏**

**C。存档**

**D。只读**

**5.下列属于网络服务提供者的是 （ABCD）**

**A.网络接入服务提供者**

**B.网络空间提供者**

**C。搜索引擎服务提供者**

**D.传输通道服务提供者**

**6。多媒体计算机可以处理的信息类型有 （ABCD）**

**A.文字**

**B.图形**

**C.数字**

**D.音频视频**

**7。乳业巨头甲公司为了打击竞争对手乙公司，雇佣公关公司在网络上大肆宣传虚假事实，称乙公司生产的牛奶中含有违禁添加剂,造成乙公司巨大损失.对此，以下观点正确的是 （AB)**

**A.该行为可能涉嫌犯罪**

**B.该行为属于不正当竞争行为**

**C。针对这一犯罪只处罚个人**

**D。公关公司直接责任人员无需承担刑事责任**

**8.国家机关及其工作人员在对履行职责中知晓的公民个人电子信息,应当 （BC）**

**A。予以封存**

**B.予以保密**

**C.不得泄露、篡改、毁损**

**D。可以提供给第三人**

**9.网络服务提供者收集和使用个人信息应当符合的条件有 （ABCD)**

**A.告知权利人**

**B.明示收集、使用信息的目的、方式和范围**

**C。经被收集者同意**

**D。经监督管理机构许可或备案**

**10.按照刑法学的分类，网络犯罪可以被分为纯正的计算机犯罪和不纯正的计算机犯罪。纯正的计算机犯罪指针对计算机信息系统本身的犯罪;不纯正的计算机犯罪是指将计算机信息系统作为实施传统犯罪的犯罪工具的行为。下列行为中，属于不纯正的计算机犯罪的有 （BC）**

**A。盗卖他人的游戏“武器装备",致他人损失巨大**

**B.侵入高校网站大批量更改学历信息，从而为他人办理假学历获利**

**C.在网上大肆散播邪教的教义，发展邪教组织**

**D.传播木马软件，致使大量网站瘫痪**

**11。下列选项中，构成网络信息违法犯罪行为，公民和其他组织有权向有关主管部门举报、控告的是 (ABD)**

**A。窃取公民个人的电子信息**

**B.出售公民的个人电子信息**

**C。为配合公安机关办案需要,披露犯罪嫌疑人的电子信息**

**D。将公民个人电子信息提供给第三人**

**12。对于网络用户利用网络服务实施侵权行为的，以下表述正确的是 (ABC)**

**A。被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施**

**B.网络服务提供者接到通知后应采取必要措施**

**C。网络服务提供者接到通知后未及时采取必要措施的,应承担法律责任**

**D.网络服务提供者只是提供平台服务，不承担法律责任**

**13.网络谣言有可能侵犯他人的 （AB)**

**A。知情权**

**B。公平竞争权**

**C.财产权**

**D.人身权**

**14.以下对电子邮件的表述,正确的是 (BCD)**

**A。通讯双方必须都在场**

**B.邮件比人工邮件传送迅速、可靠且范围更广**

**C。邮件可以同时发送给多个用户**

**D.电子邮件中可以发送文字、图像、语音等信息**

**15.在电子商务条件下,卖方应当承担的义务有 （ABC)**

**A.按照合同的规定提交标的物及单据**

**B.对标的物的权利承担担保义务**

**C.对标的物的质量承担担保义务**

**D.对标的物验收的义务**

**16.威胁网络安全的主要因素有 (CD）**

**A。自然灾害**

**B.意外事故**

**C.计算机犯罪**

**D。“黑客"行为**

**17.以下关于非对称密钥的说法，正确的是 (AD）**

**A.加密密鈅对是用公钥来加密私钥来解密**

**B。签名密钥对是用私钥来加密公钥来解密**

**C.加密密鈅对是用私钥来加密公钥来解密**

**D.签名密钥对是用公钥来加密私钥来解密**

**18。计算机指令格式基本结构的两部分为 （AC）**

**A.操作码**

**B。数据码**

**C.地址码**

**D.控制码**

**19。互联网接入服务提供者应当记录上网用户的信息有 (ABD）**

**A.上网时间**

**B.用户帐号**

**C。用户密码**

**D.互联网地址**

**20.下列有关即时通讯工具服务提供者的说法，正确的是（BCD）**

**A。即时通信工具服务提供者无需取得相关资质**

**B。即时通信工具服务提供者应当遵循“后台实名、前台自愿"的原则**

**C.即时通信工具服务提供者应当对可以发布或转载时政类新闻的公众账号加注标识**

**D.即时通信工具服务使用者为从事公众信息服务活动开设公众账号，应当经即时通信工具服务提供者审核**

1. **判断题**

**1.在管理体系中,培训管理是确保信息系统安全的前提。 对**

**2。计算机良性病毒是不破坏计算机的数据或程序。它是一种只占用计算机资源来执行而不会导致计算机系统瘫痪的计算机病毒. 对**

**3.在域名中，WWW是指万维网. 对**

**4。公钥密码比传统密码更安全. 错**

**5。某人续写他人享有著作权的网络小说,并发表在盈利网站,此种行为没有侵犯原作者的权益。 错**

**6.PKI(Public Key Infrastructure）是利用公钥原理和技术实施和提供安全服务的具有普适性的安全基础设施。 对**

**7。一但中了IE窗口炸弹马上按下主机面板上的Reset键，重起计算机。 错**

**8.李某将同学张某的小说擅自发表在网络上，该行为如果不影响张某在出版社出版该小说,就是合法的。 错**

**9.在网络环境下，未经版权所有人、表演者和录音制品制作者的许可，可以将其作品或录音制品上传到网上和在网上传播。 错**

**10。对于重要的计算机系统，更换操作人员时,应令原操作员迅速交出掌握的各种技术资料、磁盘等存储器件，同时改变系统的口令密码。 对**

1. **在一所大学里,每个学院都有自己的局域网，连接各个学院的校园网也是局域网。 对**
2. **屏幕保护的密码是需要分大小写的。 对**

**13.中学、小学校园周围200米范围内不得设立网吧。 对**

**14。被侵权人与网络服务提供者达成的一方支付报酬，另一方提供删除、屏蔽、断开链接等服务的协议，人民法院应认定无效。 对**

**15。链路加密是对相邻节点之间的链路上所传输的数据进行加密。 错**

　一、单选题

　　1、网页恶意代码通常利用( C )来实现植入并进行攻击。

　　A、 口令攻击

　　B、 U盘工具

　　C、 IE浏览器的漏洞

　　D、 拒绝服务攻击

　　2、要安全浏览网页，不应该( A )。

　　A、 在他人计算机上使用“自动登录”和“记住密码”功能

　　B、 禁止使用Active（错）控件和Java 脚本

　　C、 定期清理浏览器Cookies

　　D、 定期清理浏览器缓存和上网历史记录

　　3、用户暂时离开时，锁定Windows系统以免其他人非法使用。锁定系统的快捷方式为同时按住( ） 。

　　A、 WIN键和Z键

　　B、 F1键和L键

　　C、 WIN键和L键

　　D、 F1键和Z键

　　4、网站的安全协议是https时,该网站浏览时会进行（ D )处理。

　　A、 口令验证B、 增加访问标记C、 身份验证D、 加密

　　5、为了规范互联网电子邮件服务，依法治理垃圾电子邮件问题，保障互联网电子邮件用户的合法权益,信息产业部于2006年2月20日颁布了，自2006年3月30日开始施行。 ( B )

　　A、《互联网信息服务管理办法》 B、《互联网电子邮件服务管理办法》

　　C、《互联网电子公告服务管理规定》

　　6、为了防范垃圾电子邮件，互联网电子邮件服务提供者应当按照信息产业部制定的技术标准建设互联网电子邮件服务系统,电子邮件服务器( C ）匿名转发功能。

　　A、使用 B、开启 C、关闭

　　7、互联网电子邮件服务提供者对用户的( A )和互联网电子邮件地址负有保密的义务。

　　A、个人注册信息 B、收入信息 C、所在单位的信息

　　8、任何组织或个人不得利用互联网电子邮件从事传播淫秽色情信息、窃取他人信息或者等违法犯罪活动，否则构成犯罪的，依法追究刑事责任,尚不构成犯罪的，由公安机关等依照有关法律、行zd规的规定予以处罚；电信业务提供者从事上述活动的，并由电信管理机构依据( A ）有关行zd规处罚。

　　A、故意传播计算机病毒 B、发送商业广告 C、传播公益信息

　　9、为了鼓励用户对违规电子邮件发送行为进行举报，发动全社会的监督作用,信息产业部委托中国互联网协会设立了互联网电子邮件举报受理中心,其举报电话是010-12321，举报电子邮箱地址为（ A )。

　　A、abuse＠anti—spam、cn B、register@china-cic、org

　　C、member＠china—cic、org

　　10、为了依法加强对通信短信息服务和使用行为的监管，信息产业部和有关部门正在联合制定（ B ）。

　　A、《通信服务管理办法》 B、《通信短信息服务管理规定》

　　C、《短信息管理条例》

　　11、如果您发现自己被手机短信或互联网站上的信息诈骗后，应当及时向（ C ）报案，以查处诈骗者，挽回经济损失。

　　A、消费者协会 B、电信监管机构 C、公安机关

　　12、为了有效抵御网络黑客攻击,可以采用作为安全防御措施. ( C ）

　　A、绿色上网软件 B、杀病毒软件 C、防火墙

　　13、按照《互联网电子公告服务管理规定》，任何人不得在互联网上的电子布告牌(BBS）、电子白板、电子论坛、（ B ）、留言板等电子公告服务系统中发布淫秽、色情、赌博、暴力、恐怖等违法有害信息.

　　A、网站 B、网络聊天室 C、电子邮箱

　　14、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，这属于什么攻击类型? （A)

　　A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

　　15、为了防御网络监听，最常用的方法是 ( B )

　　A、采用物理传输（非网络） B、信息加密 C、无线网 D、使用专线传输

　　16、向有限的空间输入超长的字符串是哪一种攻击手段?(A)

　　A、缓冲区溢出 B、网络监听 C、拒绝服务 D、IP欺骗

　　17、主要用于加密机制的协议是(D）

　　A、HTTP B、FTP C、TELNET D、SSL

　　18、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？ ( B ）

　　A、缓存溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDOS攻击

　　19、在以下认证方式中，最常用的认证方式是：(A）

　　A、基于账户名/口令认证 B、基于摘要算法认证

　　C、基于PKI认证 D、基于数据库认证

　　20、下列不属于系统安全的技术是（ B ）

　　A、防火墙 ;B、加密狗 ;C、认证 ; D、防病毒

　　21、抵御电子邮箱入侵措施中，不正确的是（ D )

　　A、不用生日做密码 B、不要使用少于5位的密码 C、不要使用纯数字

　　D、自己做服务器

　　22、不属于常见的危险密码是（ D ）

　　A、跟用户名相同的密码 B、使用生日作为密码 C、只有4位数的密码

　　D、10位的综合型密码

　　23、不属于计算机病毒防治的策略的是( D ）

　　A、

　　B、

　　C、

　　D、 确认您手头常备一张真正“干净”的引导盘 及时、可靠升级反病毒产品 新购置的计算机软件也要进行病毒检测 整理磁盘

　　24、在每天下午5点使用计算机结束时断开终端的连接属于( A ）

　　A、外部终端的物理安全 B、通信线的物理安全 C、窃听数据 D、网络地址欺骗

　　25、当今IT 的发展与安全投入，安全意识和安全手段之间形成( B ）

　　A、安全风险屏障 B、安全风险缺口

　　C、管理方式的变革 D、管理方式的缺口

　　26、我国的计算机年犯罪率的增长是（ C )

　　A、10% B、160％ C、60％ D、300％

　　27、信息安全风险缺口是指( A ）

　　A、IT 的发展与安全投入，安全意识和安全手段的不平衡

　　B、信息化中,信息不足产生的漏洞

　　C、计算机网络运行，维护的漏洞

　　D、计算中心的火灾隐患

　　28、网络攻击与防御处于不对称状态是因为( C )

　　A、管理的脆弱性 B、应用的脆弱性

　　C、网络软硬件的复杂性 D、软件的脆弱性

　　29、网络攻击的种类（ A ）

　　A、物理攻击，语法攻击,语义攻击 B、黑客攻击，病毒攻击

　　C、硬件攻击，软件攻击 D、物理攻击，黑客攻击,病毒攻击

　　30、语义攻击利用的是( A )

　　A、信息内容的含义 B、病毒对软件攻击

　　C、黑客对系统攻击 D、黑客和病毒的攻击

　　31、计算机网络最早出现在哪个年代? ( B )

　　A、20世纪50年代 B、20世纪60年代

　　C、20世纪80年代 D、20世纪90年代

　　32、最早研究计算机网络的目的是什么?( C )

　　A、直接的个人通信; B、共享硬盘空间、打印机等设备;

　　C、共享计算资源; D、大量的数据交换。

　　33、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

　　34、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?( C )

　　A、安装防火墙 B、安装入侵检测系统

　　C、给系统安装最新的补丁 D、安装防病毒软件

　　35、以网络为本的知识文明人们所关心的主要安全是（ C ）

　　A、人身安全 B、社会安全 C、信息安全

　　47、第一次出现”HACKER”这个词是在( B ）

　　A、BELL实验室 B、麻省理工AI实验室 C、AT＆T实验室

　　36、可能给系统造成影响或者破坏的人包括( A ）

　　A、所有网络与信息系统使用者 B、只有黑客 C、只有管理员

　　37、黑客的主要攻击手段包括（ A )

　　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

　　38、从统计的情况看，造成危害最大的黑客攻击是( C )

　　A、漏洞攻击 B、蠕虫攻击 C、病毒攻击

　　39、第一个计算机病毒出现在( B ）

　　A、40年代 B、70 年代 C、90年代

　　40、口令攻击的主要目的是（ B ）

　　A、获取口令破坏系统 B、获取口令进入系统 C、仅获取口令没有用途

　　41、通过口令使用习惯调查发现有大约\_B的人使用的口令长度低于5个字符的

　　A、50、5％ B、51、 5％ C、52、5%

　　42、通常一个三个字符的口令破解需要（ B ）

　　A、18毫秒 B、18 秒 C、18分钟

　　43、邮件炸弹攻击主要是( B ）

　　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

　　44、逻辑炸弹通常是通过（ B )

　　A、必须远程控制启动执行，实施破坏

　　B、指定条件或外来触发启动执行，实施破坏

　　C、通过管理员控制启动执行，实施破坏

　　45、扫描工具（ C ）

　　A、只能作为攻击工具 B、只能作为防范工具

　　C、既可作为攻击工具也可以作为防范工具

　　46、黑客造成的主要安全隐患包括( A )

　　A、破坏系统、窃取信息及伪造信息

　　B、攻击系统、获取信息及假冒信息

　　C、进入系统、损毁信息及谣传信息

　　47、从统计的资料看，内部攻击是网络攻击的( B )

　　A、次要攻击 B、最主要攻击 C、不是攻击源

　　48、一般性的计算机安全事故和计算机违法案件可由\_\_\_\_\_受理( C )

　　A、案发地市级公安机关公共信息网络安全监察部门

　　B、案发地当地县级(区、市）公安机关治安部门。

　　C、案发地当地县级(区、市)公安机关公共信息网络安全监察部门

　　D、案发地当地公安派出所

　　49、计算机刑事案件可由\_\_\_\_\_受理( A )

　　A、案发地市级公安机关公共信息网络安全监察部门

　　B、案发地市级公安机关治安部门

　　C、案发地当地县级（区、市)公安机关公共信息网络安全监察部门

　　D、案发地当地公安派出所

　　50、计算机信息系统发生安全事故和案件，应当\_\_\_\_\_\_在内报告当地公安机关公

　　共信息网络安全监察部门（ D )

　　A、8小时 B、48小时 C、36小时 D、24小时

　　51、对计算机安全事故的原因的认定或确定由\_\_\_\_\_作出( C ）

　　A、人民法院 B、公安机关 C、发案单位 D、以上都可以

　　52、对发生计算机安全事故和案件的计算机信息系统,如存在安全隐患的， B 应当要求限期整改。

　　A、人民法院 B、公安机关 C、发案单位的主管部门 D、以上都可以

　　53、传入我国的第一例计算机病毒是（ B ）

　　A、大麻病毒 B、小球病毒 C、1575病毒 D、米开朗基罗病毒

　　54、我国是在\_\_年出现第一例计算机病毒（ C )

　　A、1980 B、1983 C、1988 D、1977

　　55、计算机病毒是( A )

　　A、计算机程序 B、数据 C、临时文件 D、应用软件 56、1994年我国颁布的第一个与信息安全有关的法规是( D ）

　　A、国际互联网管理备案规定 B、计算机病毒防治管理办法

　　C、网吧管理规定 D、中华人民共和国计算机信息系统安全保护条例

　　57、网页病毒主要通过以下途径传播（ C )

　　A、邮件 B、文件交换 C、网络浏览 D、光盘

　　58、故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行, 后果严重的，将受到\_\_\_\_处罚( A ）

　　A、处五年以下有期徒刑或者拘役 B、拘留 C、罚款 D、警告

　　59、计算机病毒防治产品根据\_\_\_\_标准进行检验（ A )

　　A、计算机病毒防治产品评级准测 B、计算机病毒防治管理办法

　　C、基于DOS系统的安全评级准则 D、计算机病毒防治产品检验标准

　　60、《计算机病毒防治管理办法》是在哪一年颁布的( C )

　　A、1994 B、1997 C、2000 D、1998

　　61、VPN是指（ A ）

　　A、虚拟的专用网络 B、虚拟的协议网络 C、虚拟的包过滤网络

　　62、目前的防火墙防范主要是( B ）

　　A、主动防范 B、被动防范 C、不一定

　　63、IP地址欺骗通常是（ A ）

　　A、黑客的攻击手段 B、防火墙的专门技术 C、IP 通讯的一种模式 黑客在攻击中进行端口扫描可以完成( D ).

　　A、 检测黑客自己计算机已开放哪些端口

　　B、口令破译

　　C、 获知目标主机开放了哪些端口服务

　　D、截获网络流量

　　64、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？(C）

　　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

　　65、木马程序一般是指潜藏在用户电脑中带有恶意性质的 ( A ），利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息.

　　A、远程控制软件 B、计算机操作系统 C、木头做的马

　　66、为了防止各种各样的病毒对计算机系统造成危害，可以在计算机上安装防病毒软件,并注意及时 （ B ）,以保证能防止和查杀新近出现的病毒。

　　A、 分析 B、 升级 C、检查

　　67、局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样,则（ C ）。

　　A、两台计算机都正常

　　B、两台计算机都无法通讯

　　C、一台正常通讯一台无法通讯

　　68、企业重要数据要及时进行( C )，以防出现以外情况导致数据丢失. A、杀毒 B、加密 C、备份

　　69、窃听是一种（ ）攻击，攻击者( ）将自己的系统插入到发送站和接收站之间。截获是一种( ）攻击，攻击者（ ）将自己的系统插入到发送站和接受站之间。（A)

　　A、 被动,无须，主动,必须

　　B、 主动,必须,被动，无须

　　C、 主动，无须，被动，必须

　　D、 被动，必须，主动，无须

　　70、可以被数据完整性机制防止的攻击方式是(D）。

　　A、 假冒源地址或用户的地址欺骗攻击

　　B、 抵赖做过信息的递交行为

　　C、 数据中途被攻击者窃听获取

　　D、 数据在途中被攻击者篡改或破坏

　　71、王某,未经著作权人许可，以私服营运方式，通过信息网络向公众传播他人网络游戏软件，获利14万余元，其行为均构成（ A ).

　　A、侵犯著作权罪 B、侵犯商业秘密罪

　　C、非法侵入计算机信息系统罪 D、非法经营罪

　　72、任何组织或者个人注册微博客账号,制作、复制、发布、传播信息内容的，应当使用（ A ），不得以虚假、冒用的居民身份信息、企业注册信息、组织机构代码信息进行注册.网站开展微博客服务,应当保证前款规定的注册用户信息真实。

　　A真实身份信息 B正确的网站信息 C真实的ID D工商注册信息

　　73、2010年年底，熊某偶尔登录到一个境外的淫秽网站,发现该网站有大量的淫秽图片及视频可以观看,便在该网站上注册成为会员。之后，熊某渐渐沉迷于这些淫秽图片和视频，不能自拔。为获得更大的浏览权限,熊某便陆续发了17篇包含淫秽信息的帖子共被点击查看29410次，以不断提高自身的会员等级。熊某的行为（ B )

　　A不构成犯罪 B构成传播淫秽物品罪

　　C构成非法经营罪 D构成制作、复制、出版、贩卖、传播淫秽物品牟利罪

　　74、文艺青年张小五写了一部反映社会现实的小说，发表后引起热烈反响，好评如潮.甲网站觉得有利可图，擅自将该小说发布在网络上,供网民在线阅读。该网站侵犯了张小五的哪种著作权?（ B )

　　A发表权 B信息网络传播权 C复制权 D发行权

　　75、著作权行政管理部门对侵犯互联网信息服务活动中的信息网络传播权的行为实施行政处罚，适用（ A )

　　A《著作权行政处罚实施办法》

　　B《互联网著作权行政保护办法》

　　C民法中关于知识产权的相关规定

　　D《商标法》

　　二、判断题

　　1、VPN的主要特点是通过加密使信息能安全的通过Internet传递。（对）

　　2、密码保管不善属于操作失误的安全隐患。（错）

　　3、漏洞是指任何可以造成破坏系统或信息的弱点。（对）

　　4、安全审计就是日志的记录。(错）

　　5、计算机病毒是计算机系统中自动产生的。(错）

　　6、对于一个计算机网络来说，依靠防火墙即可以达到对网络内部和外部的安全防护（错）

　　7、网络安全应具有以下四个方面的特征:保密性、完整性、可用性、可查性。（错）

　　8、最小特权、纵深防御是网络安全原则之一。（对)

　　9、安全管理从范畴上讲，涉及物理安全策略、访问控制策略、信息加密策略和网络安全管理策略。(对）

　　10、用户的密码一般应设置为16位以上。（对)

　　11、开放性是UNIX系统的一大特点。(对)

　　12、防止主机丢失属于系统管理员的安全管理范畴.(错）

　　13、我们通常使用SMTP协议用来接收E-MAIL。（错）

　　14、在堡垒主机上建立内部DNS服务器以供外界访问，可以增强DNS服务器的安全性。(错）

　　15、为了防御网络监听，最常用的方法是采用物理传输。（错)

　　16、使用最新版本的网页浏览器软件可以防御黑客攻击。(对)

　　17、通过使用SOCKS5代理服务器可以隐藏QQ的真实IP。（对)

　　18、一但中了IE窗口炸弹马上按下主机面板上的Reset键，重起计算机。(错）

　　19、禁止使用活动脚本可以防范IE执行本地任意程序。（对)

　　20、只要是类型为TXT的文件都没有危险。(错)

　　21、不要打开附件为SHS格式的文件。（对）

　　22、发现木马，首先要在计算机的后台关掉其程序的运行。(对）

　　23、限制网络用户访问和调用cmd的权限可以防范Unicode漏洞.(对)

　　24、解决共享文件夹的安全隐患应该卸载Microsoft网络的文件和打印机共享.(对）

　　25、不要将密码写到纸上。(对)

　　26、屏幕保护的密码是需要分大小写的。(对）

　　27、计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒.（对)

　　28、木马不是病毒.（对）

　　29.复合型防火墙防火墙是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用，同时也常结合过滤器的功能。（对)

　　30、非法访问一旦突破数据包过滤型防火墙，即可对主机上的软件和配置漏洞进行攻击。（错)

　　31、ATM 技术领先于TCP/IP技术，即将取代IP技术，实现语音、视频、数据传输网络的三网合一（错）

　　32、Internet设计之初，考虑了核战争的威胁,因此充分考虑到了网络安全问(错)

　　33、我的计算机在网络防火墙之内,所以其他用户不可能对我计算机造成威胁（错)

　　34、Internet没有一个集中的管理权威（对）

　　35、统计表明，网络安全威胁主要来自内部网络，而不是Internet（对)

　　36、只要设置了足够强壮的口令,黑客不可能侵入到计算机中（错）

　　37、路由器在转发IP分组时，一般不检查IP分组的源地址，因此可以伪造IP分组的源地址进行攻击，使得网络管理员无法追踪。(对)

　　38、发起大规模的DDoS攻击通常要控制大量的中间网络或系统（对)

　　39、路由协议如果没有认证功能,就可以伪造路由信息，导致路由表混乱，从而使网络瘫痪（对）

　　40、目前入侵检测系统可以及时的阻止黑客的攻击。(错）

　　41、TCSEC是美国的计算机安全评估机构和安全标准制定机构(对)

　　42、蠕虫、特洛伊木马和病毒其实是一回事（错）

　　43、只要选择一种最安全的操作系统，整个系统就可以保障安全(错）

　　44、在计算机系统安全中，人的作用相对于软件，硬件和网络而言，不是很重要（错）

　　45、在设计系统安全策略时要首先评估可能受到的安全威胁（对）

　　46、安装系统后应当根据厂商或安全咨询机构的建议对系统进行必要的安全配置(对)

　　47、系统安全的责任在于IT技术人员，最终用户不需要了解安全问题(错)

　　48.网络的发展促进了人们的交流,同时带来了相应的安全问题(错）

　　49。具有政治目的的黑客只对政府的网络与信息资源造成危害(错）

　　50、病毒攻击是危害最大、影响最广、发展最快的攻击技术(错)

　　51、黑色星期四”是因有人通过BELL实验室与Internet连接的有漏洞的机器上放置了一个蠕虫程序而引起网络灾难得名的(错)

　　52、邮件的附件如果是带有。exe、.com、.pif、。pl、.src和。vbs为后缀的文件，应确定其安全后再打开 (对)

　　53、在信息战中中立国的体现要比非信息战简单(错)

　　54、信息战的军事目标是指一个国家军队的网络系统、信息系统、数据资源（错)

　　55、计算机病毒是计算机系统中自动产生的(错)

　　56、小球病毒属于引导型病毒（对）

　　57、公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作(对)

　　58、计算机病毒防治产品实行销售许可证制度(对）

　　59、计算机病毒防治产品分为三级，其中三级品为最高级(错)

　　60，删除不必要的网络共享可以提高防范病毒的能力（对）

　　61、带VPN的防火墙一旦设置了VPN 功能，则所有通过防火墙的数据包都将

　　62、通过VPN通道进行通讯（错）

　　63、VPN的所采取的两项关键技术是认证与加密（对)

　　64、要保证一个公司总部与其分支机构的网络通讯安全只有通过VPN来实现（错）

　　65、网络安全工程实施的关键是质量，而质量的关键是服务的长期保障能力（对)

　　66、网络安全服务的开展与网络安全防范是一对矛盾(对）

　　67、网络安全边界防范的不完备性仅指防外不防内（错）

　　68、使用最新版本的网页浏览器软件可以防御黑客攻击。(错）

　　69、不要将密码写到纸上.(对)

　　70、计算机数据恢复在实际生活当中可以百分百恢复。(错）

　　71、违反国家法律、法规的行为，危及计算机信息系统安全的事件，称为计算机案件。(对)

　　72、计算机犯罪是行为人以计算机为工具或以计算机资产为犯罪对象实施的,依照我国刑法应受处罚的,具有社会危害性的行为.（对）

　　73、 计算机信息系统的安全威胁同时来自内、外两个方面。 (对)

　　74、外单位人员如可以随意接入奇瑞公司内网。（错）

　　75、格式化过后的计算机，原来的数据就找不回来了（错）

　　问答题:

　　1、今年我国首届国家网络安全宣传周的主题是什么？

　　答案:共建网络安全，共享网络文明

　　2、罗定职业技术学院的官方网址是什么?

　　答案：www.niubb。net和 www。niubb.net

　　3、罗定职业技术学院政务和公益机构域名是什么?

　　答案：罗定职业技术学院.公益

　　4、首次使用CRP数字校园、校园一卡通等信息系统时，为了保存自已的信息和财产安全应当怎么做？

　　答案：进入信息系统修改密码，并将其设置为一个复杂的密码。

　　5、计算机网络最突出的优点是什么?

　　答案：共享资源

　　6、信息安全有哪些常见的威胁？

　　答案：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击,恶意代码。

　　7、解决互联网安全问题的根本条件是什么？

　　答案：提高整个社会网民的互联网道德本质。

　　8、什么是钓鱼网站?

　　答案：“钓鱼网站”是一种网络欺诈行为,指不法分子利用各种手段，仿冒真实网站的URL地址以及页面内容，或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的HTML代码,以此来骗取用户银行或信用卡账号、密码等私人资料。

　　9、什么是网络安全?

　　答案：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续可靠正常地运行，网络服务不被中断。

　　10、什么是木马？

　　答案:木马是一种带有恶意性质的远程控制软件。木马一般分为客户端

　　(client）和服务器端（server)。客户端就是本地使用的各种命令的控制台,服务器端则是要给别人运行，只有运行过服务器端的计算机才能够完全受控。木马不会像病毒那样去感染文件。

　　11、什么是后门？

　　答案：后门是指一种绕过安全性控制而获取对程序或系统访问权的方法。

　　12、防范网络黑客防措施有哪些？

　　答案：①选用安全的口令②口令不得以明文方式存放在系统中③建立帐号锁定机制④实施存取控制⑤确保数据的安全

　　13、网络病毒的来源有哪些?

　　答案：邮件附件、E—mail 、Web服务器、文件共享。

　　14、局域网内部若出现ARP攻击，会出现哪两种两句现象?

　　答案：1.不断弹出“本机的（错）（错）（错）段地址与网络中的（错）(错）(错）段地址冲突"的对话框。2.计算机不能正常上网，出现网络中断的症状。

　　15、控制USB接口使用的目的?

　　答案：1、网络的安全 2、信息的保密

　　16、什么是IP欺骗?

　　答案：攻击者可通过伪装成被信任源IP地址等方式来骗取目标主机的信任.

　　17、电子邮件存在哪些安全性问题？

　　1、垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷,影响网络传输速度，占用邮件服务器的空间。2、诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜，发信人能迅速让大量受害者上当。3、邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为，信箱不能承受时就会崩溃。4、通过电子邮件传播的病毒，大多数采用附件的形式夹带在电子邮件中。当收信人打开附件后,病毒会查询他的通讯簿，给其上所有或部分人发信，并将自身放入附件中，以此方式继续传播扩散.

　　18、什么是网络蠕虫？

　　答案：网络蠕虫是一种智能化、自动化，综合网络攻击、密码学和计算机病毒技术，无须计算机使用者干预即可运行的攻击程序或代码。

　　19、网络蠕虫有什么特征？

　　答案：具有病毒的特征，传染性，隐蔽性，破坏性；不利用文件寄生,可以主动传播,并且通过网络可快速传播，容易造成网络拥塞；具有智能化、自动化和高技术化;

　　20、防火墙的基本功能有哪些?

　　答案：1过滤进出网络的数据；2管理进出网络的访问行为；3封堵某些禁止的业务；4记录进出网络的信息和活动;5对网络的攻击进行将侧和报警.

　　21、因特网电子商务系统必须保证网络安全的四大要素是什么？

　　答案：1传输数据的保密性;2数据的完整性;3交易各方身份的真实性； 4交易的不可抵赖性;

　　21、对蠕虫病毒和一般病毒进行比较有什么区别?

　　答案：存在形式：普通病毒寄存在文件上，蠕虫病毒寄存在独立程序上; 传染机制：普通病毒在宿主程序上运行,蠕虫病毒会主动攻击；

　　传染目标：普通病毒传染本地文件，蠕虫病毒传染整个网络的计算机.

　　22、黑客攻击的动机都有哪些?

　　答案：1.好奇心理2。挑战性.3。报复心理4,经济利益5,政治目的，6。情报获取

　　23、什么是密码破解，有哪些方法？

　　答案：通过猜解或者直接破坏原密码的密码验证机制来达到和密码分析一样的最终效果，或者是密码对应的权限。

　　一般的密码破解大致分为以下几类.

　　1)使用软件无限次尝试密码。2)绕过密码验证机制。3)如果密码加密，使用替代密码代替原密码

　　24、后门程序与计算机病毒的差别是什么?

　　答案：后门程序又称特洛伊木马，其用途是潜伏在用户的计算机中，进行信息搜集或便于黑客进入。后门程序和计算机病毒最大的差别,在于后门程序不一定有自我复制的动作，即后门程序不一定会“感染”其他计算机.

　　25、黑客技术发展趋势是什么?

　　答案：（1）网络攻击的自动化程度和攻击速度不断提高（2）攻击工具越来越复杂(3）黑客利用安全漏洞的速度越来越快(4）防火墙被攻击者渗透的情况越来越多（5)安全威胁的不对称性在增加(6)攻击网络基础设施产生的破坏效果越来越大

　　26、什么是漏洞?

　　答案：漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

　　27、网络面临的安全威胁主要有哪些方面?

　　网络面临的安全威胁可分为两种：一是对网络数据的威胁;二是对网络设备的威胁.概括起来主要威胁包括以下几个方面:1)由自然力造成的非人为的数据丢失、设备失效、线路阻断。2）人为但属于操作人员无意的失误造成的数据丢失.3)来自外部和内部人员的恶意攻击和入侵.

　　28、IPv6先对IPv4有哪些优势？

　　IPv6优势：首先，IPv6解决了IP地址数量短缺的问题;其次，IPv6对IPv4协议中诸多不完善之处进行了较大的改进，在网络保密性、完整性方面作了更好的改进，在可控性和抗否认性方面有了新的保证。

　　29、计算机病毒传染的一般过程是什么?？

　　答案：1)判断传染目标(文件)是否符合感染条件(是否已经被感染）

　　2）若目标符合感染条件，则将病毒链接到传染目标的特点位置，并存入磁盘。

　　3)继续监视系统的运行，寻找新的传染目标

　　30、网络安全服务包括哪些?

　　答案:1、对等实体认证服务2、数据源点认证服务3数据保密服务4数据完整性服务5访问控制服务6可用性

**一、单选题**

**1。大学生小吴在网上以一个知名作家的名义写博客,但事先没有征得该作家同意。小吴应当承担(A）**

**A。侵权责任 B。违约责任 C.刑事责任 D.行政责任**

**2。绿色上网软件可以安装在家庭和学校的（B）**

**A.电视机上 B.个人电脑上 C.电话上 D.幻灯机上**

**3。以下有关秘钥的表述，错误的是（A)**

**A.密钥是一种硬件 B.密钥分为对称密钥与非对称密钥**

**C。对称密钥加密是指信息的发送方和接收方使用同一个密钥去加密和解密数据**

**D。非对称密钥加密需要使用不同的密钥来分别完成加密和解密操作**

**4。浏览网页时,遇到的最常见的网络广告形式是(B）**

**A.飘移广告 B。旗帜广告 C.竞价广告 D.邮件列表**

**5.下列选项中,不属于个人隐私信息的是（B)**

**A.恋爱经历 B.工作单位 C.日记 D。身体健康状况**

**6.根据《互联网上网服务营业场所管理条例》,网吧每日营业时间限于(C）**

**A.6时至24时 B。7时至24时 C。8时至24时 D.9时至24时**

**7.李某将同学张某的小说擅自发表在网络上,该行为（B)**

**A。不影响张某在出版社出版该小说，因此合法 B.侵犯了张某的著作权 C。并未给张某造成直接财产损失，因此合法**

**D。扩大了张某的知名度,应该鼓励**

**8。在设定网上交易流程方面,一个好的电子商务网站必须做到(B）**

**A.对客户有所保留**

**B。不论购物流程在网站的内部操作多么复杂,其面对用户的界面必须是简单和操作方便的**

**C。使客户购物操作繁复但安全**

**D.让客户感到在网上购物与在现实世界中的购物流程是有区别的**

**9.我国出现第一例计算机病毒的时间是（C）**

**A。1968年 B.1978年 C.1988年 D。1998年 10。表演者对其表演享有许可他人通过网络向公众传播其表演并获得报酬的权利.该权利的保护期限是(A) A。50年 B.60年 C。30年 D。没有期限**

**11。国际电信联盟将每年的5月17日确立为世界电信日.2014年已经是第46届，其世界电信日的主题为（D）**

**A。“让全球网络更安全” B。“信息通信技术:实现可持续发展的途径" C.“行动起来创建公平的信息社会" D。“宽带促进可持续发展"**

**12。下列有关隐私权的表述,错误的是（C)**

**A.网络时代,隐私权的保护受到较大冲击 B.虽然网络世界不同于现实世界，但也需要保护个人隐私 C。由于网络是虚拟世界，所以在网上不需要保护个人的隐私 D.可以借助法律来保护网络隐私权**

**13.在原告起诉被告抢注域名案件中,以下不能判定被告对其域名的注册、使用具有恶意的是（D） A。为商业目的将他人驰名商标注册为域名的 B.为商业目的注册与原告的域名近似的域名，故意造成与原告网站的混淆，误导网络用户访问其网站的 C.曾要约高价出售其域名获取不正当利益的 D。注册域名后自己准备使用的**

**14。根据《治安管理处罚法》的规定,煽动民族仇恨、民族歧视，或者在出版物、计算机信息网络中刊载民族歧视、侮辱内容的,处10日以上15日以下拘留,可以并处（B)以下罚款.**

**A。500元 B.1000元 C。3000元 D。5000元**

**二、多选题**

**1。“三网合一”的“三网"是指（ABC) A。电信网 B。有线电视网 C。计算机网 D。交换网**

**2。未经权利人许可,不得将其作品或录音制品上传到网上和在网上传播。 这里 的权利人包括（ABC） A。版权所有人 B。表演者 C。录音制品制作者 D。网站管理者 3.下列有关局域网的说法，正确的是（ACD） A.局域网是一种通信网 B。连入局域网的数据通信设备只包括计算机 C.局域网覆盖有限的地理范围 D。局域网具有高数据传输率**

**4.用户可设置的文件的属性有（BCD) A.只写 B.隐藏 C.存档 D。只读**

单选题

1。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,这属于什么攻击类型？ (A)

A、拒绝服务

B、文件共享

C、BIND漏洞

D、远程过程调用

2。为了防御网络监听,最常用的方法是 （B）

A、采用物理传输(非网络）

B、信息加密

C、无线网

D、使用专线传输

3.向有限的空间输入超长的字符串是哪一种攻击手段?(A)

A、缓冲区溢出;

B、网络监听

C、拒绝服务

D、IP欺骗

4.主要用于加密机制的协议是（D)

A、HTTP

B、FTP

C、TELNET

D、SSL

5。用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码,这是属于何种攻击手段? (B）

A、缓存溢出攻击;

B、钓鱼攻击

C、暗门攻击；

D、DDOS攻击

6。Windows NT 和Windows 2000系统能设置为在几次无效登录后锁定帐号,这可以防止(B)

A、木马;

B、暴力攻击;

C、IP欺骗；

D、缓存溢出攻击

7.在以下认证方式中,最常用的认证方式是：(A）

A基于账户名／口令认证

B基于摘要算法认证 ;

C基于PKI认证 ；

D基于数据库认证

8.以下哪项不属于防止口令猜测的措施? (B)

A、严格限定从一个给定的终端进行非法认证的次数;

B、确保口令不在终端上再现;

C、防止用户使用太短的口令;

D、使用机器产生的口令

9。下列不属于系统安全的技术是(B)

A、防火墙

B、加密狗

C、认证

D、防病毒

10。抵御电子邮箱入侵措施中,不正确的是( D ）

A、不用生日做密码

B、不要使用少于5位的密码

C、不要使用纯数字

D、自己做服务器

11.不属于常见的危险密码是（ D )

A、跟用户名相同的密码

B、使用生日作为密码

C、只有4位数的密码

D、10位的综合型密码

12.不属于计算机病毒防治的策略的是（ D ）

1. 确认您手头常备一张真正“干净”的引导盘
2. 及时、可靠升级反病毒产品
3. 新购置的计算机软件也要进行病毒检测
4. 整理磁盘

13.针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，这是（ ）防火墙的特点。(D)

A、包过滤型

B、应用级网关型

C、复合型防火墙

D、代理服务型

14.在每天下午5点使用计算机结束时断开终端的连接属于（ A ）

A、外部终端的物理安全

B、通信线的物理安全

C、窃听数据

D、网络地址欺骗

15.2003年上半年发生的较有影响的计算机及网络病毒是什么（B)

(A)SARS

（B）SQL杀手蠕虫

(C)手机病毒

（D）小球病毒

16。SQL 杀手蠕虫病毒发作的特征是什么(A）

（A)大量消耗网络带宽

(B)攻击个人PC终端

（C）破坏PC游戏程序

（D）攻击手机网络

17。当今IT 的发展与安全投入，安全意识和安全手段之间形成(B)

(A）安全风险屏障

(B)安全风险缺口

（C)管理方式的变革

(D）管理方式的缺口

18.我国的计算机年犯罪率的增长是(C)

(A)10%

(B)160%

（C)60％

(D)300%

19。信息安全风险缺口是指(A)

(A）IT 的发展与安全投入,安全意识和安全手段的不平衡

（B)信息化中,信息不足产生的漏洞  
（C)计算机网络运行,维护的漏洞

(D)计算中心的火灾隐患

20.信息网络安全的第一个时代（B)

(A)九十年代中叶

(B)九十年代中叶前

（C）世纪之交

（D)专网时代

21。信息网络安全的第三个时代（A)

(A）主机时代, 专网时代, 多网合一时代

（B)主机时代, PC机时代， 网络时代

(C)PC机时代,网络时代，信息时代

（D）2001年,2002年,2003年

22。信息网络安全的第二个时代(A）

（A）专网时代

（B)九十年代中叶前

（C)世纪之交

23.网络安全在多网合一时代的脆弱性体现在（C)

（A）网络的脆弱性

（B)软件的脆弱性

（C）管理的脆弱性

(D)应用的脆弱性

24.人对网络的依赖性最高的时代(C）

(A)专网时代

（B)PC时代

（C）多网合一时代

(D）主机时代

25.网络攻击与防御处于不对称状态是因为（C)

（A）管理的脆弱性

（B)应用的脆弱性

（C)网络软，硬件的复杂性

(D）软件的脆弱性

26。网络攻击的种类（A)

(A）物理攻击，语法攻击，语义攻击

（B）黑客攻击，病毒攻击

(C）硬件攻击,软件攻击

(D）物理攻击，黑客攻击，病毒攻击

27.语义攻击利用的是（A）

(A）信息内容的含义

(B）病毒对软件攻击

（C）黑客对系统攻击

(D）黑客和病毒的攻击

28。1995年之后信息网络安全问题就是(A)

（A)风险管理

（B）访问控制

（C)消除风险

(D)回避风险

29.风险评估的三个要素(D)

（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

30。信息网络安全（风险）评估的方法（A）

(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

31.PDR模型与访问控制的主要区别（A）

(A)PDR把安全对象看作一个整体

(B)PDR作为系统保护的第一道防线

（C)PDR采用定性评估与定量评估相结合

(D)PDR的关键因素是人

32。信息安全中PDR模型的关键因素是(A)

（A）人

（B）技术

（C)模型

(D）客体

33。计算机网络最早出现在哪个年代(B）

(A）20世纪50年代

(B)20世纪60年代

(C)20世纪80年代

(D）20世纪90年代

34。最早研究计算机网络的目的是什么？（C）

（A)直接的个人通信；

（B)共享硬盘空间、打印机等设备;

(C)共享计算资源；

D大量的数据交换.

35.最早的计算机网络与传统的通信网络最大的区别是什么?(B)

(A）计算机网络带宽和速度大大提高。

（B)计算机网络采用了分组交换技术.

（C）计算机网络采用了电路交换技术

(D)计算机网络的可靠性大大提高。

36.关于80年代Mirros 蠕虫危害的描述，哪句话是错误的？(B)

（A）该蠕虫利用Unix系统上的漏洞传播

（B)窃取用户的机密信息，破坏计算机数据文件  
（C）占用了大量的计算机处理器的时间，导致拒绝服务

(D）大量的流量堵塞了网络,导致网络瘫痪

37.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

38.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？（C)

（A）安装防火墙

（B)安装入侵检测系统

(C）给系统安装最新的补丁

（D）安装防病毒软件

39.下面哪个功能属于操作系统中的安全功能 （C)

(A)控制用户的作业排序和运行

(B)实现主机和外设的并行处理以及异常情况的处理  
(C）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

(D）对计算机用户访问系统和资源的情况进行记录

40。下面哪个功能属于操作系统中的日志记录功能（D）

（A)控制用户的作业排序和运行

(B)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  
(C）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

(D）对计算机用户访问系统和资源的情况进行记录

42。Windows NT提供的分布式安全环境又被称为(A）

（A)域（Domain)

（B）工作组

（C)对等网

(D）安全网

43.下面哪一个情景属于身份验证(Authentication）过程(A)

（A)用户依照系统提示输入用户名和口令  
(B)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  
（C)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  
（D)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

44.下面哪一个情景属于授权（Authorization)（B）

（A）用户依照系统提示输入用户名和口令  
（B）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  
（C）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  
(D）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

45。下面哪一个情景属于审计（Audit）（D）

(A）用户依照系统提示输入用户名和口令  
（B)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  
(C）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  
（D）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

46.以网络为本的知识文明人们所关心的主要安全是（C)

(A）人身安全

（B）社会安全

（C）信息安全

47。第一次出现"HACKER"这个词是在(B)

（A)BELL实验室

(B)麻省理工AI实验室

(C）AT＆T实验室

48.可能给系统造成影响或者破坏的人包括（A）

（A）所有网络与信息系统使用者

（B)只有黑客

(C)只有跨客

49.黑客的主要攻击手段包括(A）

(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

50。从统计的情况看，造成危害最大的黑客攻击是（C)

（A)漏洞攻击

(B)蠕虫攻击

(C)病毒攻击

51。第一个计算机病毒出现在（B)

(A）40年代

(B)70 年代

（C）90年代

52.口令攻击的主要目的是（B）

（A）获取口令破坏系统

（B）获取口令进入系统

(C）仅获取口令没有用途

53.通过口令使用习惯调查发现有大约\_\_\_%的人使用的口令长度低于5个字符的（B）

(A）50.5

(B)51。 5

（C)52.5

54。通常一个三个字符的口令破解需要(B）

（A）18毫秒

（B)18 秒

（C）18分

55.黑色星期四是指（A）

（A）1998年11月3日星期四

(B）1999年6月24日星期四

（C）2000年4月13日星期四

56。大家所认为的对Internet安全技术进行研究是从\_\_\_\_\_\_\_时候开始的  （C)

(A)Internet 诞生

(B)第一个计算机病毒出现

（ C）黑色星期四

57.计算机紧急应急小组的简称是（A）

(A)CERT

（B）FIRST

（C)SANA

58。邮件炸弹攻击主要是（B)

（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

59。逻辑炸弹通常是通过（B)

（A）必须远程控制启动执行，实施破坏

（B)指定条件或外来触发启动执行,实施破坏

(C)通过管理员控制启动执行，实施破坏

60.1996年上海某寻呼台发生的逻辑炸弹事件，造事者被判”情节轻微,无罪释放"是因为（C)

(A)证据不足

（B)没有造成破坏

(C)法律不健全

61。扫描工具（C)

（A)只能作为攻击工具

（B)只能作为防范工具

(C)既可作为攻击工具也可以作为防范工具

62。DDOS攻击是利用\_\_\_\_\_进行攻击(C）

（A）其他网络

（B）通讯握手过程问题

(C)中间代理

63.全国首例计算机入侵银行系统是通过(A）

（A)安装无限MODEM进行攻击

(B)通过内部系统进行攻击

（C）通过搭线进行攻击

64。黑客造成的主要安全隐患包括（A)

(A）破坏系统、窃取信息及伪造信息

（B）攻击系统、获取信息及假冒信息

(C)进入系统、损毁信息及谣传信息

65.从统计的资料看，内部攻击是网络攻击的（B）

(A）次要攻击

(B）最主要攻击

(C）不是攻击源

66.江泽民主席指出信息战的主要形式是（A）

（A)电子战和计算机网络战

（B）信息攻击和网络攻击

(C）系统破坏和信息破坏

67。广义地说，信息战是指敌对双方为达成各自的国家战略目标，为夺取\_\_\_\_\_\_在等各个领域的信息优势，运用信息和信息技术手段而展开的信息斗争（B）

(A)政治、经济、国防、领土、文化、外交

（B)政治、经济、军事、科技、文化、外交

（C）网络、经济、信息、科技、文化、外交

68.狭义地说，信息战是指军事领域里的信息斗争.它是敌对双方为争夺信息的\_\_\_\_\_\_,通过利用、破坏敌方和保护己方的信息、信息系统而采取的作战形式 （C)

（A）占有权、控制权和制造权

（B）保存权、制造权和使用权

(C）获取权、控制权和使用权

69.信息战的战争危害较常规战争的危害（C）

（A)轻

B)重

（C)不一定

70。信息战的军人身份确认较常规战争的军人身份确认（A)

（A)难

（B）易

(C)难说

71。互联网用户应在其网络正式联通之日起\_\_\_\_\_内，到公安机关办理国际联网备案手续(A)

（A)三十日

（B)二十日

(C)十五日

(D）四十日

72。一般性的计算机安全事故和计算机违法案件可由\_\_\_\_\_受理(C）

（A）案发地市级公安机关公共信息网络安全监察部门  
(B）案发地当地县级（区、市）公安机关治安部门。  
(C)案发地当地县级（区、市）公安机关公共信息网络安全监察部门  
（D)案发地当地公安派出所

73。计算机刑事案件可由\_\_\_\_\_受理(A)

（A)案发地市级公安机关公共信息网络安全监察部门  
(B)案发地市级公安机关治安部门  
(C）案发地当地县级（区、市）公安机关公共信息网络安全监察部门  
(D）案发地当地公安派出所

74.计算机信息系统发生安全事故和案件,应当\_\_\_\_\_\_在内报告当地公安机关公共信息网络安全监察部门(D)

(A）8小时

（B)48小时

(C)36小时

（D）24小时

75。对计算机安全事故的原因的认定或确定由\_\_\_\_\_作出（C）

（A)人民法院

（B）公安机关

(C)发案单位

(D）以上都可以

76.对发生计算机安全事故和案件的计算机信息系统，如存在安全隐患的,\_\_\_\_\_\_应当要求限期整改（B）

（A)人民法院

（B）公安机关

(C)发案单位的主管部门

(D）以上都可以

77.传入我国的第一例计算机病毒是＿＿(B)

（A）大麻病毒

(B）小球病毒

(C）1575病毒

（D）米开朗基罗病毒

78.我国是在＿＿年出现第一例计算机病毒(C)

(A）1980

（B)1983

（C)1988

（D）1977

79.计算机病毒是\_\_\_\_\_（A)

(A）计算机程序

(B）数据

（C）临时文件

（D)应用软件

80。计算机病毒能够\_\_\_\_\_（ABC)

（A)破坏计算机功能或者毁坏数据

(B)影响计算机使用

(C）能够自我复制

（D)保护版权

81。1994年我国颁布的第一个与信息安全有关的法规是\_\_\_\_\_（D)

(A）国际互联网管理备案规定

（B）计算机病毒防治管理办法

（C）网吧管理规定

(D)中华人民共和国计算机信息系统安全保护条例

82.网页病毒主要通过以下途径传播（C)

（A）1>邮件

（B)文件交换

(C）网络浏览

(D）光盘

83。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行,后果严重的,将受到\_\_\_\_处罚（A）

（A）处五年以下有期徒刑或者拘役

(B)拘留

(C)罚款

（D）警告

84.计算机病毒防治产品根据\_\_\_\_标准进行检验(A)

（A）计算机病毒防治产品评级准测

（B)计算机病毒防治管理办法

(C）基于DOS系统的安全评级准则

（D)计算机病毒防治产品检验标准

85.《计算机病毒防治管理办法》是在哪一年颁布的（C)

(A）1994

（B）1997

(C)2000

（D)1998

86。边界防范的根本作用是(C)

（A）对系统工作情况进行检验与控制,防止外部非法入侵  
（B)对网络运行状况进行检验与控制，防止外部非法入侵  
（C）对访问合法性进行检验与控制，防止外部非法入侵

87.路由设置是边界防范的(A）

(A)基本手段之一

（B）根本手段

(C）无效手段

88。网络物理隔离是指（C)

(A)两个网络间链路层在任何时刻不能直接通讯  
（B)两个网络间网络层在任何时刻不能直接通讯  
（C）两个网络间链路层、网络层在任何时刻都不能直接通讯

89。VPN是指（A）

（A）虚拟的专用网络

(B)虚拟的协议网络

C)虚拟的包过滤网络

90。带VPN的防火墙的基本原理流程是（A）

(A）先进行流量检查

(B)先进行协议检查

(C）先进行合法性检查

91.防火墙主要可以分为(A)

（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

92。NAT 是指(B）

（A)网络地址传输

（B)网络地址转换

（C)网络地址跟踪

93.VPN通常用于建立\_\_\_\_之间的安全通道(A）

（A)总部与分支机构、与合作伙伴、与移动办公用户  
(B)客户与客户、与合作伙伴、与远程用户  
(C)总部与分支机构、与外部网站、与移动办公用户

94.在安全区域划分中DMZ 区通常用做（B)

（A)数据区

（B)对外服务区

(C）重要业务区

95。目前用户局域网内部区域划分通常通过\_\_\_\_实现（B)

(A)物理隔离

(B）Vlan 划分

（C）防火墙防范

96。防火墙的部署(B）

（A)只需要在与Internet 相连接的出入口设置

(B）在需要保护局域网络的所有出入口设置

（C）需要在出入口和网段之间进行部署

97.防火墙是一个（A)

（A)分离器、限制器、分析器

（B)隔离器、控制器、分析器

（C)分离器、控制器、解析器

98。目前的防火墙防范主要是（B）

(A)主动防范

(B)被动防范

（C）不一定

99。目前的防火墙防范主要是（B)

（A)主动防范

(B)被动防范

（C）不一定

100。IP地址欺骗通常是(A)

(A）黑客的攻击手段

(B)防火墙的专门技术

(C）IP 通讯的一种模式

101。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?(C）

（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

102）现代主动安全防御的主要手段是（A）

A>探测、预警、监视、警报

B>嘹望、烟火、巡更、敲梆

C>调查、报告、分析、警报

103）古代主动安全防御的典型手段有（B）

A>探测、预警、监视、警报

B〉嘹望、烟火、巡更、敲梆

C>调查、报告、分析、警报

（104)．计算机信息系统，是指由（B ）及其相关的和配套的设备、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。

A．计算机硬件

B．计算机

C．计算机软件

D．计算机网络

（105)．计算机信息系统的安全保护，应当保障（A ），运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行.

A．计算机及其相关的和配套的设备、设施(含网络）的安全

B．计算机的安全

C．计算机硬件的系统安全

D．计算机操作人员的安全

（106）．当前奇瑞股份有限公司所使用的杀毒软件是：（C ） 。

A 瑞星企业版

B卡巴斯基

C 趋势防病毒网络墙

D 诺顿企业版

（107）．计算机病毒是指：（C ）

A .带细菌的磁盘

B. 已损坏的磁盘

C。 具有破坏性的特制程序

D。被破坏了的程序

（108）．计算机连网的主要目的是\_\_\_\_A\_\_\_\_\_\_\_\_\_\_。

A资源共享

B．共用一个硬盘

C．节省经费

D．提高可靠性

(109）．关于计算机病毒知识，叙述不正确的是D

A . 计算机病毒是人为制造的一种破坏性程序

B 。 大多数病毒程序具有自身复制功能

C. 安装防病毒卡,并不能完全杜绝病毒的侵入

D. 不使用来历不明的软件是防止病毒侵入的有效措施

（110）．公司USB接口控制标准：院中心研发部门（ A ），一般职能部门( A ）。

A 2% 5%

B 4% 10％

Ｃ 5％　10％

D 2％ 4%。

（111）．木马程序一般是指潜藏在用户电脑中带有恶意性质的 A ，利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息。

A 远程控制软件

B 计算机操作系统

C 木头做的马

（112） 。为了防止各种各样的病毒对计算机系统造成危害，可以在计算机上安装防病毒软件，并注意及时 B ，以保证能防止和查杀新近出现的病毒。

A 分析

B 升级

C 检查

（113). 局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样，则（ C ）。

A 两台计算机都正常

B 两台计算机都无法通讯

C 一台正常通讯一台无法通讯

（114）。同一根网线的两头插在同一交换机上会（ A )。

A 网络环路

B 根本没有影响

Ｃ　短路

D 回路

（115）企业重要数据要及时进行（　C　），以防出现以外情况导致数据丢失。

Ａ杀毒

Ｂ加密

Ｃ备份

（116).WINDOWS主机推荐使用（ A）格式

A NTFS

B FAT32

C FAT

D LINUX

117。 计算机网络是地理上分散的多台（C）遵循约定的通信协议，通过软硬件互联的系统。

A。 计算机

B。 主从计算机

C. 自主计算机

D。 数字设备

118. 密码学的目的是（C）。

A. 研究数据加密

B. 研究数据解密

C. 研究数据保密

D. 研究信息安全

119。 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（A)。

A。 对称加密技术

B. 分组密码技术

C。 公钥加密技术

D. 单向函数密码技术

120. 网络安全最终是一个折衷的方案，即安全强度和安全操作代价的折衷,除增加安全设施投资外，还应考虑（D）.

A。 用户的方便性

B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持

D。 上面3项都是

121．A方有一对密钥（KA公开，KA秘密）,B方有一对密钥（KB公开,KB秘密），A方向B方发送数字签名M，对信息M加密为：M’= KB公开(KA秘密(M））。B方收到密文的解密方案是（C）。

A。 KB公开（KA秘密（M’))

B. KA公开（KA公开（M’）)

C。 KA公开（KB秘密(M'）)

D。 KB秘密(KA秘密(M’））

122。 “公开密钥密码体制”的含义是（C）。

A. 将所有密钥公开

B。 将私有密钥公开，公开密钥保密

C。 将公开密钥公开，私有密钥保密

D。 两个密钥相同

123。 PKI支持的服务不包括（D）。

A. 非对称密钥技术及证书管理

B. 目录服务

C。 对称密钥的产生和分发

D. 访问控制服务

124。 PKI的主要组成不包括(B)。

A。 证书授权CA

B. SSL

C。 注册授权RA

D。 证书存储库CR

125. PKI管理对象不包括(A）。

A。 ID和口令

B. 证书

C。 密钥

D. 证书撤消

126. 下面不属于PKI组成部分的是（D)。

A. 证书主体

B. 使用证书的应用和系统

C. 证书权威机构

D。 AS

127。 SSL产生会话密钥的方式是(C）。

A。 从密钥管理数据库中请求获得

B。 每一台客户机分配一个密钥的方式

C。 随机由客户机产生并加密后通知服务器

D。 由服务器产生并分配给客户机

128。属于Web中使用的安全协议(C）。

A. PEM、SSL

B。 S—HTTP、S/MIME

C. SSL、S—HTTP

D. S/MIME、SSL

129。 传输层保护的网络采用的主要技术是建立在（A）基础上的（A)。

A. 可靠的传输服务，安全套接字层SSL协议

B。 不可靠的传输服务，S-HTTP协议

C. 可靠的传输服务， S-HTTP协议

D. 不可靠的传输服务，安全套接字层SSL协议

130. 通常所说的移动VPN是指（A）。

A。 Access VPN

B. Intranet VPN

C。 Extranet VPN

D. 以上皆不是

131。 属于第二层的VPN隧道协议有(B)。

A。 IPSec

B。 PPTP

C。GRE

D。 以上皆不是

132. GRE协议的乘客协议是(D）。

A. IP

B. IPX

C. AppleTalk

D。 上述皆可

133 VPN的加密手段为（C）.

A. 具有加密功能的防火墙

B. 具有加密功能的路由器

C. VPN内的各台主机对各自的信息进行相应的加密

D。 单独的加密设备

134. 将公司与外部供应商、客户及其他利益相关群体相连接的是（B)。

A。 内联网VPN

B. 外联网VPN

C. 远程接入VPN

D。 无线VPN

135. PPTP、L2TP和L2F隧道协议属于(B)协议。

A. 第一层隧道

B. 第二层隧道

C. 第三层隧道

D. 第四层隧道

136．不属于隧道协议的是（C）。

A. PPTP

B. L2TP

C。 TCP/IP

D. IPSec

137.不属于VPN的核心技术是(C)。

A。 隧道技术

B. 身份认证

C. 日志记录

D. 访问控制

138．目前，VPN使用了（A)技术保证了通信的安全性。

1. 隧道协议、身份认证和数据加密
2. 身份认证、数据加密
3. 隧道协议、身份认证
4. 隧道协议、数据加密

139。（A）通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部

网的远程访问。

A。 Access VPN

B。 Intranet VPN

C. Extranet VPN

D. Internet VPN

140．L2TP隧道在两端的VPN服务器之间采用（A）来验证对方的身份。

A。 口令握手协议CHAP

B。 SSL

C。 Kerberos

D. 数字证书

141．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0。5，则k约等于＿＿。B

A．2128

B．264

C．232

D．2256

142．Bell—LaPadula模型的出发点是维护系统的＿＿＿，而Biba模型与Bell—LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题.它们存在共同的缺点:直接绑定主体与客体，授权工作困难。C

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

143、口令破解的最好方法是（B）

A暴力破解

B组合破解

C字典攻击

D生日攻击

144、杂凑码最好的攻击方式是（D）

A 穷举攻击

B中途相遇

C字典攻击

D生日攻击

145、可以被数据完整性机制防止的攻击方式是（D）

A假冒\*\*＊

B抵赖\*\*＊\*

C数据中途窃取

D数据中途篡改

146、会话侦听与劫持技术属于（B）技术

A密码分析还原

B协议漏洞渗透

C应用漏洞分析与渗透

D DOS攻击

147、PKI的主要组成不包括(B）

A CA

B SSL

C RA

D CR

148.恶意代码是（指没有作用却会带来危险的代码D)

A 病毒\*\*\*

B 广告\*＊＊

C间谍\*＊

D 都是

149.社会工程学常被黑客用于（踩点阶段信息收集A)

A 口令获取

B ARP

C TCP

D DDOS

150.windows中强制终止进程的命令是（C）

A Tasklist

B Netsat

C Taskkill

D Netshare

151.现代病毒木马融合了（D)新技术

A 进程注入

B注册表隐藏

C漏洞扫描

D都是

152。溢出攻击的核心是(A）

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

153.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外部网络

D自由连接

多选题

（1）网络安全工作的目标包括(ABCD)  
A、信息机密性;

B、信息完整性；

C、服务可用性;

D、可审查性

(2)智能卡可以应用的地方包括（ABCD）  
A、进入大楼；

B、使用移动电话；

C、登录特定主机;

D、执行银行和电子商务交易

（3)计算机信息系统安全保护的目标是要保护计算机信息系统的(ABCD)

（A）实体安全

(B）运行安全

(C)信息安全

(D)人员安全

(4)计算机信息系统的运行安全包括(ABC)

（A)系统风险管理

(B)审计跟踪

(C）备份与恢复

（D）电磁信息泄漏

(5)实施计算机信息系统安全保护的措施包括（AB）

（A）安全法规

(B)安全管理

（C）组织建设

(D）制度建设

（6）计算机信息系统安全管理包括(ACD)

（A）组织建设

（B)事前检查

（C）制度建设

（D）人员意识

(7)公共信息网络安全监察工作的性质（ABCD）

(A)是公安工作的一个重要组成部分

（B）是预防各种危害的重要手段

(C)是行政管理的重要手段

（D)是打击犯罪的重要手段

(8）公共信息网络安全监察工作的一般原则（ABCD)

（A）预防与打击相结合的原则

（B）专门机关监管与社会力量相结合的原则  
(C)纠正与制裁相结合的原则

（D）教育和处罚相结合的原则

（9)安全员应具备的条件: （ABD）

(A）具有一定的计算机网络专业技术知识

(B)经过计算机安全员培训，并考试合格  
(C)具有大本以上学历

（D）无违法犯罪记录

（10)网络操作系统应当提供哪些安全保障（ABCDE）

（A)验证（Authentication)

（B）授权(Authorization）  
（C)数据保密性（Data Confidentiality）

（D）数据一致性(Data Integrity)  
（E）数据的不可否认性（Data Nonrepudiation)

（11）Windows NT的"域"控制机制具备哪些安全特性？（ABC)

(A）用户身份验证

（B)访问控制  
（C)审计(日志）

（D）数据通讯的加密

（12）从系统整体看，安全”漏洞”包括哪些方面（ABC)

（A)技术因素

(B）人的因素

（C）规划,策略和执行过程

（13）从系统整体看,下述那些问题属于系统安全漏洞(ABCDE)

（A)产品缺少安全功能

（B)产品有Bugs

(C)缺少足够的安全知识

（D）人为错误

(E)缺少针对安全的系统设计

(14）应对操作系统安全漏洞的基本方法是什么？(ABC）

（A)对默认安装进行必要的调整

(B)给所有用户设置严格的口令

（C)及时安装最新的安全补丁

（D)更换到另一种操作系统

(15）造成操作系统安全漏洞的原因(ABC)

（A）不安全的编程语言

(B）不安全的编程习惯

(C)考虑不周的架构设计

（16）严格的口令策略应当包含哪些要素(ABCD)

（A）满足一定的长度，比如8位以上

(B)同时包含数字，字母和特殊字符  
（C）系统强制要求定期更改口令

(D）用户可以设置空口令

(17）计算机安全事件包括以下几个方面(ABCD）

(A)重要安全技术的采用

（B)安全标准的贯彻  
(C)安全制度措施的建设与实施

（D）重大安全隐患、违法违规的发现，事故的发生

（18）计算机案件包括以下几个内容(ABC）

(A)违反国家法律的行为

(B)违反国家法规的行为  
（C)危及、危害计算机信息系统安全的事件

（D）计算机硬件常见机械故障

（19)重大计算机安全事故和计算机违法案件可由\_\_\_\_\_受理(AC)

（A）案发地市级公安机关公共信息网络安全监察部门

（B)案发地当地县级（区、市）公安机关治安部门  
(C）案发地当地县级（区、市）公安机关公共信息网络安全监察部门

(D）案发地当地公安派出所

(20）现场勘查主要包括以下几个环节\_\_\_\_\_(ABCD）

(A）对遭受破坏的计算机信息系统的软硬件的描述及被破坏程度

（B)现场现有电子数据的复制和修复  
(C）电子痕迹的发现和提取，证据的固定与保全

(D）现场采集和扣押与事故或案件有关的物品

(21)计算机安全事故原因的认定和计算机案件的数据鉴定，\_\_\_\_ （ABC）

（A)是一项专业性较强的技术工作

（B)必要时可进行相关的验证或侦查实验  
(C）可聘请有关方面的专家，组成专家鉴定组进行分析鉴定

（D）可以由发生事故或计算机案件的单位出具鉴定报告

（22)有害数据通过在信息网络中的运行，主要产生的危害有（ABC)

（A）攻击国家政权,危害国家安全

（B）破坏社会治安秩序

(C)破坏计算机信息系统，造成经济的社会的巨大损失

（23）计算机病毒的特点\_\_\_\_\_\_（ACD)

（A)传染性

（B)可移植性

（C）破坏性

(D)可触发性

（24)计算机病毒按传染方式分为\_\_\_\_(BCD）

（A）良性病毒

(B）引导型病毒

(C）文件型病毒

(D)复合型病毒

（25）计算机病毒的危害性有以下几种表现(ABC）

（A）删除数据

(B)阻塞网络

（C）信息泄漏

（D)烧毁主板

（26)计算机病毒由\_\_\_\_\_部分组成(ABD)

(A）引导部分

(B）传染部分

（C)运行部分

（D)表现部分

（27)以下哪些措施可以有效提高病毒防治能力(ABCD）

（A)安装、升级杀毒软件

(B)升级系统、打补丁

(C)提高安全防范意识

（D）不要轻易打开来历不明的邮件

（28)计算机病毒的主要传播途径有(ABCD)

（A)电子邮件

（B）网络

（C）存储介质

(D）文件交换

（29）计算机病毒的主要来源有\_\_\_\_(ACD）

（A）黑客组织编写

(B)计算机自动产生

（C）恶意编制

（D）恶作剧

（30）发现感染计算机病毒后,应采取哪些措施(ABC)

（A)断开网络

（B）使用杀毒软件检测、清除  
(C）如果不能清除，将样本上报国家计算机病毒应急处理中心

(D）格式化系统

填空：

1． 信息安全包含:\_\_物理\_\_\_\_安全、\_\_\_\_信息系统\_\_\_\_\_\_\_\_安全和\_\_数据\_安全。

2. 数据安全包含\_\_\_可用性\_、\_\_\_\_完整性\_\_、\_\_\_保密性\_三个基本特性.

2．公司对电脑密码的强壮度要求是：\_字母加数字组合8位以上\_\_\_\_。

3．员工离开自己的计算机时要立即设置\_\_\_锁屏\_\_\_\_\_\_\_\_\_.

4。信息安全四大要素是：\_\_技术、\_\_\_制度、流程、\_\_\_人\_。

5.未来信息安全的发展趋势是由\_\_\_\_\_防外\_转变为\_\_\_\_\_防内\_\_\_\_。

6。 新修订《刑法》中有关失泄密处罚条款：以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的，给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金;造成特别严重后果的,处三年以上\_\_七\_\_年以下有期徒刑，并处罚金

7.工作人员因工作需要必须使用Internet时,需由各部门信息化管理员提交\_\_\_OA\_\_申请.

8.密码系统包括以下4个方面:明文空间、密文空间、密钥空间和密码算法。

9。解密算法D是加密算法E的 逆运算 .

10。常规密钥密码体制又称为 对称密钥密码体制 ,是在公开密钥密码体制以前使用的密码体制。

11.如果加密密钥和解密密钥 相同 ,这种密码体制称为对称密码体制。

12.DES算法密钥是 64 位,其中密钥有效位是 56 位。

13.RSA算法的安全是基于 分解两个大素数的积 的困难。

14.公开密钥加密算法的用途主要包括两个方面：密钥分配、数字签名。

15。消息认证是 验证信息的完整性 ，即验证数据在传送和存储过程中是否被篡改、重放或延迟等。

16.MAC函数类似于加密,它于加密的区别是MAC函数 不 可逆。

.大学生小吴在网上以一个知名作家的名义写博客,但事先没有征得该作家同意。小吴应当承担(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.侵权责任

B.违约责任

C.刑事责任

D.行政责任

2.绿色上网软件可以安装在家庭和学校的

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。电视机上

B。个人电脑上

C.电话上

D。幻灯机上

3.以下有关秘钥的表述，错误的是()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。密钥是一种硬件

B。密钥分为对称密钥与非对称密钥

C。对称密钥加密是指信息的发送方和接收方使用同一个密钥去加密和解密数据

D。非对称密钥加密需要使用不同的密钥来分别完成加密和解密操作

4。浏览网页时,遇到的最常见的网络广告形式是(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。飘移广告

B。旗帜广告

C。竞价广告

D。邮件列表

5。下列选项中，不属于个人隐私信息的是（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.恋爱经历

B.工作单位

C。日记

D。身体健康状况

6。根据《互联网上网服务营业场所管理条例》,网吧每日营业时间限于（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。6时至24时

B.7时至24时

C。8时至24时

D。9时至24时

7。李某将同学张某的小说擅自发表在网络上,该行为（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。不影响张某在出版社出版该小说，因此合法

B.侵犯了张某的著作权

C。并未给张某造成直接财产损失，因此合法

D.扩大了张某的知名度,应该鼓励

8.在设定网上交易流程方面，一个好的电子商务网站必须做到（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。对客户有所保留

B。不论购物流程在网站的内部操作多么复杂，其面对用户的界面必须是简单和操作方便的

C。使客户购物操作繁复但安全

D.让客户感到在网上购物与在现实世界中的购物流程是有区别的

9.我国出现第一例计算机病毒的时间是（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.1968年

B。1978年

C.1988年

D。1998年

10。表演者对其表演享有许可他人通过网络向公众传播其表演并获得报酬的权利.该权利的保护期限是（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。50年

B.60年

C.30年

D.没有期限

11.国际电信联盟将每年的5月17日确立为世界电信日.2014年已经是第46届,其世界电信日的主题为（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。“让全球网络更安全”

B。“信息通信技术：实现可持续发展的途径"

C.“行动起来创建公平的信息社会"

D.“宽带促进可持续发展"

12。下列有关隐私权的表述，错误的是(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。网络时代,隐私权的保护受到较大冲击

B。虽然网络世界不同于现实世界，但也需要保护个人隐私

C。由于网络是虚拟世界,所以在网上不需要保护个人的隐私

D。可以借助法律来保护网络隐私权

13.在原告起诉被告抢注域名案件中，以下不能判定被告对其域名的注册、使用具有恶意的是()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。为商业目的将他人驰名商标注册为域名的

B.为商业目的注册与原告的域名近似的域名,故意造成与原告网站的混淆，误导网络用户访问其网站的

C.曾要约高价出售其域名获取不正当利益的

D。注册域名后自己准备使用的

14。根据《治安管理处罚法》的规定，煽动民族仇恨、民族歧视,或者在出版物、计算机信息网络中刊载民族歧视、侮辱内容的，处10日以上15日以下拘留，可以并处()以下罚款。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。500元

B.1000元

C。3000元

D.5000元

15。关于网络游戏的经营规则,下列说法错误的是（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。网络游戏运营企业应当要求网络游戏用户使用有效身份证件进行实名注册

B.网络游戏运营企业终止运营网络游戏应当提前60日予以公告

C。我国对国产网络游戏实行备案制

D。我国对进口网络游戏实行备案制

二、多选题

1.“三网合一”的“三网”是指（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.电信网

B.有线电视网

C。计算机网

D.交换网

2.未经权利人许可，不得将其作品或录音制品上传到网上和在网上传播.这里的权利人包括()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.版权所有人

B。表演者

C。录音制品制作者

D.网站管理者

3.下列有关局域网的说法,正确的是（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.局域网是一种通信网

B.连入局域网的数据通信设备只包括计算机

C。局域网覆盖有限的地理范围

D.局域网具有高数据传输率

4.用户可设置的文件的属性有（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.只写

B。隐藏

C。存档

D。只读

5.下列属于网络服务提供者的是(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.网络接入服务提供者

B.网络空间提供者

C.搜索引擎服务提供者

D。传输通道服务提供者

6。多媒体计算机可以处理的信息类型有(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.文字

B.图形

C.数字

D.音频视频

7。乳业巨头甲公司为了打击竞争对手乙公司,雇佣公关公司在网络上大肆宣传虚假事实,称乙公司生产的牛奶中含有违禁添加剂,造成乙公司巨大损失。对此,以下观点正确的是（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。该行为可能涉嫌犯罪

B.该行为属于不正当竞争行为

C。针对这一犯罪只处罚个人

D.公关公司直接责任人员无需承担刑事责任

8。国家机关及其工作人员在对履行职责中知晓的公民个人电子信息，应当(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。予以封存

B.予以保密

C。不得泄露、篡改、毁损

D。可以提供给第三人

9.网络服务提供者收集和使用个人信息应当符合的条件有（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。告知权利人

B。明示收集、使用信息的目的、方式和范围

C。经被收集者同意

D.经监督管理机构许可或备案

10.按照刑法学的分类,网络犯罪可以被分为纯正的计算机犯罪和不纯正的计算机犯罪。纯正的计算机犯罪指针对计算机信息系统本身的犯罪;不纯正的计算机犯罪是指将计算机信息系统作为实施传统犯罪的犯罪工具的行为.下列行为中，属于不纯正的计算机犯罪的有(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.盗卖他人的游戏“武器装备”,致他人损失巨大

B.侵入高校网站大批量更改学历信息，从而为他人办理假学历获利

C。在网上大肆散播邪教的教义,发展邪教组织

D.传播木马软件,致使大量网站瘫痪

11。下列选项中，构成网络信息违法犯罪行为，公民和其他组织有权向有关主管部门举报、控告的是()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.窃取公民个人的电子信息

B。出售公民的个人电子信息

C.为配合公安机关办案需要,披露犯罪嫌疑人的电子信息

D.将公民个人电子信息提供给第三人

12。对于网络用户利用网络服务实施侵权行为的，以下表述正确的是()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施

B.网络服务提供者接到通知后应采取必要措施

C。网络服务提供者接到通知后未及时采取必要措施的，应承担法律责任

D。网络服务提供者只是提供平台服务,不承担法律责任

13.网络谣言有可能侵犯他人的（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.知情权

B。公平竞争权

C.财产权

D。人身权

14.以下对电子邮件的表述，正确的是()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.通讯双方必须都在场

B.邮件比人工邮件传送迅速、可靠且范围更广

C。邮件可以同时发送给多个用户

D.电子邮件中可以发送文字、图像、语音等信息

15.在电子商务条件下,卖方应当承担的义务有(）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。按照合同的规定提交标的物及单据

B。对标的物的权利承担担保义务

C.对标的物的质量承担担保义务

D。对标的物验收的义务

16.威胁网络安全的主要因素有()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.自然灾害

B。意外事故

C.计算机犯罪

D。“黑客"行为

17。以下关于非对称密钥的说法，正确的是()

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。加密密鈅对是用公钥来加密私钥来解密

B。签名密钥对是用私钥来加密公钥来解密

C.加密密鈅对是用私钥来加密公钥来解密

D。签名密钥对是用公钥来加密私钥来解密

18.计算机指令格式基本结构的两部分为（)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。操作码

B。数据码

C.地址码

D.控制码

19.互联网接入服务提供者应当记录上网用户的信息有（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A。上网时间

B.用户帐号

C.用户密码

D.互联网地址

20.下列有关即时通讯工具服务提供者的说法,正确的是（）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A.即时通信工具服务提供者无需取得相关资质

B.即时通信工具服务提供者应当遵循“后台实名、前台自愿”的原则

C.即时通信工具服务提供者应当对可以发布或转载时政类新闻的公众账号加注标识

D.即时通信工具服务使用者为从事公众信息服务活动开设公众账号，应当经即时通信工具服务提供者审核

三、判断题

1。在管理体系中，培训管理是确保信息系统安全的前提。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

2.计算机良性病毒是不破坏计算机的数据或程序。它是一种只占用计算机资源来执行而不会导致计算机系统瘫痪的计算机病毒。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

3.在域名中，WWW是指万维网。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

4。公钥密码比传统密码更安全.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

5。某人续写他人享有著作权的网络小说，并发表在盈利网站,此种行为没有侵犯原作者的权益.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

6.PKI(Public Key Infrastructure）是利用公钥原理和技术实施和提供安全服务的具有普适性的安全基础设施.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

7。一但中了IE窗口炸弹马上按下主机面板上的Reset键，重起计算机。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

8.李某将同学张某的小说擅自发表在网络上，该行为如果不影响张某在出版社出版该小说,就是合法的。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

9.在网络环境下，未经版权所有人、表演者和录音制品制作者的许可，可以将其作品或录音制品上传到网上和在网上传播。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

10。对于重要的计算机系统，更换操作人员时,应令原操作员迅速交出掌握的各种技术资料、磁盘等存储器件，同时改变系统的口令密码。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

11.在一所大学里,每个学院都有自己的局域网，连接各个学院的校园网也是局域网.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

12。屏幕保护的密码是需要分大小写的。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

13。中学、小学校园周围200米范围内不得设立网吧。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

14。被侵权人与网络服务提供者达成的一方支付报酬,另一方提供删除、屏蔽、断开链接等服务的协议,人民法院应认定无效。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

15.链路加密是对相邻节点之间的链路上所传输的数据进行加密。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对

错

**网络安全知识竞赛题库**

一、单选题

1、网页恶意代码通常利用（ C ）来实现植入并进行攻击。

A、 口令攻击

B、 U盘工具

C、 IE浏览器的漏洞

D、 拒绝服务攻击

2、要安全浏览网页，不应该( A ）.

A、 在他人计算机上使用“自动登录”和“记住密码”功能

B、 禁止使用Active（错)控件和Java 脚本

C、 定期清理浏览器Cookies

D、 定期清理浏览器缓存和上网历史记录

3、用户暂时离开时，锁定Windows系统以免其他人非法使用。锁定系统的快捷方式为同时按住( ) 。

A、 WIN键和Z键

B、 F1键和L键

C、 WIN键和L键

D、 F1键和Z键

4、网站的安全协议是https时,该网站浏览时会进行（ D )处理.

A、 口令验证B、 增加访问标记C、 身份验证D、 加密

6、为了防范垃圾电子邮件，互联网电子邮件服务提供者应当按照信息产业部制定的技术标准建设互联网电子邮件服务系统，电子邮件服务器（ C ）匿名转发功能。

A、使用 B、开启 C、关闭

7、互联网电子邮件服务提供者对用户的( A )和互联网电子邮件地址负有保密的义务。

A、个人注册信息 B、收入信息 C、所在单位的信息

8、任何组织或个人不得利用互联网电子邮件从事传播淫秽色情信息、窃取他人信息或者等违法犯罪活动,否则构成犯罪的,依法追究刑事责任，尚不构成犯罪的，由公安机关等依照有关法律、行政法规的规定予以处罚；电信业务提供者从事上述活动的，并由电信管理机构依据( A ）有关行政法规处罚.

A、故意传播计算机病毒 B、发送商业广告 C、传播公益信息

11、如果您发现自己被手机短信或互联网站上的信息诈骗后，应当及时向（ C )报案，以查处诈骗者,挽回经济损失.

A、消费者协会 B、电信监管机构 C、公安机关

12、为了有效抵御网络黑客攻击，可以采用作为安全防御措施. （ C )

A、绿色上网软件 B、杀病毒软件 C、防火墙

13、按照《互联网电子公告服务管理规定》，任何人不得在互联网上的电子布告牌(BBS）、电子白板、电子论坛、( B )、留言板等电子公告服务系统中发布淫秽、色情、赌博、暴力、恐怖等违法有害信息。

A、网站 B、网络聊天室 C、电子邮箱

14、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，这属于什么攻击类型？ (A）

A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

15、为了防御网络监听,最常用的方法是 （ B ）

A、采用物理传输（非网络) B、信息加密 C、无线网 D、使用专线传输

16、向有限的空间输入超长的字符串是哪一种攻击手段?（A）

A、缓冲区溢出 B、网络监听 C、拒绝服务 D、IP欺骗

17、主要用于加密机制的协议是(D）

A、HTTP B、FTP C、TELNET D、SSL

18、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？ ( B )

A、缓存溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDOS攻击

19、在以下认证方式中，最常用的认证方式是：（A)

A、基于账户名／口令认证 B、基于摘要算法认证

C、基于PKI认证 D、基于数据库认证

20、下列不属于系统安全的技术是( B ）

A、防火墙 ;B、加密狗 ；C、认证 ； D、防病毒

21、抵御电子邮箱入侵措施中,不正确的是（ D ）

A、不用生日做密码 B、不要使用少于5位的密码 C、不要使用纯数字 D、自己做服务器

22、不属于常见的危险密码是（ D ）

A、跟用户名相同的密码 B、使用生日作为密码 C、只有4位数的密码 D、10位的综合型密码

23、不属于计算机病毒防治的策略的是（ D )

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

25、当今IT 的发展与安全投入,安全意识和安全手段之间形成( B ）

A、安全风险屏障 B、安全风险缺口

C、管理方式的变革 D、管理方式的缺口

26、我国的计算机年犯罪率的增长是( C )

A、10% B、160％ C、60% D、300％

27、信息安全风险缺口是指（ A ）

A、IT 的发展与安全投入,安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行,维护的漏洞

D、计算中心的火灾隐患

28、网络攻击与防御处于不对称状态是因为( C )

A、管理的脆弱性 B、应用的脆弱性

C、网络软硬件的复杂性 D、软件的脆弱性

29、网络攻击的种类( A ）

A、物理攻击，语法攻击，语义攻击 B、黑客攻击，病毒攻击

C、硬件攻击，软件攻击 D、物理攻击,黑客攻击，病毒攻击

30、语义攻击利用的是（ A ）

A、信息内容的含义 B、病毒对软件攻击

C、黑客对系统攻击 D、黑客和病毒的攻击

31、计算机网络最早出现在哪个年代？ ( B ）

A、20世纪50年代 B、20世纪60年代

C、20世纪80年代 D、20世纪90年代

32、最早研究计算机网络的目的是什么?( C )

A、直接的个人通信； B、共享硬盘空间、打印机等设备；

C、共享计算资源； D、大量的数据交换。

33、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

34、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?（ C )

A、安装防火墙 B、安装入侵检测系统

C、给系统安装最新的补丁 D、安装防病毒软件

35、以网络为本的知识文明人们所关心的主要安全是（ C )

A、人身安全 B、社会安全 C、信息安全

47、第一次出现”HACKER"这个词是在（ B )

A、BELL实验室 B、麻省理工AI实验室 C、AT＆T实验室

36、可能给系统造成影响或者破坏的人包括（ A ）

A、所有网络与信息系统使用者 B、只有黑客 C、只有管理员

37、黑客的主要攻击手段包括( A ）

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

38、从统计的情况看,造成危害最大的黑客攻击是（ C ）

A、漏洞攻击 B、蠕虫攻击 C、病毒攻击

39、第一个计算机病毒出现在( B ）

A、40年代 B、70 年代 C、90年代

40、口令攻击的主要目的是( B ）

A、获取口令破坏系统 B、获取口令进入系统 C、仅获取口令没有用途

41、通过口令使用习惯调查发现有大约\_B的人使用的口令长度低于5个字符的

A、50、5% B、51、 5% C、52、5％

42、通常一个三个字符的口令破解需要( B )

A、18毫秒 B、18 秒 C、18分钟

43、邮件炸弹攻击主要是( B ）

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

44、逻辑炸弹通常是通过（ B ）

A、必须远程控制启动执行，实施破坏

B、指定条件或外来触发启动执行，实施破坏

C、通过管理员控制启动执行，实施破坏

45、扫描工具( C ）

A、只能作为攻击工具 B、只能作为防范工具

C、既可作为攻击工具也可以作为防范工具

46、黑客造成的主要安全隐患包括( A )

A、破坏系统、窃取信息及伪造信息

B、攻击系统、获取信息及假冒信息

C、进入系统、损毁信息及谣传信息

47、从统计的资料看,内部攻击是网络攻击的( B ）

A、次要攻击 B、最主要攻击 C、不是攻击源

48、一般性的计算机安全事故和计算机违法案件可由\_\_\_\_\_受理（ C ）

A、案发地市级公安机关公共信息网络安全监察部门

B、案发地当地县级（区、市）公安机关治安部门。

C、案发地当地县级(区、市）公安机关公共信息网络安全监察部门

D、案发地当地公安派出所

49、计算机刑事案件可由\_\_\_\_\_受理（ A )

A、案发地市级公安机关公共信息网络安全监察部门

B、案发地市级公安机关治安部门

C、案发地当地县级（区、市）公安机关公共信息网络安全监察部门

D、案发地当地公安派出所

50、计算机信息系统发生安全事故和案件，应当\_\_\_\_\_\_在内报告当地公安机关公共信息网络安全监察部门（ D ）

A、8小时 B、48小时 C、36小时 D、24小时

51、对计算机安全事故的原因的认定或确定由\_\_\_\_\_作出（ C ）

A、人民法院 B、公安机关 C、发案单位 D、以上都可以

52、对发生计算机安全事故和案件的计算机信息系统，如存在安全隐患的,

B 应当要求限期整改。

A、人民法院 B、公安机关 C、发案单位的主管部门 D、以上都可以

53、传入我国的第一例计算机病毒是( B )

A、大麻病毒 B、小球病毒 C、1575病毒 D、米开朗基罗病毒

54、我国是在＿＿年出现第一例计算机病毒( C ）

A、1980 B、1983 C、1988 D、1977

55、计算机病毒是( A ）

A、计算机程序 B、数据 C、临时文件 D、应用软件

56、1994年我国颁布的第一个与信息安全有关的法规是（ D )

A、国际互联网管理备案规定 B、计算机病毒防治管理办法

C、网吧管理规定 D、中华人民共和国计算机信息系统安全保护条例

57、网页病毒主要通过以下途径传播（ C ）

A、邮件 B、文件交换 C、网络浏览 D、光盘

58、故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，

后果严重的，将受到\_\_\_\_处罚( A )

A、处五年以下有期徒刑或者拘役 B、拘留 C、罚款 D、警告

59、计算机病毒防治产品根据\_\_\_\_标准进行检验（ A )

A、计算机病毒防治产品评级准测 B、计算机病毒防治管理办法

C、基于DOS系统的安全评级准则 D、计算机病毒防治产品检验标准

60、《计算机病毒防治管理办法》是在哪一年颁布的( C )

A、1994 B、1997 C、2000 D、1998

61、VPN是指( A ）

A、虚拟的专用网络 B、虚拟的协议网络 C、虚拟的包过滤网络

62、目前的防火墙防范主要是（ B )

A、主动防范 B、被动防范 C、不一定

63、IP地址欺骗通常是( A ）

A、黑客的攻击手段 B、防火墙的专门技术 C、IP 通讯的一种模式

黑客在攻击中进行端口扫描可以完成( D ）。

A、 检测黑客自己计算机已开放哪些端口

B、口令破译

C、 获知目标主机开放了哪些端口服务

D、截获网络流量

64、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?(C)

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

65、木马程序一般是指潜藏在用户电脑中带有恶意性质的 ( A )，利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息。

A、远程控制软件 B、计算机操作系统 C、木头做的马

66、为了防止各种各样的病毒对计算机系统造成危害,可以在计算机上安装防病毒软件，并注意及时 （ B ），以保证能防止和查杀新近出现的病毒.

A、 分析 B、 升级 C、检查

67、局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样,则（ C )。

A、两台计算机都正常

B、两台计算机都无法通讯

C、一台正常通讯一台无法通讯

68、企业重要数据要及时进行（ C )，以防出现以外情况导致数据丢失。

Ａ、杀毒 Ｂ、加密 Ｃ、备份

69、窃听是一种（ )攻击，攻击者（ ）将自己的系统插入到发送站和接收站之间。截获是一种（ ）攻击，攻击者（ )将自己的系统插入到发送站和接受站之间。（A）

A、 被动，无须，主动，必须

B、 主动,必须,被动，无须

C、 主动,无须,被动，必须

D、 被动,必须,主动,无须

70、可以被数据完整性机制防止的攻击方式是（D).

A、 假冒源地址或用户的地址欺骗攻击

B、 抵赖做过信息的递交行为

C、 数据中途被攻击者窃听获取

D、 数据在途中被攻击者篡改或破坏

71、王某,未经著作权人许可，以私服营运方式，通过信息网络向公众传播他人网络游戏软件，获利14万余元，其行为均构成（ A ）.

A、侵犯著作权罪 B、侵犯商业秘密罪

C、非法侵入计算机信息系统罪 D、非法经营罪

72、任何组织或者个人注册微博客账号，制作、复制、发布、传播信息内容的，应当使用（ A ），不得以虚假、冒用的居民身份信息、企业注册信息、组织机构代码信息进行注册。网站开展微博客服务，应当保证前款规定的注册用户信息真实.

A真实身份信息 B正确的网站信息 C真实的ID D工商注册信息

73、2010年年底，熊某偶尔登录到一个境外的淫秽网站，发现该网站有大量的淫秽图片及视频可以观看，便在该网站上注册成为会员。之后,熊某渐渐沉迷于这些淫秽图片和视频，不能自拔。为获得更大的浏览权限，熊某便陆续发了17篇包含淫秽信息的帖子共被点击查看29410次，以不断提高自身的会员等级。熊某的行为（ B ）

A不构成犯罪 B构成传播淫秽物品罪

C构成非法经营罪 D构成制作、复制、出版、贩卖、传播淫秽物品牟利罪

74、文艺青年张小五写了一部反映社会现实的小说，发表后引起热烈反响，好评如潮。甲网站觉得有利可图，擅自将该小说发布在网络上,供网民在线阅读.该网站侵犯了张小五的哪种著作权?（ B ）

A发表权 B信息网络传播权 C复制权 D发行权

75、著作权行政管理部门对侵犯互联网信息服务活动中的信息网络传播权的行为实施行政处罚，适用（ A )

A《著作权行政处罚实施办法》

B《互联网著作权行政保护办法》

C民法中关于知识产权的相关规定

D《商标法》

二、判断题

1、VPN的主要特点是通过加密使信息能安全的通过Internet传递。（对)

2、密码保管不善属于操作失误的安全隐患。（错）

3、漏洞是指任何可以造成破坏系统或信息的弱点.(对)

4、安全审计就是日志的记录。（错）

5、计算机病毒是计算机系统中自动产生的。（错）

6、对于一个计算机网络来说，依靠防火墙即可以达到对网络内部和外部的安全防护（错）

7、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（错）

8、最小特权、纵深防御是网络安全原则之一。（对）

9、安全管理从范畴上讲,涉及物理安全策略、访问控制策略、信息加密策略和网络安全管理策略。（对)

10、用户的密码一般应设置为16位以上.（对)

11、开放性是UNIX系统的一大特点.(对）

12、防止主机丢失属于系统管理员的安全管理范畴。（错)

13、我们通常使用SMTP协议用来接收E-MAIL。（错）

14、在堡垒主机上建立内部DNS服务器以供外界访问，可以增强DNS服务器的安全性。（错）

15、为了防御网络监听，最常用的方法是采用物理传输。(错）

16、使用最新版本的网页浏览器软件可以防御黑客攻击。（对)

17、通过使用SOCKS5代理服务器可以隐藏QQ的真实IP。（对）

18、一但中了IE窗口炸弹马上按下主机面板上的Reset键,重起计算机.（错）

19、禁止使用活动脚本可以防范IE执行本地任意程序。(对)

20、只要是类型为TXT的文件都没有危险.（错)

21、不要打开附件为SHS格式的文件。(对）

22、发现木马，首先要在计算机的后台关掉其程序的运行。(对）

23、限制网络用户访问和调用cmd的权限可以防范Unicode漏洞。（对）

24、解决共享文件夹的安全隐患应该卸载Microsoft网络的文件和打印机共享。(对）

25、不要将密码写到纸上.(对）

26、屏幕保护的密码是需要分大小写的。（对)

27、计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒.(对)

28、木马不是病毒。(对)

29．复合型防火墙防火墙是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用,同时也常结合过滤器的功能。（对）

30、非法访问一旦突破数据包过滤型防火墙,即可对主机上的软件和配置漏洞进行攻击.(错）

31、ATM 技术领先于TCP/IP技术，即将取代IP技术，实现语音、视频、数据传输网络的三网合一（错)

32、Internet设计之初，考虑了核战争的威胁，因此充分考虑到了网络安全问（错)

33、我的计算机在网络防火墙之内，所以其他用户不可能对我计算机造成威胁（错）

34、Internet没有一个集中的管理权威（对）

35、统计表明，网络安全威胁主要来自内部网络，而不是Internet（对）

36、只要设置了足够强壮的口令，黑客不可能侵入到计算机中(错）

37、路由器在转发IP分组时，一般不检查IP分组的源地址,因此可以伪造IP分组的源地址进行攻击,使得网络管理员无法追踪。（对）

38、发起大规模的DDoS攻击通常要控制大量的中间网络或系统(对）

39、路由协议如果没有认证功能，就可以伪造路由信息，导致路由表混乱，从而使网络瘫痪（对）

40、目前入侵检测系统可以及时的阻止黑客的攻击。（错）

41、TCSEC是美国的计算机安全评估机构和安全标准制定机构（对）

42、蠕虫、特洛伊木马和病毒其实是一回事(错）

43、只要选择一种最安全的操作系统，整个系统就可以保障安全（错）

44、在计算机系统安全中，人的作用相对于软件，硬件和网络而言，不是很重要（错）

45、在设计系统安全策略时要首先评估可能受到的安全威胁（对）

46、安装系统后应当根据厂商或安全咨询机构的建议对系统进行必要的安全配置（对）

47、系统安全的责任在于IT技术人员,最终用户不需要了解安全问题（错)

48．网络的发展促进了人们的交流，同时带来了相应的安全问题（错）

49．具有政治目的的黑客只对政府的网络与信息资源造成危害（错)

50、病毒攻击是危害最大、影响最广、发展最快的攻击技术(错）

51、黑色星期四”是因有人通过BELL实验室与Internet连接的有漏洞的机器上放置了一个蠕虫程序而引起网络灾难得名的（错)

52、邮件的附件如果是带有.exe、。com、.pif、。pl、。src和。vbs为后缀的文件,应确定其安全后再打开 (对)

53、在信息战中中立国的体现要比非信息战简单（错）

54、信息战的军事目标是指一个国家军队的网络系统、信息系统、数据资源（错)

55、计算机病毒是计算机系统中自动产生的（错）

56、小球病毒属于引导型病毒(对）

57、公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作（对）

58、计算机病毒防治产品实行销售许可证制度（对）

59、计算机病毒防治产品分为三级，其中三级品为最高级(错）

60，删除不必要的网络共享可以提高防范病毒的能力（对）

61、带VPN的防火墙一旦设置了VPN 功能，则所有通过防火墙的数据包都将

62、通过VPN通道进行通讯（错）

63、VPN的所采取的两项关键技术是认证与加密（对）

64、要保证一个公司总部与其分支机构的网络通讯安全只有通过VPN来实现（错）

65、网络安全工程实施的关键是质量，而质量的关键是服务的长期保障能力（对）

66、网络安全服务的开展与网络安全防范是一对矛盾（对)

67、网络安全边界防范的不完备性仅指防外不防内（错)

68、使用最新版本的网页浏览器软件可以防御黑客攻击。（错)

69、不要将密码写到纸上。（对)

70、计算机数据恢复在实际生活当中可以百分百恢复。（错）

71、违反国家法律、法规的行为,危及计算机信息系统安全的事件，称为计算机案件。（对）

72、计算机犯罪是行为人以计算机为工具或以计算机资产为犯罪对象实施的，依照我国刑法应受处罚的,具有社会危害性的行为。（对）

73、 计算机信息系统的安全威胁同时来自内、外两个方面. （对）

74、外单位人员如可以随意接入奇瑞公司内网.(错)

75、格式化过后的计算机，原来的数据就找不回来了(错）

问答题：

1、今年我国首届国家网络安全宣传周的主题是什么？

答案：共建网络安全，共享网络文明

2、罗定职业技术学院的官方网址是什么？

答案:www.ldpoly。com 和 www.ldptc.cn

3、罗定职业技术学院政务和公益机构域名是什么?

答案:罗定职业技术学院。公益

4、首次使用CRP数字校园、校园一卡通等信息系统时，为了保存自已的信息和财产安全应当怎么做?

答案:进入信息系统修改密码，并将其设置为一个复杂的密码。

5、计算机网络最突出的优点是什么？

答案:共享资源

6、信息安全有哪些常见的威胁?

答案：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。

7、解决互联网安全问题的根本条件是什么?

答案：提高整个社会网民的互联网道德本质.

8、什么是钓鱼网站？

答案：“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的URL地址以及页面内容，或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的HTML代码，以此来骗取用户银行或信用卡账号、密码等私人资料.

9、什么是网络安全？

答案：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续可靠正常地运行，网络服务不被中断.

10、什么是木马？

答案：木马是一种带有恶意性质的远程控制软件。木马一般分为客户端（client）和服务器端（server）。客户端就是本地使用的各种命令的控制台，服务器端则是要给别人运行，只有运行过服务器端的计算机才能够完全受控。木马不会像病毒那样去感染文件。

11、什么是后门？

答案：后门是指一种绕过安全性控制而获取对程序或系统访问权的方法.

12、防范网络黑客防措施有哪些？

答案：①选用安全的口令②口令不得以明文方式存放在系统中③建立帐号锁定机制④实施存取控制⑤确保数据的安全

13、网络病毒的来源有哪些?

答案：邮件附件、E-mail 、Web服务器、文件共享。

14、局域网内部若出现ARP攻击，会出现哪两种两句现象？

答案：1.不断弹出“本机的（错)（错）（错）段地址与网络中的(错）（错）(错）段地址冲突”的对话框。2。计算机不能正常上网，出现网络中断的症状.

15、控制USB接口使用的目的？

答案：1、网络的安全 2、信息的保密

16、什么是IP欺骗？

答案：攻击者可通过伪装成被信任源IP地址等方式来骗取目标主机的信任。

17、电子邮件存在哪些安全性问题？

1、垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷，影响网络传输速度,占用邮件服务器的空间。2、诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜,发信人能迅速让大量受害者上当。3、邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为,信箱不能承受时就会崩溃.4、通过电子邮件传播的病毒，大多数采用附件的形式夹带在电子邮件中。当收信人打开附件后，病毒会查询他的通讯簿,给其上所有或部分人发信，并将自身放入附件中，以此方式继续传播扩散.

18、什么是网络蠕虫？

答案：网络蠕虫是一种智能化、自动化，综合网络攻击、密码学和计算机病毒技术,无须计算机使用者干预即可运行的攻击程序或代码.

19、网络蠕虫有什么特征？

答案：具有病毒的特征，传染性，隐蔽性，破坏性;不利用文件寄生，可以主动传播，并且通过网络可快速传播，容易造成网络拥塞；具有智能化、自动化和高技术化；

20、防火墙的基本功能有哪些?

答案：1过滤进出网络的数据；2管理进出网络的访问行为；3封堵某些禁止的业务；4记录进出网络的信息和活动；5对网络的攻击进行将侧和报警.

21、因特网电子商务系统必须保证网络安全的四大要素是什么？

答案：1传输数据的保密性;2数据的完整性；3交易各方身份的真实性；

4交易的不可抵赖性；

21、对蠕虫病毒和一般病毒进行比较有什么区别？

答案：存在形式：普通病毒寄存在文件上，蠕虫病毒寄存在独立程序上;

传染机制：普通病毒在宿主程序上运行，蠕虫病毒会主动攻击;

传染目标：普通病毒传染本地文件，蠕虫病毒传染整个网络的计算机.

22、黑客攻击的动机都有哪些？

答案：1。好奇心理2.挑战性.3。报复心理4，经济利益5,政治目的，6.情报获取

23、什么是密码破解，有哪些方法？

答案：通过猜解或者直接破坏原密码的密码验证机制来达到和密码分析一样的最终效果，或者是密码对应的权限.

一般的密码破解大致分为以下几类。

1)使用软件无限次尝试密码.2）绕过密码验证机制。3）如果密码加密，使用替代密码代替原密码

24、后门程序与计算机病毒的差别是什么?

答案:后门程序又称特洛伊木马，其用途是潜伏在用户的计算机中，进行信息搜集或便于黑客进入。后门程序和计算机病毒最大的差别,在于后门程序不一定有自我复制的动作，即后门程序不一定会“感染”其他计算机.

25、黑客技术发展趋势是什么？

答案：（1）网络攻击的自动化程度和攻击速度不断提高（2)攻击工具越来越复杂(3）黑客利用安全漏洞的速度越来越快（4）防火墙被攻击者渗透的情况越来越多（5）安全威胁的不对称性在增加（6)攻击网络基础设施产生的破坏效果越来越大

26、什么是漏洞？

答案：漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷,从而可以使攻击者能够在未授权的情况下访问或破坏系统。

27、网络面临的安全威胁主要有哪些方面？

网络面临的安全威胁可分为两种：一是对网络数据的威胁；二是对网络设备的威胁。概括起来主要威胁包括以下几个方面：1）由自然力造成的非人为的数据丢失、设备失效、线路阻断。2）人为但属于操作人员无意的失误造成的数据丢失。3）来自外部和内部人员的恶意攻击和入侵。

28、IPv6先对IPv4有哪些优势?

IPv6优势：首先，IPv6解决了IP地址数量短缺的问题；其次，IPv6对IPv4协议中诸多不完善之处进行了较大的改进，在网络保密性、完整性方面作了更好的改进，在可控性和抗否认性方面有了新的保证。

29、计算机病毒传染的一般过程是什么?？

答案:1）判断传染目标（文件)是否符合感染条件（是否已经被感染）

2）若目标符合感染条件，则将病毒链接到传染目标的特点位置，并存入磁盘。

3）继续监视系统的运行，寻找新的传染目标

30、网络安全服务包括哪些？

答案:1、对等实体认证服务2、数据源点认证服务3数据保密服务4数据完整性服务5访问控制服务6可用性

1. 单选题  
   1.张某某出于好玩的心理入侵了关于国防事务的网站,但没有实施任何破坏行为。张某的行为()  
   A.不构成违法犯罪

**B.构成非法侵入计算机信息系统罪**

C.构成妨害公务罪

D.构成盗窃罪

2。小李开发了一款游戏外挂软件,让玩家不亲自进行游戏就可以让角色自动升级.对该软件，以下表述正确的是(）  
A.软件合法,小张享有著作权

B.软件合法,但小张不享有著作权

C。软件非法,但小张享有著作权   

**D.软件非法，小张不享有著作权**

3.以下有关防火墙的说法，不正确的是（）  
A。防火墙可是软件的，也可以是硬件的

B。防火墙可以用普通PC机安装包过滤软件来提供

C。防火墙虽然提供了一定的网络防护能力，但不能防止保护网内部的攻击

**D。防火墙可以查杀病毒**

4.符合条件的互联网新闻信息服务提供者实行特殊管理股制度,具体实施办法由哪个部门另行制定?  
 A。宣传部门    **B.国家互联网信息办公室**    C.公安局    D。法院

5。国家支持网络运营者之间在网络安全信息\_\_\_\_、\_\_\_\_、\_\_\_\_和\_\_\_\_\_\_\_\_等方面进行合作,提高网络运营者的安全保障能力。

A。收集 分析 管理 应急处置

**B.收集 分析 通报 应急处置**

C。发布 收集 分析 事故处理

D.审计 转发 处置 事故处理

6.下列以数字形式流通的货币是（）  
A.游戏币    **B.电子现金** C.现金   D.支票

7.下列表述中正确的是  
**A。发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施,按照规定及时告知用户并向有关主管部门报告**

B。在规定或者当事人约定的期限内,可以终止提供安全维护

C.网络产品、服务的提供者不需要为其产品、服务持续提供安全维护

D。网络产品、服务具有收集用户信息功能的,其提供者可以随意使用

8。信息网络安全的三个时代划分是()  
A.PC机时代、网络时代、信息时代

B.主机时代、 PC机时代、网络时代

**C.主机时代、专网时代、多网合一时代**

D.70年代、80年代、90年代

9。《互联网新闻信息服务管理规定》已经国家互联网信息办公室室务会议审议通过,现予公布，自(）起施行.  
 **A.2017/6/1**   B.2017/10/1    C.2016/6/1    D.2016/10/1

10。第一代计算机主要使用(）  
A。高级语言    **B。机器语言**     C。数据库管理系统    D。BASIC和FORTRAN

1. 统一域名争议解决机制的核心是强制性行政程序,只适用于以下( )情况  
   **A。因恶意注册域名侵害他人商标权而引发的域名纠纷**

B。因注册域名无效而引发的域名争议

C。因恶意注册域名侵害他人名誉权而引发的域名纠纷

D.因网站管理而引发的域名纠纷

12。绿色上网软件可以安装在家庭和学校的  
A。电视机上   B.电话上   **C.个人电脑上**    D.幻灯机上

13。网上银行系统的一次转账操作过程中发生了转账金额被非法篡改的行为，这破坏了信息安全的什么属性。  
**A。完整性**   B。保密性    C.不可否认性    D。可用性

14。计算机病毒防治产品检验标准时(）  
A.**计算机病毒防治产品检验标准**

B。计算机病毒防治管理办法

C.基于DOS系统的安全评级准则

**D。**计算机病毒防治产品评级准则

15。以下表述不属于计算机病毒防治策略的是（）  
**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

16。互联网新闻信息服务提供者应当设立什么职位,使其对互联网新闻信息内容负总责?  
A.站长   **B.总编辑**   C。记者    D。台长

17。“口令”是保证系统安全的一种简单而有效的方法.一个好的口令不应该  
**A。只使用小写字母**

B。混合使用大写字母和小写字母

C。混合使用标点符号和数字

D.混合使用字母和标的符合

18。在被保护网络与外部公共网之间用于访问控制和信息过滤的设备是（)  
A。交换机    **B。防火墙**   C.路由器    D.网桥

19.国家()负责统筹协调网络安全工作和相关监督管理工作。  
**A。网信部门**   B。公安部门    C.工业和信息化部门  D.通讯管理部门

20。下列不属于数据电文的是（）  
A.电子邮件    **B.书面合同**    C。微信    **D.**手机短信

1. 以下关于对称密钥加密的说法，正确的是(）  
   A.加密方和解密方可以使用不同的算法

B。加密密钥和解密密钥可以是不同的

**C.加密密钥和解密密钥必须是相同的**

D。密钥的管理非常简单

22.构成计算机物理实体的部件被称为（)  
A.计算机系统    **B.计算机硬件**    C.计算机软件    D。计算机程序

23.以下有关云计算的表达，不恰当的是()  
A。云计算是一种按使用量付费的模式

B。这种模式提供可用的、便捷的、按需的网络访问

C。云计算的可配置计算资源共享池包括网络、服务器、存储、应用软件、服务等资源

**D。云计算服务是通过卫星进行的数据服务**

24.访问控制是指确定(）以及实施访问权限的过程.  
**A。用户权限**

B.可给与哪些主体访问权限

C.可被用户访问的资源

D.系统是否遭受攻击

25。下列关于大数据的表述，不恰当地是（)  
A。大数据技术指的是所涉及的资料量规模巨大，至少1YB字节以上

B。大数据所指的数据量一般无法通过目前主流软件工具在合理时间内进行处理

**C。大数据的4V特点是指Volume（大量）、Velocity（高速）、Variety（多样）、value(价值）**

D.大数据最核心的价值就是在于对于海量数据进行存储和分析

26.以下防止用户被冒名所欺骗的方法是正确的是  
**A.对信息源发送方进行身份验证**

B.进行数据加密

C.对访问网络的流量进行过滤和保护

D。采用防火墙

27。《互联网直播服务管理规定》什么时候在全国实行  
 A。2016/6/1    **B.2016/12/1**    C.2017/3/1    D。2017/6/1

28.在德国卡尔斯鲁厄大学(Karlsruhe University)维纳•措恩（Werner Zorn）教授带领的科研小组的帮助下，王运丰教授和李澄炯博士等在北京计算机应用技术研究所(ICA）建成一个电子邮件节点，并向德国成功发出了一封电子邮件,邮件内容为“Across the Great Wall we can reach every corner in the world。（越过长城,走向世界)”。该邮件的发送时间为()  
  
**A.1987年**  B.1986年    C.1985年    D。1988年  
29。互联网直播服务提供者应当记录互联网直播服务使用者发布内容和日志信息,保存  
 A.30天    **B。60天**   C.100天    D。6个月

30.虚假恐怖信息是指以严重威胁公共安全的事件为内容,可能引起社会恐慌或者公共安全危机的不真实信息。以下不属于虚假**恐怖**信息的是（）  
A。虚假鼠疫信息   B.虚假地震信息  C。虚假劫持航空器信息  **D。虚假中奖信息**

1. 我国于（）年在刑法修订时新增加了非法侵入计算机信息系统罪。  
    **A。1997**  B.1999    C.1998    D.1996

32.为了有效抵御网络黑客攻击,可以采用（）作为安全防御措施。  
 A。绿色上网软件    B。杀病毒软件  **C.防火墙**   D.审计软件

33。微软公司于2014年4月8日后停止技术支持与更新服务的操作系统是（）  
 A.Windows 98    B。Windows 7    C.Windows 8    **D。Windows XP**

34.以下有关秘钥的表述,不正确的是(）  
**A.密钥是一种硬件**

B。密钥分为对称密钥与非对称密钥

C.对称密钥加密是指信息的发送方和接收方使用同一个密钥去加密和解密数据

D.非对称密钥加密需要使用不同的密钥来分别完成加密和解密操作

**？35.**某网站为黄色网站，有人向网站所在的服务器托管公司举报,请求关闭该网站。但服务器托管公司负责人认为，该网站每年上交3万多元的服务费,拒绝关闭该网站.张三的行为(）  
A.不构成犯罪  B。仅仅属于行政违法  C。构成包庇罪  D。构成传播淫秽物品牟利罪

36.从事危害网络安全的活动,或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助,尚不构成犯罪的，由公安机关没收违法所得,处（)日以下拘留,可以并处（)万元以上()万元以下罚款  
 **A.5 5 50**   B.5 10 50    C。10 5 50    D.10 10 50

37.密码学的目的是（）。  
A。研究数据加密   B.研究数据解密    **C.研究数据保密**    D。研究信息安全

38.木马程序一般是指潜藏在用户电脑中带有恶意性质的（）  
**A。远程控制软件**   B。计算机操作系统    C。游戏软件    D。视频播放器

39.以下说法不正确的是  
A.国务院相关管理部门依据职责对互联网直播服务实施相应监督管理。

B。**国家互联网信息办公室不负责全国互联网直播服务信息内容的监督管理执法工作。**

C。地方互联网信息办公室依据职责负责本行政区域内的互联网直播服务信息内容的监督管理执法工作。  

D.各级互联网信息办公室应当建立日常监督检查和定期检查相结合的监督管理制度,指导督促互联网直播服务提供者依据法律法规和服务协议规范互联网直播服务行为.

**？40.**世界上第一个计算机病毒出现在20世纪(）

A。60年代 **B.70 年代**  C。80年代 D。90年代

1. 多选题  
   1。下面关于安全员的表述,正确的有（）  
   **A。依据国家有关法规政策,从事本单位的信息网络安全保护工作,确保网络安全运行**

**B.隶属于本单位领导**

**C.向本单位的负责人提出改进计算机信息网络安全工作的意见和建议**

**D.在公安机关的指导下工作**

2。应用程序的安装方式有()  
**A。最小安装    B.完全安装    C.定制安装** D。最大安装

3。下列关于密码安全的描述，正确的是（）  
A。容易被他人记住的密码不安全

**B。相对而言，密码越长越安全**

**C.密码要定期更换**

**D.密码中使用的字符种类越多越不容易被猜中**

4.198、 重大计算机安全事故和计算机违法案件可由（)受理。  
**A.案发地市级公安机关公共信息网络安全监察部门**

**B。案发地当地县级(区、市）公安机关治安部门**

C。案发地当地县级（区、市）公安机关公共信息网络安全监察部门

D。案发地当地公安派出所

5。网络广告的特点有（）  
**A。快速准确    B.成本低廉    C。信息丰富**    D.不能保存

6。设立互联网上网服务营业场所，经营单位应具备的条件有()  
**A.有企业的名称、住所、组织机构和章程**

**B。有固定的网络地址和与其经营活动相适应的计算机等装置及附属设备**

**C.有健全、完善的信息网络安全管理制度和安全技术措施**

**D。有与其经营活动相适应的资金**

7.小方的极品游戏装备被盗，该装备被盗的原因是该游戏的软件确实存在漏洞,有被黑客攻击的可能性。小方不可以(）  
A.起诉该游戏公司

**B。自己也去盗别人的装备,补偿损失**

**C.发帖辱骂盗其装备的人**

**D.找到盗装备的人，并在他电脑中植入木马病毒**

8.下列选项中,收集网络个人信息资料声明应包括的主要内容有（）  
**A。收集网络个人信息资料目的的声明**

**B.网络个人信息资料的共享或再利用的声明**

**C。查阅、修正及更新网络个人信息资料的声明**

**D。网络个人信息资料的保护措施及隐私权保护政策链接的声明**

9.开展网络安全认证、检测、风险评估等活动需要向社会发布(）网络安全信息。  
**A.系统漏洞    B。计算机病毒    C。网络攻击    D。网络侵入**

10。以下操作中，**可以**清除文件型计算机病毒的是(）  
**A.删除感染计算机病毒的文件**

B。将感染计算机病毒的文件更名

**C.格式化感染计算机病毒的磁盘**

**D.用杀毒软件进行清除**

1. 单选题  
   1。吴某出于好玩的心理入侵了关于国防事务的网站，但没有实施任何破坏行为。吴某的行为()  
   A.不构成违法犯罪   **B.构成非法侵入计算机信息系统罪**   C.构成妨害公务罪    D.构成盗窃罪

2。非法获取计算机信息系统数据、非法控制计算机信息系统罪的犯罪主体是年满（)周岁并具有刑事责任能力的自然人。  
  
 A。10.0    **B。16.0**  C.14.0    D.18.0  
3。组建以太网时，通常都是用双绞线把若干台计算机连到一个中心的设备上,这个设备叫做（)  
  
 A.网络适配器    **B.集线器**  **C.服务器**   D。总线  
4.人和计算机下棋,这一应用属于()  
  
 A。过程控制    B.数据处理    C.科学计算    **D。人工智能**5.提供互联网新闻信息服务,还应当依法向()部门办理互联网信息服务许可或备案手续.  
  
 A。公安局   **B。电信主管部门**   C。消防部门    D。税务局  
6.(）是最常用的一类访问控制机制,用来决定一个用户是否有权访问一些特定客体的一种访问约束机制.  
  
 A.强制访问控制    B.访问控制列表    **C。自主访问控制**    D。访问控制矩阵  
7.网络安全工作的目标包括：  
 A。信息机密性   B。信息完整性  C。服务可用性    **D.以上都是**  
8.网络游戏防沉迷系统是一种旨在解决未成年人沉迷网络游戏的技术手段，未成年玩家如玩游戏时间超过3个小时的健康时间，游戏将会提出警示,并通过经验值减半、收益减半等方式促使玩家下线休息.这一系统开始在全国网络游戏中正式推广的时间是()  
  
**A.2005年**   B。2008年   **C。2007年**   D。2010年  
9.未经许可或超越许可范围开展互联网新闻信息服务活动的，由国家和省、自治区、直辖市互联网信息办公室依据职责责令停止相关服务活动,处多少罚款?  
  
 A。一万元以下   **B。一万元以上三万元以下**   C.三万元以上五万元以下    D。五万元以上  
10.国内第一家网上银行是(）  
A。中国农业银行网上银行    **B。招商银行网上银行**    C。中国银行网上银行    D。中国建设银行网上银行

11。甲冒充新闻工作者,以在新闻网站上发布隐私为要挟,向乙、丙、丁等人索取了数十万财物。甲的行为应当认定为（）  
  
 **A.敲诈勒索罪**   B。诈骗罪    C。招摇撞骗罪    D。寻衅滋事罪  
12。互联网直播服务提供者应当记录互联网直播服务使用者发布内容和日志信息,保存时长为?  
  
 A.一周    B。三十日   **C.六十日**    D.半年  
13.邮件炸弹攻击主要是(）  
  
 A。破坏被攻击者邮件服务器    B。破坏被攻击者邮件客户端    C.**填满被攻击者邮箱**    D。破坏被攻击者邮件文本  
14.《互联网新闻信息服务管理规定》已经国家互联网信息办公室室务会议审议通过,现予公布，自()起施行。  
  
 A。2016/6/1    B.2017/10/1   **C。2017/6/1**   D。2016/10/1  
15.申请互联网新闻信息传播平台服务许可的,国家和省、自治区、直辖市互联网信息办公室应当在规定期限内依法作出批准或不予批准的决定。省、自治区、直辖市互联网信息办公室应当自作出批准决定之日起（）工作日内,向国家互联网信息办公室报告有关情况。  
  
 A.12个    B。10个   **C.7个**    D。15个  
16。下列选项中,不属于系统软件的是（)  
 A.操作系统    **B.字处理程序**    C.语言处理程序    D.数据库管理系统  
17。统一域名争议解决机制的核心是强制性行政程序，只适用于(）  
  
**A。因恶意注册域名侵害他人商标权而引发的域名纠纷**    B。因注册域名无效而引发的域名争议    C.因恶意注册域名侵害他人名誉权而引发的域名纠纷  D。因网站管理而引发的域名纠纷  
18。数据库中存储的是（)  
  
A。数据之间的联系  B.数据 **C.数据以及数据之间的联系** D。数据模型  
19.通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务不包括互联网新闻信息  
 A。转载服务    B.采编发布服务    **C.公共服务**    D。传播平台服务  
20.非公有资本介入互联网新闻信息采编业务的，由国家和地方互联网信息办公室依据职责给予警告；情节严重或拒不改正的,暂停新闻信息更新，并处多少罚款?  
 A。一千元以下    B.一千元以上五千元以下    **C。五千元以上三万元以下**    D。三万元以上

1. 未经国家允许,在网上擅自发行、销售彩票的，如果构成犯罪，则罪名为（）  
   A。洗钱罪  B.赌博罪    **C.非法经营罪**    D。抢劫罪
2. 22。网上银行系统的一次转账操作过程中发生了转账金额被非法篡改的行为,这破坏了信息安全的( )属性。  
     
    A.不可否认性   B。保密性   **C.完整性**    D。可用性  
   23.《预防未成年人犯罪法》规定：“禁止在中小学附近开办营业性歌舞厅、营业性电子游戏场所以及其他未成年人不适宜进入的场所。”对此，下列认识不正确的是()  
     
    A.这有助于未成年人抵制不良诱惑    B。这有助于净化未成年人的成长环境    **C。这会抑制未成年人好奇心的发展**    D。这有助于未成年人健康成长  
   24。通常意义上的网络黑客是指通过互联网并利用非正常手段（）  
     
    A。上网的人    **B.入侵他人计算机系统的人**   C.在网络上行骗的人    D。在网络上卖东西的人  
   25.“口令”是保证系统安全的一种简单而有效的方法。一个好的口令不应该  
     
    **A。只使用小写字母**   B.混合使用大写字母和小写字母    C。混合使用标点符号和数字    D.混合使用字母和标的符合  
   26。世界上第一台计算机的名称是（）  
     
    A。IBM    B.APPLE    C.MAC   **D。ENIAC**27.商品按照顾客指定的时间和方式送到指定地点的活动,被称为（)  
     
    A.订单接收    B.在线订购    C。在线支付   **D.订单履行**28。向他人发送包含商业广告内容的互联网电子邮件时，应当在电子邮件标题的前部注明(）  
     
    A.“推销”字样    B.“商业信函”字样    **C。“广告”或“AD” 字样**    D。不用注明任何字样  
   29。网络安全在多网合一时代的脆弱性体现在  
     
    A。网络的脆弱性    B。软件的脆弱性   **C。管理的脆弱性**   D。应用的脆弱性  
   30.需报备的IP地址信息不包含()  
     
    A。备案单位基本情况    B。备案单位的IP地址来源信息    C。备案单位的IP地址分配使用信息    **D。备案单位对于IP地址的资金投入情况**31.方某利用网络获取某公司上网账号和密码后,以按月出租的方式提供给他人使用，从中获利5000元，给该公司造成数万元的巨大损失.方某的行为构成（)  
     
    **A.盗窃罪**   B.诈骗罪    C。侵占罪    D。非法经营罪  
   32.近几年，“天价烟"事件、“表哥"事件等频频被爆出,反映了网络在()方面具有巨大作用.  
     
   A.提高网民素质  B.增强智慧  **C.舆论监督**   D。学习交往  
   33.以下关于大数据的表述，不恰当地是(）  
   A。大数据技术指的是所涉及的资料量规模巨大,至少1YB字节以上

B。大数据所指的数据量一般无法通过目前主流软件工具在合理时间内进行处理

**C。大数据的4V特点是指Volume（大量）、Velocity(高速）、Variety(多样)、value(价值）**

D.大数据最核心的价值就是在于对于海量数据进行存储和分析

34。下列关于宏病毒的表述，正确的是()  
A。宏病毒主要感染可执行文件

B。宏病毒仅向办公自动化程序编制的文档进行传染

C。宏病毒主要感染U盘、硬盘的引导扇区或主引导扇区

**D.CIH病毒属于宏病毒**

35.语义攻击利用的是（)  
A.病毒对软件攻击B。黑客对系统攻击**C。信息内容的含义** D。黑客和病毒的攻击

36.互联网新闻信息服务提供者为用户提供互联网新闻信息传播平台服务，应当按照《中华人民共和国网络安全法》的规定,要求用户提供  
A。他人身份信息  B.网络身份信息 **C。真实身份信息** D。虚假身份信息

37.浏览网页时,遇到的最常见的网络广告形式是（)  
A。飘移广告   **B.旗帜广告**  C。竞价广告    D.邮件列表

38.为保护青少年健康成长,绿色上网软件可以自动过滤或屏蔽互联网上的(）  
A.网络游戏    B.网络聊天信息   **C。淫秽色情信息**    D。网络新闻信息  
39。最高人民法院于2014年10月9日发布了《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》,首次划定了个人信息保护的范围,涉及网络平台规避责任,有偿删帖,网络水军等多方面。这是()在互联网领域的具体化.  
A。科技兴国政策**B.依法治国政策** C。以德治国政策   D.四项基本原则

40。《互联网新闻信息服务许可证》有效期届满，需继续从事互联网新闻信息服务活动的，应当于有效期届满多长时间前申请续办?  
A.七天   **B。三十天**   C。两个月    D。三个月

1. 多选题  
   1.国家互联网信息办公室2015年2月4日发布《互联网用户账号名称管理规定》，规定指出，互联网信息服务使用者在(）等注册信息中不得出现违法和不良信息。  
     
    **A.头像    B。账号名称    C.简介**   D.签名  
   ？2.内部网需要防范的攻击有(）  
     
    A.间谍    B。盗窃    C.破坏系统    D.网络钓鱼  
   3.防火墙的作用有（)  
    **A。网络安全的屏障    B.可以强化网络安全策略    C。对网络存取和访问进行监控、审计**   D。防止内部信息的外泄

4.建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施(）

**A.同步规划    B。同步建设**   C.同步投运   **D.同步使用**5。以下不属于侵犯网络隐私权的情形有（)  
**A。用户在注册邮箱的时候,要求填写其个人联系方式和真实姓名**

**B.根据相关法律，在网络游戏进行注册的时候需要填写个人身份证号码以验证用户是否为成年人**

**C。张某想要开一家淘宝商店,淘宝要求商户注册的时候实名认证**

D。商家收集消费者的购物倾向，制定针对个别消费者的营销策略追求商业利益

6.下列有关计算机使用的说法，错误的是()  
**A。在买计算机时,一定要买最高档的**

**B.频繁开、关机对计算机的使用寿命并无影响**

**C。为防止计算机感染病毒，应常用消毒液清洗计算机**

D.系统启动盘应写保护,且一般在该盘中不要存放用户程序及数据

7.防火墙的局限性有（)  
**A.网络上有些攻击可以绕过防火墙**

**B。防火墙不能防范来自内部网络的攻击**

**C。防火墙不能对被病毒感染的程序和文件的传输提供保护**

**D。防火墙不能防范全新的网络威胁**

8.对已感染病毒的磁盘，以下做法不正确的是(）  
**A.不能使用只能丢掉**   B.用杀毒软件杀毒后可继续使用    C**.用酒精消毒后可继续使用    D.可直接使用,对系统无任何影响**

9。以下选项是正确的  
A。互联网直播服务提供者应当与互联网直播服务使用者签订服务协议,明确双方权利义务,但不一定签署平台公约

**B.互联网直播服务协议和平台公约的必备条款由互联网直播服务提供者所在地省、自治区、直辖市互联网信息办公室指导制定**

**C.互联网直播服务提供者应当建立互联网直播发布者信用等级管理体系，提供与信用等级挂钩的管理和服务。**

**D.省、自治区、直辖市互联网信息办公室应当建立黑名单通报制度,并向国家互联网信息办公室报告。**

10。根据“谁主管，谁负责;谁应用，谁负责"的原则,各重点单位应建立健全的安全管理制度有（)  
**A.与公安机关的联系制度    B。计算机技术人员和管理人员管理制度    C.灾难恢复制度    D。日志管理制度**

单选题

1.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，这属于什么攻击类型？ （A)

A、拒绝服务

B、文件共享

C、BIND漏洞

D、远程过程调用

2.为了防御网络监听，最常用的方法是 （B)

A、采用物理传输（非网络)

B、信息加密

C、无线网

D、使用专线传输

3。向有限的空间输入超长的字符串是哪一种攻击手段？（A）

A、缓冲区溢出；

B、网络监听

C、拒绝服务

D、IP欺骗

4。主要用于加密机制的协议是(D)

A、HTTP

B、FTP

C、TELNET

D、SSL

5。用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码,这是属于何种攻击手段？ (B)

A、缓存溢出攻击；

B、钓鱼攻击

C、暗门攻击;

D、DDOS攻击

6。Windows NT 和Windows 2000系统能设置为在几次无效登录后锁定帐号，这可以防止（B）

A、木马;

B、暴力攻击;

C、IP欺骗;

D、缓存溢出攻击

7。在以下认证方式中,最常用的认证方式是:(A)

A基于账户名／口令认证

B基于摘要算法认证 ；

C基于PKI认证 ;

D基于数据库认证

8。以下哪项不属于防止口令猜测的措施？ （B)

A、严格限定从一个给定的终端进行非法认证的次数;

B、确保口令不在终端上再现；

C、防止用户使用太短的口令；

D、使用机器产生的口令

9.下列不属于系统安全的技术是(B)

A、防火墙

B、加密狗

C、认证

D、防病毒

10.抵御电子邮箱入侵措施中，不正确的是（ D ）

A、不用生日做密码

B、不要使用少于5位的密码

C、不要使用纯数字

D、自己做服务器

11。不属于常见的危险密码是（ D )

A、跟用户名相同的密码

B、使用生日作为密码

C、只有4位数的密码

D、10位的综合型密码

12。不属于计算机病毒防治的策略的是（ D ）

1. 确认您手头常备一张真正“干净”的引导盘
2. 及时、可靠升级反病毒产品
3. 新购置的计算机软件也要进行病毒检测
4. 整理磁盘

13。针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，这是（ ）防火墙的特点。（D）

A、包过滤型

B、应用级网关型

C、复合型防火墙

D、代理服务型

14。在每天下午5点使用计算机结束时断开终端的连接属于（ A ）

A、外部终端的物理安全

B、通信线的物理安全

C、窃听数据

D、网络地址欺骗

15.2003年上半年发生的较有影响的计算机及网络病毒是什么(B)

(A)SARS

(B)SQL杀手蠕虫

（C)手机病毒

（D）小球病毒

16。SQL 杀手蠕虫病毒发作的特征是什么（A）

（A）大量消耗网络带宽

(B)攻击个人PC终端

(C）破坏PC游戏程序

（D）攻击手机网络

17.当今IT 的发展与安全投入，安全意识和安全手段之间形成(B)

(A）安全风险屏障

（B）安全风险缺口

（C)管理方式的变革

（D)管理方式的缺口

18。我国的计算机年犯罪率的增长是（C)

（A)10%

（B）160%

（C)60%

(D）300%

19。信息安全风险缺口是指（A）

（A)IT 的发展与安全投入，安全意识和安全手段的不平衡

(B)信息化中,信息不足产生的漏洞  
（C）计算机网络运行，维护的漏洞

（D）计算中心的火灾隐患

20.信息网络安全的第一个时代（B)

(A)九十年代中叶

(B)九十年代中叶前

(C）世纪之交

(D)专网时代

21。信息网络安全的第三个时代(A)

(A）主机时代, 专网时代, 多网合一时代

（B）主机时代, PC机时代， 网络时代

（C)PC机时代,网络时代，信息时代

(D)2001年，2002年，2003年

22。信息网络安全的第二个时代(A）

(A）专网时代

(B）九十年代中叶前

(C)世纪之交

23。网络安全在多网合一时代的脆弱性体现在（C）

（A)网络的脆弱性

(B）软件的脆弱性

(C）管理的脆弱性

（D)应用的脆弱性

24.人对网络的依赖性最高的时代（C）

（A)专网时代

（B)PC时代

(C)多网合一时代

（D)主机时代

25。网络攻击与防御处于不对称状态是因为(C）

（A）管理的脆弱性

（B)应用的脆弱性

（C）网络软，硬件的复杂性

(D）软件的脆弱性

26。网络攻击的种类（A)

(A)物理攻击，语法攻击,语义攻击

(B)黑客攻击，病毒攻击

（C)硬件攻击,软件攻击

(D）物理攻击，黑客攻击，病毒攻击

27。语义攻击利用的是(A)

(A)信息内容的含义

（B)病毒对软件攻击

(C）黑客对系统攻击

（D)黑客和病毒的攻击

28。1995年之后信息网络安全问题就是（A)

（A）风险管理

(B）访问控制

(C)消除风险

(D）回避风险

29。风险评估的三个要素(D）

(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

30。信息网络安全（风险)评估的方法（A）

（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

31.PDR模型与访问控制的主要区别(A）

（A）PDR把安全对象看作一个整体

(B）PDR作为系统保护的第一道防线

（C)PDR采用定性评估与定量评估相结合

(D）PDR的关键因素是人

32.信息安全中PDR模型的关键因素是（A）

(A）人

(B）技术

（C)模型

(D）客体

33.计算机网络最早出现在哪个年代（B）

（A）20世纪50年代

(B)20世纪60年代

（C）20世纪80年代

(D)20世纪90年代

34。最早研究计算机网络的目的是什么？(C）

(A)直接的个人通信；

（B）共享硬盘空间、打印机等设备；

（C）共享计算资源；

D大量的数据交换。

35。最早的计算机网络与传统的通信网络最大的区别是什么?（B）

(A)计算机网络带宽和速度大大提高。

(B)计算机网络采用了分组交换技术。

(C）计算机网络采用了电路交换技术

(D）计算机网络的可靠性大大提高。

36.关于80年代Mirros 蠕虫危害的描述，哪句话是错误的？(B）

（A)该蠕虫利用Unix系统上的漏洞传播

(B)窃取用户的机密信息，破坏计算机数据文件  
(C）占用了大量的计算机处理器的时间，导致拒绝服务

(D)大量的流量堵塞了网络，导致网络瘫痪

37.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

38。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？(C)

（A）安装防火墙

(B)安装入侵检测系统

（C）给系统安装最新的补丁

(D)安装防病毒软件

39。下面哪个功能属于操作系统中的安全功能 （C)

（A)控制用户的作业排序和运行

（B）实现主机和外设的并行处理以及异常情况的处理  
（C）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

（D）对计算机用户访问系统和资源的情况进行记录

40.下面哪个功能属于操作系统中的日志记录功能（D)

(A）控制用户的作业排序和运行

（B）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  
(C)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

（D）对计算机用户访问系统和资源的情况进行记录

42.Windows NT提供的分布式安全环境又被称为（A)

(A）域（Domain)

（B）工作组

（C）对等网

（D）安全网

43。下面哪一个情景属于身份验证(Authentication）过程（A）

（A）用户依照系统提示输入用户名和口令  
（B）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  
(C)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  
(D）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

44.下面哪一个情景属于授权(Authorization）(B)

（A）用户依照系统提示输入用户名和口令  
(B)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  
(C）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  
（D）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

45.下面哪一个情景属于审计（Audit）（D）

（A)用户依照系统提示输入用户名和口令  
(B)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  
(C）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  
（D）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

46。以网络为本的知识文明人们所关心的主要安全是(C）

(A)人身安全

(B)社会安全

(C)信息安全

47。第一次出现"HACKER”这个词是在(B）

(A）BELL实验室

（B)麻省理工AI实验室

(C)AT&T实验室

48。可能给系统造成影响或者破坏的人包括(A)

(A）所有网络与信息系统使用者

（B）只有黑客

(C）只有跨客

49.黑客的主要攻击手段包括(A）

(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

50.从统计的情况看，造成危害最大的黑客攻击是（C）

（A)漏洞攻击

（B)蠕虫攻击

（C)病毒攻击

51.第一个计算机病毒出现在（B)

(A）40年代

(B）70 年代

(C）90年代

52.口令攻击的主要目的是(B)

（A）获取口令破坏系统

(B)获取口令进入系统

（C)仅获取口令没有用途

53。通过口令使用习惯调查发现有大约\_\_\_％的人使用的口令长度低于5个字符的(B)

(A)50。5

（B）51. 5

（C）52.5

54.通常一个三个字符的口令破解需要(B）

(A）18毫秒

(B)18 秒

（C)18分

55。黑色星期四是指（A)

(A)1998年11月3日星期四

（B）1999年6月24日星期四

(C)2000年4月13日星期四

56.大家所认为的对Internet安全技术进行研究是从\_\_\_\_\_\_\_时候开始的  （C）

(A）Internet 诞生

（B)第一个计算机病毒出现

( C）黑色星期四

57。计算机紧急应急小组的简称是（A）

(A）CERT

(B)FIRST

(C)SANA

58.邮件炸弹攻击主要是（B)

(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

59.逻辑炸弹通常是通过（B）

（A）必须远程控制启动执行，实施破坏

（B）指定条件或外来触发启动执行,实施破坏

（C)通过管理员控制启动执行，实施破坏

60.1996年上海某寻呼台发生的逻辑炸弹事件，造事者被判"情节轻微,无罪释放"是因为(C）

(A）证据不足

（B)没有造成破坏

（C)法律不健全

61.扫描工具(C）

(A)只能作为攻击工具

（B)只能作为防范工具

（C)既可作为攻击工具也可以作为防范工具

62.DDOS攻击是利用\_\_\_\_\_进行攻击（C）

(A)其他网络

（B)通讯握手过程问题

(C)中间代理

63.全国首例计算机入侵银行系统是通过(A)

（A)安装无限MODEM进行攻击

(B)通过内部系统进行攻击

（C)通过搭线进行攻击

64.黑客造成的主要安全隐患包括（A)

（A）破坏系统、窃取信息及伪造信息

(B）攻击系统、获取信息及假冒信息

(C)进入系统、损毁信息及谣传信息

65。从统计的资料看，内部攻击是网络攻击的（B）

（A)次要攻击

(B)最主要攻击

（C)不是攻击源

66.江泽民主席指出信息战的主要形式是(A）

(A）电子战和计算机网络战

（B)信息攻击和网络攻击

(C)系统破坏和信息破坏

67。广义地说，信息战是指敌对双方为达成各自的国家战略目标，为夺取\_\_\_\_\_\_在等各个领域的信息优势，运用信息和信息技术手段而展开的信息斗争(B)

(A）政治、经济、国防、领土、文化、外交

（B）政治、经济、军事、科技、文化、外交

（C)网络、经济、信息、科技、文化、外交

68.狭义地说，信息战是指军事领域里的信息斗争.它是敌对双方为争夺信息的\_\_\_\_\_\_，通过利用、破坏敌方和保护己方的信息、信息系统而采取的作战形式 （C)

(A）占有权、控制权和制造权

（B)保存权、制造权和使用权

（C)获取权、控制权和使用权

69.信息战的战争危害较常规战争的危害（C)

(A)轻

B）重

(C)不一定

70.信息战的军人身份确认较常规战争的军人身份确认（A)

（A)难

（B)易

(C）难说

71.互联网用户应在其网络正式联通之日起\_\_\_\_\_内，到公安机关办理国际联网备案手续（A）

（A）三十日

（B）二十日

(C)十五日

（D)四十日

72。一般性的计算机安全事故和计算机违法案件可由\_\_\_\_\_受理（C)

（A)案发地市级公安机关公共信息网络安全监察部门  
(B)案发地当地县级（区、市）公安机关治安部门。  
(C）案发地当地县级（区、市）公安机关公共信息网络安全监察部门  
(D)案发地当地公安派出所

73.计算机刑事案件可由\_\_\_\_\_受理（A）

（A）案发地市级公安机关公共信息网络安全监察部门  
(B)案发地市级公安机关治安部门  
(C)案发地当地县级（区、市)公安机关公共信息网络安全监察部门  
(D）案发地当地公安派出所

74。计算机信息系统发生安全事故和案件，应当\_\_\_\_\_\_在内报告当地公安机关公共信息网络安全监察部门（D）

（A)8小时

（B)48小时

（C)36小时

(D)24小时

75。对计算机安全事故的原因的认定或确定由\_\_\_\_\_作出(C）

(A)人民法院

(B)公安机关

（C)发案单位

（D）以上都可以

76。对发生计算机安全事故和案件的计算机信息系统，如存在安全隐患的，\_\_\_\_\_\_应当要求限期整改(B）

(A)人民法院

（B)公安机关

(C）发案单位的主管部门

（D)以上都可以

77。传入我国的第一例计算机病毒是＿＿(B）

(A）大麻病毒

(B)小球病毒

（C）1575病毒

（D）米开朗基罗病毒

78.我国是在＿＿年出现第一例计算机病毒（C）

(A)1980

（B)1983

(C）1988

(D)1977

79.计算机病毒是\_\_\_\_\_（A）

(A）计算机程序

（B)数据

（C）临时文件

（D）应用软件

80。计算机病毒能够\_\_\_\_\_(ABC）

（A）破坏计算机功能或者毁坏数据

（B)影响计算机使用

(C)能够自我复制

（D）保护版权

81。1994年我国颁布的第一个与信息安全有关的法规是\_\_\_\_\_（D)

(A）国际互联网管理备案规定

（B）计算机病毒防治管理办法

（C）网吧管理规定

(D)中华人民共和国计算机信息系统安全保护条例

82。网页病毒主要通过以下途径传播（C）

(A)1〉邮件

（B）文件交换

(C）网络浏览

(D)光盘

83。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，将受到\_\_\_\_处罚（A)

（A）处五年以下有期徒刑或者拘役

（B)拘留

(C)罚款

(D)警告

84。计算机病毒防治产品根据\_\_\_\_标准进行检验(A)

（A）计算机病毒防治产品评级准测

(B)计算机病毒防治管理办法

(C)基于DOS系统的安全评级准则

(D）计算机病毒防治产品检验标准

85。《计算机病毒防治管理办法》是在哪一年颁布的（C)

（A）1994

(B)1997

(C)2000

（D）1998

86。边界防范的根本作用是（C)

（A）对系统工作情况进行检验与控制,防止外部非法入侵  
（B）对网络运行状况进行检验与控制，防止外部非法入侵  
（C)对访问合法性进行检验与控制，防止外部非法入侵

87。路由设置是边界防范的（A)

(A）基本手段之一

(B)根本手段

(C）无效手段

88.网络物理隔离是指(C)

（A)两个网络间链路层在任何时刻不能直接通讯  
（B）两个网络间网络层在任何时刻不能直接通讯  
(C)两个网络间链路层、网络层在任何时刻都不能直接通讯

89.VPN是指（A)

(A)虚拟的专用网络

（B)虚拟的协议网络

C）虚拟的包过滤网络

90.带VPN的防火墙的基本原理流程是（A)

(A)先进行流量检查

(B)先进行协议检查

(C)先进行合法性检查

91。防火墙主要可以分为（A）

（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

92.NAT 是指(B)

（A）网络地址传输

（B）网络地址转换

(C）网络地址跟踪

93.VPN通常用于建立\_\_\_\_之间的安全通道(A)

（A）总部与分支机构、与合作伙伴、与移动办公用户  
(B）客户与客户、与合作伙伴、与远程用户  
(C）总部与分支机构、与外部网站、与移动办公用户

94。在安全区域划分中DMZ 区通常用做（B）

(A）数据区

(B）对外服务区

（C)重要业务区

95。目前用户局域网内部区域划分通常通过\_\_\_\_实现（B）

（A）物理隔离

（B)Vlan 划分

(C）防火墙防范

96。防火墙的部署(B）

(A)只需要在与Internet 相连接的出入口设置

(B）在需要保护局域网络的所有出入口设置

（C)需要在出入口和网段之间进行部署

97.防火墙是一个(A)

（A)分离器、限制器、分析器

(B)隔离器、控制器、分析器

(C)分离器、控制器、解析器

98。目前的防火墙防范主要是(B)

（A)主动防范

(B)被动防范

(C）不一定

99。目前的防火墙防范主要是（B)

（A)主动防范

（B）被动防范

（C）不一定

100.IP地址欺骗通常是(A）

（A)黑客的攻击手段

(B）防火墙的专门技术

(C)IP 通讯的一种模式

101。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？（C）

(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

102）现代主动安全防御的主要手段是（A)

A〉探测、预警、监视、警报

B>嘹望、烟火、巡更、敲梆

C>调查、报告、分析、警报

103)古代主动安全防御的典型手段有(B）

A>探测、预警、监视、警报

B〉嘹望、烟火、巡更、敲梆

C〉调查、报告、分析、警报

（104)．计算机信息系统，是指由（B )及其相关的和配套的设备、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。

A．计算机硬件

B．计算机

C．计算机软件

D．计算机网络

(105)．计算机信息系统的安全保护，应当保障（A )，运行环境的安全，保障信息的安全,保障计算机功能的正常发挥,以维护计算机信息系统的安全运行.

A．计算机及其相关的和配套的设备、设施（含网络）的安全

B．计算机的安全

C．计算机硬件的系统安全

D．计算机操作人员的安全

（106）．当前奇瑞股份有限公司所使用的杀毒软件是：（C ） 。

A 瑞星企业版

B卡巴斯基

C 趋势防病毒网络墙

D 诺顿企业版

（107）．计算机病毒是指:（C ）

A .带细菌的磁盘

B。 已损坏的磁盘

C. 具有破坏性的特制程序

D。被破坏了的程序

（108)．计算机连网的主要目的是\_\_\_\_A\_\_\_\_\_\_\_\_\_\_。

A资源共享

B．共用一个硬盘

C．节省经费

D．提高可靠性

（109）．关于计算机病毒知识，叙述不正确的是D

A . 计算机病毒是人为制造的一种破坏性程序

B 。 大多数病毒程序具有自身复制功能

C. 安装防病毒卡,并不能完全杜绝病毒的侵入

D。 不使用来历不明的软件是防止病毒侵入的有效措施

（110）．公司USB接口控制标准：院中心研发部门（ A ）,一般职能部门( A ）。

A 2％ 5%

B 4% 10%

Ｃ 5％　10％

D 2％ 4%。

（111)．木马程序一般是指潜藏在用户电脑中带有恶意性质的 A ，利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息。

A 远程控制软件

B 计算机操作系统

C 木头做的马

（112） 。为了防止各种各样的病毒对计算机系统造成危害，可以在计算机上安装防病毒软件，并注意及时 B ，以保证能防止和查杀新近出现的病毒。

A 分析

B 升级

C 检查

（113）. 局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样，则（ C )。

A 两台计算机都正常

B 两台计算机都无法通讯

C 一台正常通讯一台无法通讯

（114）.同一根网线的两头插在同一交换机上会（ A )。

A 网络环路

B 根本没有影响

Ｃ　短路

D 回路

(115)企业重要数据要及时进行（　C　），以防出现以外情况导致数据丢失。

Ａ杀毒

Ｂ加密

Ｃ备份

（116）.WINDOWS主机推荐使用（ A）格式

A NTFS

B FAT32

C FAT

D LINUX

117. 计算机网络是地理上分散的多台（C）遵循约定的通信协议,通过软硬件互联的系统.

A. 计算机

B. 主从计算机

C。 自主计算机

D. 数字设备

118. 密码学的目的是(C）。

A. 研究数据加密

B. 研究数据解密

C. 研究数据保密

D。 研究信息安全

119. 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（A）。

A。 对称加密技术

B. 分组密码技术

C。 公钥加密技术

D. 单向函数密码技术

120. 网络安全最终是一个折衷的方案,即安全强度和安全操作代价的折衷,除增加安全设施投资外，还应考虑（D）。

A. 用户的方便性

B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持

D。 上面3项都是

121．A方有一对密钥（KA公开，KA秘密）,B方有一对密钥（KB公开，KB秘密），A方向B方发送数字签名M，对信息M加密为：M'= KB公开(KA秘密（M））。B方收到密文的解密方案是（C)。

A。 KB公开（KA秘密（M’））

B。 KA公开（KA公开(M’））

C。 KA公开(KB秘密（M’））

D. KB秘密（KA秘密（M’））

122。 “公开密钥密码体制"的含义是（C）。

A。 将所有密钥公开

B. 将私有密钥公开，公开密钥保密

C. 将公开密钥公开，私有密钥保密

D. 两个密钥相同

123. PKI支持的服务不包括（D）。

A. 非对称密钥技术及证书管理

B。 目录服务

C。 对称密钥的产生和分发

D. 访问控制服务

124。 PKI的主要组成不包括（B）。

A. 证书授权CA

B。 SSL

C. 注册授权RA

D. 证书存储库CR

125. PKI管理对象不包括（A）。

A. ID和口令

B。 证书

C. 密钥

D。 证书撤消

126。 下面不属于PKI组成部分的是（D）。

A. 证书主体

B. 使用证书的应用和系统

C。 证书权威机构

D。 AS

127。 SSL产生会话密钥的方式是（C).

A. 从密钥管理数据库中请求获得

B。 每一台客户机分配一个密钥的方式

C. 随机由客户机产生并加密后通知服务器

D. 由服务器产生并分配给客户机

128.属于Web中使用的安全协议（C).

A。 PEM、SSL

B. S-HTTP、S/MIME

C。 SSL、S—HTTP

D。 S/MIME、SSL

129. 传输层保护的网络采用的主要技术是建立在（A)基础上的（A)。

A. 可靠的传输服务，安全套接字层SSL协议

B。 不可靠的传输服务，S-HTTP协议

C。 可靠的传输服务， S-HTTP协议

D。 不可靠的传输服务，安全套接字层SSL协议

130. 通常所说的移动VPN是指（A)。

A. Access VPN

B。 Intranet VPN

C. Extranet VPN

D. 以上皆不是

131. 属于第二层的VPN隧道协议有（B)。

A. IPSec

B。 PPTP

C.GRE

D。 以上皆不是

132. GRE协议的乘客协议是(D）。

A. IP

B。 IPX

C. AppleTalk

D. 上述皆可

133 VPN的加密手段为(C）。

A. 具有加密功能的防火墙

B。 具有加密功能的路由器

C。 VPN内的各台主机对各自的信息进行相应的加密

D。 单独的加密设备

134。 将公司与外部供应商、客户及其他利益相关群体相连接的是（B）。

A。 内联网VPN

B。 外联网VPN

C。 远程接入VPN

D. 无线VPN

135. PPTP、L2TP和L2F隧道协议属于（B）协议.

A. 第一层隧道

B。 第二层隧道

C。 第三层隧道

D。 第四层隧道

136．不属于隧道协议的是（C）。

A。 PPTP

B. L2TP

C。 TCP/IP

D。 IPSec

137.不属于VPN的核心技术是（C）.

A. 隧道技术

B。 身份认证

C. 日志记录

D。 访问控制

138．目前,VPN使用了(A）技术保证了通信的安全性。

1. 隧道协议、身份认证和数据加密
2. 身份认证、数据加密
3. 隧道协议、身份认证
4. 隧道协议、数据加密

139。（A)通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部

网的远程访问。

A. Access VPN

B。 Intranet VPN

C. Extranet VPN

D. Internet VPN

140．L2TP隧道在两端的VPN服务器之间采用（A）来验证对方的身份。

A. 口令握手协议CHAP

B。 SSL

C。 Kerberos

D。 数字证书

141．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0。5，则k约等于＿＿。B

A．2128

B．264

C．232

D．2256

142．Bell—LaPadula模型的出发点是维护系统的＿＿＿,而Biba模型与Bell—LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题。它们存在共同的缺点:直接绑定主体与客体，授权工作困难。C

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

143、口令破解的最好方法是(B）

A暴力破解

B组合破解

C字典攻击

D生日攻击

144、杂凑码最好的攻击方式是（D）

A 穷举攻击

B中途相遇

C字典攻击

D生日攻击

145、可以被数据完整性机制防止的攻击方式是（D）

A假冒\*＊\*

B抵赖\*\*＊\*

C数据中途窃取

D数据中途篡改

146、会话侦听与劫持技术属于(B）技术

A密码分析还原

B协议漏洞渗透

C应用漏洞分析与渗透

D DOS攻击

147、PKI的主要组成不包括(B)

A CA

B SSL

C RA

D CR

148.恶意代码是(指没有作用却会带来危险的代码D）

A 病毒\*＊\*

B 广告\*\*＊

C间谍＊＊

D 都是

149。社会工程学常被黑客用于（踩点阶段信息收集A）

A 口令获取

B ARP

C TCP

D DDOS

150.windows中强制终止进程的命令是(C）

A Tasklist

B Netsat

C Taskkill

D Netshare

151.现代病毒木马融合了（D）新技术

A 进程注入

B注册表隐藏

C漏洞扫描

D都是

152。溢出攻击的核心是（A）

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

153.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外部网络

D自由连接

多选题

（1)网络安全工作的目标包括（ABCD）  
A、信息机密性;

B、信息完整性;

C、服务可用性;

D、可审查性

（2）智能卡可以应用的地方包括（ABCD）  
A、进入大楼；

B、使用移动电话；

C、登录特定主机；

D、执行银行和电子商务交易

(3）计算机信息系统安全保护的目标是要保护计算机信息系统的(ABCD)

（A)实体安全

(B）运行安全

（C）信息安全

(D)人员安全

(4)计算机信息系统的运行安全包括（ABC)

(A）系统风险管理

（B)审计跟踪

(C)备份与恢复

(D)电磁信息泄漏

(5)实施计算机信息系统安全保护的措施包括(AB)

（A）安全法规

（B）安全管理

(C）组织建设

（D)制度建设

(6)计算机信息系统安全管理包括（ACD)

(A)组织建设

(B）事前检查

(C）制度建设

（D)人员意识

(7)公共信息网络安全监察工作的性质（ABCD）

(A)是公安工作的一个重要组成部分

(B）是预防各种危害的重要手段

（C)是行政管理的重要手段

(D）是打击犯罪的重要手段

（8)公共信息网络安全监察工作的一般原则（ABCD)

（A)预防与打击相结合的原则

（B）专门机关监管与社会力量相结合的原则  
(C)纠正与制裁相结合的原则

（D）教育和处罚相结合的原则

(9）安全员应具备的条件: (ABD)

(A)具有一定的计算机网络专业技术知识

(B)经过计算机安全员培训，并考试合格  
（C）具有大本以上学历

（D)无违法犯罪记录

(10）网络操作系统应当提供哪些安全保障(ABCDE)

(A）验证(Authentication）

（B)授权(Authorization）  
（C）数据保密性(Data Confidentiality）

(D）数据一致性(Data Integrity)  
(E）数据的不可否认性(Data Nonrepudiation）

(11）Windows NT的"域"控制机制具备哪些安全特性？（ABC）

（A)用户身份验证

（B）访问控制  
(C）审计（日志)

(D)数据通讯的加密

（12）从系统整体看，安全”漏洞”包括哪些方面（ABC）

（A)技术因素

(B)人的因素

（C）规划，策略和执行过程

(13）从系统整体看,下述那些问题属于系统安全漏洞（ABCDE）

（A)产品缺少安全功能

(B）产品有Bugs

(C)缺少足够的安全知识

（D）人为错误

(E）缺少针对安全的系统设计

(14）应对操作系统安全漏洞的基本方法是什么？（ABC）

（A)对默认安装进行必要的调整

（B)给所有用户设置严格的口令

(C）及时安装最新的安全补丁

（D）更换到另一种操作系统

(15）造成操作系统安全漏洞的原因（ABC）

(A）不安全的编程语言

（B)不安全的编程习惯

（C）考虑不周的架构设计

(16）严格的口令策略应当包含哪些要素(ABCD）

（A)满足一定的长度，比如8位以上

（B）同时包含数字,字母和特殊字符  
(C)系统强制要求定期更改口令

(D)用户可以设置空口令

（17）计算机安全事件包括以下几个方面(ABCD)

（A）重要安全技术的采用

（B)安全标准的贯彻  
(C)安全制度措施的建设与实施

（D）重大安全隐患、违法违规的发现，事故的发生

（18)计算机案件包括以下几个内容(ABC）

(A）违反国家法律的行为

(B)违反国家法规的行为  
（C)危及、危害计算机信息系统安全的事件

(D)计算机硬件常见机械故障

(19）重大计算机安全事故和计算机违法案件可由\_\_\_\_\_受理(AC）

（A)案发地市级公安机关公共信息网络安全监察部门

(B)案发地当地县级(区、市）公安机关治安部门  
(C)案发地当地县级(区、市）公安机关公共信息网络安全监察部门

（D)案发地当地公安派出所

（20）现场勘查主要包括以下几个环节\_\_\_\_\_（ABCD)

(A)对遭受破坏的计算机信息系统的软硬件的描述及被破坏程度

（B)现场现有电子数据的复制和修复  
(C）电子痕迹的发现和提取，证据的固定与保全

(D)现场采集和扣押与事故或案件有关的物品

(21）计算机安全事故原因的认定和计算机案件的数据鉴定,\_\_\_\_ (ABC）

（A)是一项专业性较强的技术工作

(B）必要时可进行相关的验证或侦查实验  
（C）可聘请有关方面的专家，组成专家鉴定组进行分析鉴定

（D）可以由发生事故或计算机案件的单位出具鉴定报告

(22）有害数据通过在信息网络中的运行，主要产生的危害有（ABC)

（A）攻击国家政权,危害国家安全

(B)破坏社会治安秩序

(C)破坏计算机信息系统，造成经济的社会的巨大损失

（23）计算机病毒的特点\_\_\_\_\_\_(ACD）

（A)传染性

(B）可移植性

（C)破坏性

（D)可触发性

(24）计算机病毒按传染方式分为\_\_\_\_（BCD）

(A）良性病毒

（B）引导型病毒

(C）文件型病毒

（D）复合型病毒

（25）计算机病毒的危害性有以下几种表现(ABC)

(A)删除数据

(B）阻塞网络

(C)信息泄漏

（D）烧毁主板

（26）计算机病毒由\_\_\_\_\_部分组成（ABD)

(A）引导部分

（B)传染部分

(C)运行部分

（D）表现部分

(27）以下哪些措施可以有效提高病毒防治能力(ABCD）

(A)安装、升级杀毒软件

(B）升级系统、打补丁

（C）提高安全防范意识

(D)不要轻易打开来历不明的邮件

（28)计算机病毒的主要传播途径有（ABCD)

（A）电子邮件

（B）网络

(C）存储介质

(D)文件交换

(29）计算机病毒的主要来源有\_\_\_\_(ACD）

（A)黑客组织编写

(B）计算机自动产生

(C)恶意编制

(D)恶作剧

（30）发现感染计算机病毒后,应采取哪些措施（ABC）

（A）断开网络

(B）使用杀毒软件检测、清除  
（C)如果不能清除，将样本上报国家计算机病毒应急处理中心

(D)格式化系统

填空：

1． 信息安全包含：\_\_物理\_\_\_\_安全、\_\_\_\_信息系统\_\_\_\_\_\_\_\_安全和\_\_数据\_安全。

2. 数据安全包含\_\_\_可用性\_、\_\_\_\_完整性\_\_、\_\_\_保密性\_三个基本特性。

2．公司对电脑密码的强壮度要求是：\_字母加数字组合8位以上\_\_\_\_.

3．员工离开自己的计算机时要立即设置\_\_\_锁屏\_\_\_\_\_\_\_\_\_。

4.信息安全四大要素是：\_\_技术、\_\_\_制度、流程、\_\_\_人\_.

5.未来信息安全的发展趋势是由\_\_\_\_\_防外\_转变为\_\_\_\_\_防内\_\_\_\_.

6. 新修订《刑法》中有关失泄密处罚条款：以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的，给商业秘密的权利人造成重大损失的,处三年以下有期徒刑或者拘役,并处或者单处罚金；造成特别严重后果的，处三年以上\_\_七\_\_年以下有期徒刑，并处罚金

7.工作人员因工作需要必须使用Internet时，需由各部门信息化管理员提交\_\_\_OA\_\_申请。

8。密码系统包括以下4个方面:明文空间、密文空间、密钥空间和密码算法。

9.解密算法D是加密算法E的 逆运算 .

10。常规密钥密码体制又称为 对称密钥密码体制 ,是在公开密钥密码体制以前使用的密码体制。

11。如果加密密钥和解密密钥 相同 ，这种密码体制称为对称密码体制。

12.DES算法密钥是 64 位，其中密钥有效位是 56 位。

13。RSA算法的安全是基于 分解两个大素数的积 的困难。

14。公开密钥加密算法的用途主要包括两个方面：密钥分配、数字签名。

15.消息认证是 验证信息的完整性 ，即验证数据在传送和存储过程中是否被篡改、重放或延迟等。

16。MAC函数类似于加密，它于加密的区别是MAC函数 不 可逆.

一

2011江西首届高校信息安全知识及软件设计大赛试题

比赛qq群：117613445

希望大家能够喜欢。试题从网上找的，好的话,希望大家别忘了给个好评。

进群条件：在各大论坛发布以下信息一条以上：江西首届高校信息安全知识及软件设计大赛qq：117613445 。

然后把你发布的地址给我.为了让更多的高手进群，希望大家推广下。谢谢！

一、单选题

1。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,这属于什么攻击类型？ （A)

A、拒绝服务B、文件共享C、BIND漏洞D、远程过程调用

2。为了防御网络监听，最常用的方法是 （B)

A、采用物理传输（非网络）B、信息加密C、无线网D、使用专线传输

3。向有限的空间输入超长的字符串是哪一种攻击手段？（A）

A、缓冲区溢出；B、网络监听;C、拒绝服务D、IP欺骗

4。主要用于加密机制的协议是(D）

A、HTTP B、FTPC、TELNET D、SSL

5。用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？ （B)

A、缓存溢出攻击;B、钓鱼攻击；C、暗门攻击;D、DDOS攻击

6。Windows NT 和Windows 2000系统能设置为在几次无效登录后锁定帐号，这可以防止（B）

A、木马;B、暴力攻击；C、IP欺骗;D、缓存溢出攻击

7.在以下认证方式中，最常用的认证方式是:(A)

A基于账户名／口令认证;B基于摘要算法认证；C基于PKI认证 ;D基于数据库认证

8.以下哪项不属于防止口令猜测的措施？ (B）

A、严格限定从一个给定的终端进行非法认证的次数；B、确保口令不在终端上再现；C、防止用户使用太短的口令；D、使用机器产生的口令

9.下列不属于系统安全的技术是(B)

A、防火墙;B、加密狗；C、认证 ；D、防病毒

10.抵御电子邮箱入侵措施中，不正确的是( D ）

A、不用生日做密码 B、不要使用少于5位的密码C、不要使用纯数字 D、自己做服务器

11.不属于常见的危险密码是（ D ）

A、跟用户名相同的密码 B、使用生日作为密码C、只有4位数的密码 D、10位的综合型密码

12。不属于计算机病毒防治的策略的是（ D )

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

13。针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，这是（ )防火墙的特点。（D)

A、包过滤型 B、应用级网关型 C、复合型防火墙 D、代理服务型

14.在每天下午5点使用计算机结束时断开终端的连接属于( A ）

A、外部终端的物理安全 B、通信线的物理安全 C、窃听数据 D、网络地址欺骗

15。2003年上半年发生的较有影响的计算机及网络病毒是什么（B)

(A)SARS(B)SQL杀手蠕虫(C)手机病毒（D)小球病毒

16。SQL 杀手蠕虫病毒发作的特征是什么（A)

(A）大量消耗网络带宽(B）攻击个人PC终端(C）破坏PC游戏程序(D）攻击手机网络

17。当今IT 的发展与安全投入，安全意识和安全手段之间形成（B)

(A）安全风险屏障（B)安全风险缺口(C)管理方式的变革（D)管理方式的缺口

18.我国的计算机年犯罪率的增长是（C)

(A）10%(B）160％(C)60％(D)300％

19。信息安全风险缺口是指（A）

(A）IT 的发展与安全投入,安全意识和安全手段的不平衡（B)信息化中,信息不足产生的漏洞

(C)计算机网络运行，维护的漏洞(D）计算中心的火灾隐患

20.信息网络安全的第一个时代(B)

（A)九十年代中叶（B)九十年代中叶前（C)世纪之交(D)专网时代

21。信息网络安全的第三个时代(A)

(A)主机时代, 专网时代， 多网合一时代（B）主机时代, PC机时代， 网络时代（C)PC机时代，网络时代，信息时代(D）2001年,2002年,2003年

22.信息网络安全的第二个时代（A)

(A）专网时代(B)九十年代中叶前(C)世纪之交

23。网络安全在多网合一时代的脆弱性体现在（C）

（A)网络的脆弱性(B)软件的脆弱性(C)管理的脆弱性(D)应用的脆弱性

24。人对网络的依赖性最高的时代(C）

(A）专网时代(B)PC时代(C）多网合一时代（D）主机时代

25.网络攻击与防御处于不对称状态是因为(C）

（A）管理的脆弱性（B)应用的脆弱性（C）网络软,硬件的复杂性（D)软件的脆弱性

26.网络攻击的种类（A)

（A）物理攻击,语法攻击，语义攻击(B)黑客攻击,病毒攻击（C）硬件攻击，软件攻击（D）物理攻击，黑客攻击,病毒攻击

27.语义攻击利用的是（A)

（A）信息内容的含义（B）病毒对软件攻击（C)黑客对系统攻击（D）黑客和病毒的攻击

28.1995年之后信息网络安全问题就是(A)

(A)风险管理(B）访问控制（C)消除风险(D）回避风险

29。风险评估的三个要素(D）

（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

30.信息网络安全（风险）评估的方法（A)

（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

31。PDR模型与访问控制的主要区别(A）

(A）PDR把安全对象看作一个整体（B）PDR作为系统保护的第一道防线（C)PDR采用定性评估与定量评估相结合（D)PDR的关键因素是人

32.信息安全中PDR模型的关键因素是（A)

（A）人(B)技术（C)模型（D)客体

33.计算机网络最早出现在哪个年代（B)

(A)20世纪50年代（B)20世纪60年代(C)20世纪80年代（D）20世纪90年代

34。最早研究计算机网络的目的是什么？（C)

（A）直接的个人通信;(B)共享硬盘空间、打印机等设备；(C）共享计算资源；

35。大量的数据交换.

36.最早的计算机网络与传统的通信网络最大的区别是什么？(B)

（A)计算机网络带宽和速度大大提高。（B）计算机网络采用了分组交换技术。（C）计算机网络采用了电路交换技术。（D)计算机网络的可靠性大大提高。

37。关于80年代Mirros 蠕虫危害的描述,哪句话是错误的？（B）

（A）该蠕虫利用Unix系统上的漏洞传播（B)窃取用户的机密信息，破坏计算机数据文件

（C）占用了大量的计算机处理器的时间，导致拒绝服务（D)大量的流量堵塞了网络，导致网络瘫痪

38。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

39。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?（C)

（A）安装防火墙（B)安装入侵检测系统(C）给系统安装最新的补丁（D）安装防病毒软件

40。下面哪个功能属于操作系统中的安全功能 （C)

(A)控制用户的作业排序和运行（B)实现主机和外设的并行处理以及异常情况的处理

（C)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（D)对计算机用户访问系统和资源的情况进行记录

41.下面哪个功能属于操作系统中的日志记录功能（D）

(A)控制用户的作业排序和运行（B）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

（C)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(D）对计算机用户访问系统和资源的情况进行记录

42。Windows NT提供的分布式安全环境又被称为（A)

（A）域（Domain）(B）工作组(C）对等网(D）安全网

43.下面哪一个情景属于身份验证(Authentication）过程（A）

(A）用户依照系统提示输入用户名和口令

（B)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

（C）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

(D）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

44.下面哪一个情景属于授权（Authorization)(B)

(A)用户依照系统提示输入用户名和口令

(B）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

(C）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

(D)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

45.下面哪一个情景属于审计（Audit)(D)

（A）用户依照系统提示输入用户名和口令

（B）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

(C）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

（D）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

46。以网络为本的知识文明人们所关心的主要安全是（C)

(A）人身安全（B）社会安全(C)信息安全

47。第一次出现”HACKER”这个词是在(B)

（A)BELL实验室(B）麻省理工AI实验室（C)AT＆T实验室

48.可能给系统造成影响或者破坏的人包括（A）

（A)所有网络与信息系统使用者（B)只有黑客(C）只有跨客

49.黑客的主要攻击手段包括(A)

(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

50。从统计的情况看，造成危害最大的黑客攻击是(C)

（A)漏洞攻击(B)蠕虫攻击（C)病毒攻击

51。第一个计算机病毒出现在（B)

（A)40年代(B）70 年代(C)90年代

52。口令攻击的主要目的是(B）

（A）获取口令破坏系统（B)获取口令进入系统（C）仅获取口令没有用途

53。通过口令使用习惯调查发现有大约\_\_\_％的人使用的口令长度低于5个字符的(B)

（A）50.5（B）51。5(C)52.5

54.通常一个三个字符的口令破解需要（B）

(A）18毫秒(B）18 秒(C）18分

55。黑色星期四是指（A)

(A）1998年11月3日星期四(B）1999年6月24日星期四（C)2000年4月13日星期四

56.大家所认为的对Internet安全技术进行研究是从\_\_\_\_\_\_\_时候开始的 uds：qbody（C)

(A）Internet 诞生(B）第一个计算机病毒出现(C）黑色星期四

57.计算机紧急应急小组的简称是（A)

（A）CERT（B）FIRST(C）SANA

58。邮件炸弹攻击主要是（B)

（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

59.逻辑炸弹通常是通过(B)

（A)必须远程控制启动执行,实施破坏(B)指定条件或外来触发启动执行，实施破坏（C)通过管理员控制启动执行，实施破坏

60.1996年上海某寻呼台发生的逻辑炸弹事件，造事者被判”情节轻微,无罪释放"是因为（C）

（A）证据不足（B）没有造成破坏（C）法律不健全

61.扫描工具（C）

（A）只能作为攻击工具(B)只能作为防范工具(C)既可作为攻击工具也可以作为防范工具

62.DDOS攻击是利用\_\_\_\_\_进行攻击(C)

(A）其他网络(B）通讯握手过程问题（C)中间代理

63。全国首例计算机入侵银行系统是通过（A）

(A)安装无限MODEM进行攻击（B)通过内部系统进行攻击（C）通过搭线进行攻击

64。黑客造成的主要安全隐患包括（A)

（A)破坏系统、窃取信息及伪造信息(B）攻击系统、获取信息及假冒信息（C)进入系统、损毁信息及谣传信息

65.从统计的资料看，内部攻击是网络攻击的（B)

(A)次要攻击（B)最主要攻击(C)不是攻击源

66.江泽民主席指出信息战的主要形式是(A）

(A）电子战和计算机网络战（B)信息攻击和网络攻击（C）系统破坏和信息破坏

67.广义地说，信息战是指敌对双方为达成各自的国家战略目标,为夺取\_\_\_\_\_\_在等各个领域的信息优势，运用信息和信息技术手段而展开的信息斗争(B)

(A）政治、经济、国防、领土、文化、外交(B)政治、经济、军事、科技、文化、外交(C）网络、经济、信息、科技、文化、外交B

68。狭义地说，信息战是指军事领域里的信息斗争。它是敌对双方为争夺信息的\_\_\_\_\_\_，通过利用、破坏敌方和保护己方的信息、信息系统而采取的作战形式 (C）

（A)占有权、控制权和制造权(B)保存权、制造权和使用权（C）获取权、控制权和使用权

69。信息战的战争危害较常规战争的危害（C）

（A）轻（B）重(C）不一定

70。信息战的军人身份确认较常规战争的军人身份确认（A)

(A)难（B）易（C）难说

71.互联网用户应在其网络正式联通之日起\_\_\_\_\_内，到公安机关办理国际联网

备案手续(A)

(A)三十日(B）二十日（C）十五日（D）四十日

72.一般性的计算机安全事故和计算机违法案件可由\_\_\_\_\_受理(C)

(A)案发地市级公安机关公共信息网络安全监察部门

（B）案发地当地县级（区、市）公安机关治安部门.

（C)案发地当地县级（区、市）公安机关公共信息网络安全监察部门

（D）案发地当地公安派出所

73。计算机刑事案件可由\_\_\_\_\_受理（A）

(A）案发地市级公安机关公共信息网络安全监察部门

(B)案发地市级公安机关治安部门

(C）案发地当地县级（区、市）公安机关公共信息网络安全监察部门

(D）案发地当地公安派出所

74.计算机信息系统发生安全事故和案件，应当\_\_\_\_\_\_在内报告当地公安机关公

共信息网络安全监察部门(D）

（A）8小时

(B）48小时

(C)36小时

（D)24小时

75。对计算机安全事故的原因的认定或确定由\_\_\_\_\_作出(C)

(A）人民法院

（B)公安机关

(C)发案单位

(D）以上都可以

76.对发生计算机安全事故和案件的计算机信息系统,如存在安全隐患的,\_\_\_

\_\_\_应当要求限期整改(B）

（A)人民法院

（B)公安机关

(C)发案单位的主管部门

（D）以上都可以

77。传入我国的第一例计算机病毒是＿＿(B）

(A）大麻病毒

（B）小球病毒

（C)1575病毒

（D）米开朗基罗病毒

78。我国是在＿＿年出现第一例计算机病毒（C）

（A)1980

（B)1983

(C）1988

（D）1977

79。计算机病毒是\_\_\_\_\_（A）

（A）计算机程序

（B)数据

（C)临时文件

(D)应用软件

80。计算机病毒能够\_\_\_\_\_(ABC)

（A）破坏计算机功能或者毁坏数据

（B)影响计算机使用

（C）能够自我复制

（D）保护版权

81。1994年我国颁布的第一个与信息安全有关的法规是\_\_\_\_\_（D)

(A)国际互联网管理备案规定

（B)计算机病毒防治管理办法

（C）网吧管理规定

(D）中华人民共和国计算机信息系统安全保护条例

82.网页病毒主要通过以下途径传播(C)

（A)1〉邮件

（B）文件交换

(C)网络浏览

(D)光盘

83.故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，

后果严重的，将受到\_\_\_\_处罚（A)

（A）处五年以下有期徒刑或者拘役

（B)拘留

（C)罚款

（D）警告

84.计算机病毒防治产品根据\_\_\_\_标准进行检验（A)

（A)计算机病毒防治产品评级准测

（B）计算机病毒防治管理办法

（C)基于DOS系统的安全评级准则

(D)计算机病毒防治产品检验标准

85。《计算机病毒防治管理办法》是在哪一年颁布的（C)

（A）1994

(B）1997

（C）2000

（D)1998

86.边界防范的根本作用是（C)

（A)对系统工作情况进行检验与控制，防止外部非法入侵

(B)对网络运行状况进行检验与控制，防止外部非法入侵

（C)对访问合法性进行检验与控制，防止外部非法入侵

87.路由设置是边界防范的(A）

（A）基本手段之一

（B）根本手段

（C）无效手段

88。网络物理隔离是指（C)

（A）两个网络间链路层在任何时刻不能直接通讯

(B）两个网络间网络层在任何时刻不能直接通讯

(C)两个网络间链路层、网络层在任何时刻都不能直接通讯

89.VPN是指(A)

（A)虚拟的专用网络

(B）虚拟的协议网络

（C）虚拟的包过滤网络

90.带VPN的防火墙的基本原理流程是(A)

（A)先进行流量检查

(B)先进行协议检查

（C)先进行合法性检查

91.防火墙主要可以分为（A)

(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

92.NAT 是指(B)

(A)网络地址传输

（B）网络地址转换

(C)网络地址跟踪

93。VPN通常用于建立\_\_\_\_之间的安全通道（A)

（A)总部与分支机构、与合作伙伴、与移动办公用户

(B）客户与客户、与合作伙伴、与远程用户

（C）总部与分支机构、与外部网站、与移动办公用户

94。在安全区域划分中DMZ 区通常用做（B）

(A）数据区

（B)对外服务区

（C）重要业务区

95.目前用户局域网内部区域划分通常通过\_\_\_\_实现（B)

(A)物理隔离

(B)Vlan 划分

（C)防火墙防范

96。防火墙的部署(B）

（A）只需要在与Internet 相连接的出入口设置

（B）在需要保护局域网络的所有出入口设置

（C）需要在出入口和网段之间进行部署

97.防火墙是一个（A)

（A）分离器、限制器、分析器

(B)隔离器、控制器、分析器

(C）分离器、控制器、解析器

98。目前的防火墙防范主要是(B)

（A)主动防范

(B）被动防范

(C)不一定

99.目前的防火墙防范主要是(B）

（A）主动防范

(B）被动防范

（C）不一定

100。IP地址欺骗通常是(A）

（A)黑客的攻击手段

(B）防火墙的专门技术

（C）IP 通讯的一种模式

（101)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?（C）

（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

（ 102)现代主动安全防御的主要手段是（A)

A>探测、预警、监视、警报

B>嘹望、烟火、巡更、敲梆

C〉调查、报告、分析、警报

（ 103）古代主动安全防御的典型手段有（B）

A〉 探测、预警、监视、警报 B>嘹望、烟火、巡更、敲梆 C>调查、报告、分析、警报

（104）．计算机信息系统，是指由（B )及其相关的和配套的设备、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。

A．计算机硬件 B．计算机 C．计算机软件 D．计算机网络

（105)．计算机信息系统的安全保护,应当保障（A ),运行环境的安全,保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行.

A．计算机及其相关的和配套的设备、设施（含网络）的安全 B．计算机的安全

C．计算机硬件的系统安全 D．计算机操作人员的安全

(106)．当前奇瑞股份有限公司所使用的杀毒软件是:（C ） 。

A 瑞星企业版 B卡巴斯基 C 趋势防病毒网络墙 D 诺顿企业版

(107)．计算机病毒是指：（C ）

A .带细菌的磁盘 B. 已损坏的磁盘 C. 具有破坏性的特制程序 D。被破坏了的程序

(108）．计算机连网的主要目的是\_\_\_\_A\_\_\_\_\_\_\_\_\_\_.

A资源共享 B．共用一个硬盘 C．节省经费 D．提高可靠性

（109)．关于计算机病毒知识，叙述不正确的是D

A 。 计算机病毒是人为制造的一种破坏性程序

B 。 大多数病毒程序具有自身复制功能

C. 安装防病毒卡,并不能完全杜绝病毒的侵入

D。 不使用来历不明的软件是防止病毒侵入的有效措施

（110）．公司USB接口控制标准:院中心研发部门( A ），一般职能部门（ A ）.

A 2％ 5% B 4％ 10% Ｃ５％ 10% D 2％ 4%。

（111)．木马程序一般是指潜藏在用户电脑中带有恶意性质的 A ,利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息。

A 远程控制软件 B 计算机操作系统 C 木头做的马

（112） .为了防止各种各样的病毒对计算机系统造成危害,可以在计算机上安装防病毒软件，并注意及时 B ,以保证能防止和查杀新近出现的病毒.

A 分析 B 升级 C 检查

(113)。 局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样，则（ C ）.

A 两台计算机都正常 B 两台计算机都无法通讯 C 一台正常通讯一台无法通讯

（114)。同一根网线的两头插在同一交换机上会（ A )。

A 网络环路 B 根本没有影响 Ｃ 短路 D 回路

（115）企业重要数据要及时进行（ C )，以防出现以外情况导致数据丢失。

Ａ杀毒 Ｂ加密 Ｃ备份

（116）.WINDOWS主机推荐使用（ A）格式

A NTFS B FAT32 C FAT D LINUX

二、多选题

(1)网络安全工作的目标包括（ABCD）

A、信息机密性;B、信息完整性;C、服务可用性；D、可审查性

(2)智能卡可以应用的地方包括（ABCD）

A、进入大楼；

B、使用移动电话;

C、登录特定主机；

D、执行银行和电子商务交易

(3）计算机信息系统安全保护的目标是要保护计算机信息系统的（ABCD)

（A)实体安全

（B)运行安全

（C）信息安全

（D）人员安全

（4）计算机信息系统的运行安全包括(ABC）

（A）系统风险管理

（B）审计跟踪

（C)备份与恢复

(D）电磁信息泄漏

(5）实施计算机信息系统安全保护的措施包括（AB）

（A）安全法规

(B)安全管理

（C）组织建设

(D)制度建设

(6)计算机信息系统安全管理包括（ACD）

（A)组织建设

(B)事前检查

（C)制度建设

（D)人员意识

(7)公共信息网络安全监察工作的性质(ABCD)

(A)是公安工作的一个重要组成部分

(B)是预防各种危害的重要手段

(C)是行政管理的重要手段

(D）是打击犯罪的重要手段

(8）公共信息网络安全监察工作的一般原则（ABCD)

（A)预防与打击相结合的原则

（B)专门机关监管与社会力量相结合的原则

(C）纠正与制裁相结合的原则

(D）教育和处罚相结合的原则

（9）安全员应具备的条件: （ABD)

（A)具有一定的计算机网络专业技术知识

（B）经过计算机安全员培训,并考试合格

(C）具有大本以上学历

（D)无违法犯罪记录

(10）网络操作系统应当提供哪些安全保障（ABCDE)

（A)验证(Authentication）

(B）授权(Authorization)

（C）数据保密性(Data Confidentiality）

（D)数据一致性(Data Integrity）

(E)数据的不可否认性（Data Nonrepudiation)

(11)Windows NT的”域"控制机制具备哪些安全特性？（ABC）

(A)用户身份验证

(B)访问控制

（C）审计(日志)

（D)数据通讯的加密

(12)从系统整体看，安全"漏洞”包括哪些方面(ABC）

（A）技术因素

(B)人的因素

(C）规划，策略和执行过程

（13）从系统整体看，下述那些问题属于系统安全漏洞（ABCDE)

（A）产品缺少安全功能

（B）产品有Bugs

（C）缺少足够的安全知识

（D)人为错误

（E)缺少针对安全的系统设计

（14)应对操作系统安全漏洞的基本方法是什么?（ABC)

(A)对默认安装进行必要的调整

（B）给所有用户设置严格的口令

(C)及时安装最新的安全补丁

（D)更换到另一种操作系统

(15）造成操作系统安全漏洞的原因（ABC）

（A)不安全的编程语言

（B)不安全的编程习惯

(C）考虑不周的架构设计

（16)严格的口令策略应当包含哪些要素(ABCD)

（A)满足一定的长度,比如8位以上

（B）同时包含数字，字母和特殊字符

（C）系统强制要求定期更改口令

（D）用户可以设置空口令

（17)计算机安全事件包括以下几个方面(ABCD）

(A）重要安全技术的采用

(B)安全标准的贯彻

(C)安全制度措施的建设与实施

（D）重大安全隐患、违法违规的发现，事故的发生

(18）计算机案件包括以下几个内容(ABC）

（A)违反国家法律的行为

(B）违反国家法规的行为

（C)危及、危害计算机信息系统安全的事件

(D)计算机硬件常见机械故障

（19)重大计算机安全事故和计算机违法案件可由\_\_\_\_\_受理(AC）

（A)案发地市级公安机关公共信息网络安全监察部门

（B)案发地当地县级（区、市）公安机关治安部门

(C）案发地当地县级（区、市）公安机关公共信息网络安全监察部门

(D）案发地当地公安派出所

(20)现场勘查主要包括以下几个环节\_\_\_\_\_（ABCD）

(A)对遭受破坏的计算机信息系统的软硬件的描述及被破坏程度

(B）现场现有电子数据的复制和修复

(C)电子痕迹的发现和提取,证据的固定与保全

(D)现场采集和扣押与事故或案件有关的物品

(21)计算机安全事故原因的认定和计算机案件的数据鉴定,\_\_\_\_ （ABC）

(A）是一项专业性较强的技术工作

（B）必要时可进行相关的验证或侦查实验

（C）可聘请有关方面的专家，组成专家鉴定组进行分析鉴定

(D）可以由发生事故或计算机案件的单位出具鉴定报告

（22）有害数据通过在信息网络中的运行,主要产生的危害有(ABC)

（A)攻击国家政权，危害国家安全

（B）破坏社会治安秩序

（C)破坏计算机信息系统，造成经济的社会的巨大损失

（23）计算机病毒的特点\_\_\_\_\_\_（ACD）

（A）传染性

（B）可移植性

（C）破坏性

（D)可触发性

(24)计算机病毒按传染方式分为\_\_\_\_(BCD）

(A)良性病毒

（B)引导型病毒

(C)文件型病毒

(D）复合型病毒

(25)计算机病毒的危害性有以下几种表现（ABC)

(A)删除数据

（B)阻塞网络

（C）信息泄漏

(D）烧毁主板

(26）计算机病毒由\_\_\_\_\_部分组成（ABD)

(A）引导部分

(B）传染部分

（C)运行部分

(D）表现部分

（27)以下哪些措施可以有效提高病毒防治能力（ABCD)

(A）安装、升级杀毒软件

(B）升级系统、打补丁

（C)提高安全防范意识

（D）不要轻易打开来历不明的邮件

（28）计算机病毒的主要传播途径有（ABCD）

（A)电子邮件

（B)网络

(C)存储介质

(D)文件交换

（29）计算机病毒的主要来源有\_\_\_\_（ACD）

(A）黑客组织编写

（B）计算机自动产生

（C）恶意编制

(D）恶作剧

（30)发现感染计算机病毒后，应采取哪些措施（ABC)

（A）断开网络

（B)使用杀毒软件检测、清除

（C)如果不能清除,将样本上报国家计算机病毒应急处理中心

(D）格式化系统

三、判断题:

1.VPN的主要特点是通过加密使信息能安全的通过Internet传递。√

2。密码保管不善属于操作失误的安全隐患.X

3.漏洞是指任何可以造成破坏系统或信息的弱点。√

4。安全审计就是日志的记录。X

5。计算机病毒是计算机系统中自动产生的。X

6.对于一个计算机网络来说,依靠防火墙即可以达到对网络内部和外部的安全防护X

7.网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。X

8。最小特权、纵深防御是网络安全原则之一。√

9。安全管理从范畴上讲，涉及物理安全策略、访问控制策略、信息加密策略和网络安全管理策略。√

10。用户的密码一般应设置为16位以上。√

11。开放性是UNIX系统的一大特点。√

12。防止主机丢失属于系统管理员的安全管理范畴。X

13。我们通常使用SMTP协议用来接收E-MAIL。X

14。在堡垒主机上建立内部DNS服务器以供外界访问,可以增强DNS服务器的安全性.X

15.为了防御网络监听,最常用的方法是采用物理传输。X

16.使用最新版本的网页浏览器软件可以防御黑客攻击。√

17.WIN2000系统给NTFS格式下的文件加密，当系统被删除，重新安装后，原加密的文件就不能打开了。√

18.通过使用SOCKS5代理服务器可以隐藏QQ的真实IP。√

19。一但中了IE窗口炸弹马上按下主机面板上的Reset键，重起计算机。X

20.禁止使用活动脚本可以防范IE执行本地任意程序。√

21.只要是类型为TXT的文件都没有危险。X

22。不要打开附件为SHS格式的文件.√

23。发现木马，首先要在计算机的后台关掉其程序的运行。√

24。限制网络用户访问和调用cmd的权限可以防范Unicode漏洞。√

25.解决共享文件夹的安全隐患应该卸载Microsoft网络的文件和打印机共享。√

26。不要将密码写到纸上。√

27。屏幕保护的密码是需要分大小写的.√

28。计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒.√

29。木马不是病毒.√

30．复合型防火墙防火墙是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用，同时也常结合过滤器的功能。√

31。非法访问一旦突破数据包过滤型防火墙，即可对主机上的软件和配置漏洞进行攻击。X

32。ATM 技术领先于TCP/IP技术，即将取代IP技术，实现语音、视频、数据传输网络的三网合一X

33。Internet设计之初，考虑了核战争的威胁，因此充分考虑到了网络安全问X

34.我的计算机在网络防火墙之内，所以其他用户不可能对我计算机造成威胁X

33。Internet没有一个集中的管理权威√

34。统计表明，网络安全威胁主要来自内部网络，而不是Internet√

35。蠕虫、特洛伊木马和病毒其实是一回事X

36.只要设置了足够强壮的口令,黑客不可能侵入到计算机中X

37。路由器在转发IP分组时，一般不检查IP分组的源地址，因此可以伪造IP分组的源地址进行攻击，使得网络管理员无法追踪。√

38。发起大规模的DDoS攻击通常要控制大量的中间网络或系统√

39。路由协议如果没有认证功能，就可以伪造路由信息，导致路由表混乱,从而使网络瘫痪√

40.目前入侵检测系统可以及时的阻止黑客的攻击。X

41。TCSEC是美国的计算机安全评估机构和安全标准制定机构√

42在Winodws NT操作系统中每一个对象(如文件，用户等）都具备多个SID X

43。Windows NT域（Domain）中的用户帐号和口令信息存储在"域控制器"中√

44。Windows NT中用户登录域的口令是以明文方式传输的X

45。只要选择一种最安全的操作系统，整个系统就可以保障安全X

46.在计算机系统安全中，人的作用相对于软件,硬件和网络而言，不是很重要X

47.在设计系统安全策略时要首先评估可能受到的安全威胁√

48。安装系统后应当根据厂商或安全咨询机构的建议对系统进行必要的安全配置√

49。系统安全的责任在于IT技术人员，最终用户不需要了解安全问题X

50．网络的发展促进了人们的交流，同时带来了相应的安全问题X

51．具有政治目的的黑客只对政府的网络与信息资源造成危害X

52.病毒攻击是危害最大、影响最广、发展最快的攻击技术X

53。黑色星期四”是因有人通过BELL实验室与Internet连接的有漏洞的机器

54。上放置了一个蠕虫程序而引起网络灾难得名的X

55。在信息战中中立国的体现要比非信息战简单X

56。信息战的军事目标是指一个国家军队的网络系统、信息系统、数据资源X

57。计算机病毒是计算机系统中自动产生的X

58。小球病毒属于引导型病毒√

59。公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作√

60.计算机病毒防治产品实行销售许可证制度√

61.计算机病毒防治产品分为三级，其中三级品为最高级X

62，删除不必要的网络共享可以提高防范病毒的能力√

63。DMZ 为非军事区√

64.带VPN的防火墙一旦设置了VPN 功能，则所有通过防火墙的数据包都将

65.通过VPN通道进行通讯X

66。VPN的所采取的两项关键技术是认证与加密√

67.要保证一个公司总部与其分支机构的网络通讯安全只有通过VPN来实现X

68.网络安全工程实施的关键是质量,而质量的关键是服务的长期保障能力√

69网络安全服务的开展与网络安全防范是一对矛盾√

70.网络安全边界防范的不完备性仅指防外不防内X

71使用最新版本的网页浏览器软件可以防御黑客攻击。X

２不要将密码写到纸上.√

３WIN2000系统给NTFS格式下的文件加密，当系统被删除,重新安装后，原加密的文件就不能打开了。√

5计算机数据恢复在实际生活当中可以百分百恢复.X

6违反国家法律、法规的行为，危及计算机信息系统安全的事件，称为计算机案件.√

7计算机犯罪是行为人以计算机为工具或以计算机资产为犯罪对象实施的，依照我国刑法应受处罚的,具有社会危害性的行为。√

8。 计算机信息系统的安全威胁同时来自内、外两个方面。 √

9。公司计算机出现故障，员工可以自行带到公司外面维修X

10 外单位人员如可以随意接入奇瑞公司内网.X

11。格式化过后的计算机，原来的数据就找不回来了X

四、填空：

1． 信息安全包含：\_\_物理\_\_\_\_安全、\_\_\_\_信息系统\_\_\_\_\_\_\_\_安全和\_\_数据\_安全。

2。 数据安全包含\_\_\_可用性\_、\_\_\_\_完整性\_\_、\_\_\_保密性\_三个基本特性。

2．公司对电脑密码的强壮度要求是：\_字母加数字组合8位以上\_\_\_\_.

3．员工离开自己的计算机时要立即设置\_\_\_锁屏\_\_\_\_\_\_\_\_\_。

4.信息安全四大要素是：\_\_技术、\_\_\_制度、流程、\_\_\_人\_。

5.未来信息安全的发展趋势是由\_\_\_\_\_防外\_转变为\_\_\_\_\_防内\_\_\_\_。

6。 新修订《刑法》中有关失泄密处罚条款：以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的，给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上\_\_七\_\_年以下有期徒刑,并处罚金

7。工作人员因工作需要必须使用Internet时,需由各部门信息化管理员提交\_\_\_OA\_\_申请.

简答：

1 公司制定信息化安全管理操作规范的目的？

为了保护奇瑞公司的自主知识产权，保证奇瑞公司所有数据的安全、

信息系统和计算机本身的稳定以及规范管理员工的行为操作，特制定本操

作规范

2控制USB接口使用的目的?

1，网络的安全。2，信息的保密

二

一、选择题

1、不属于安全策略所涉及的方面是（ C ）。

A、访问控制策略 B、物理安全策略 C、防火墙策略 D、信息加密策略

2、属于安全服务产品的是 ( A）。

A、安全运营管理 B、可信计算平台 C、PKI/CA D、恶意代码防范软件

3、各国电信主管部门之间协调电信事物的国际组织是（ B )。

A、国际电子技术协议(IEC） B、国际电信联盟(ITU） C、电子工业协会（EIA) D、通信工业协会（TIA）

4、大多数网关防毒产品不能支持的协议是（ c ）。P77

A、 HTTP B、FTP C、POP3 D、SMTP

5、构建可信计算平台的基础模块是（ A ）

A、安全启动系统 B、可信平台模块 C、安全协处理器 D、密码加速器

6、如果一个单位的两个部分各有一个局域网，那么将它们互联的最简单的方法是使用（ C )

A。 网关 B。 中继器 C. 路由器 D. 网桥

7、（ D ）协议主要用于加密机制。

A、HTTP B、FTP C、TELNET D、SSL

8、目前，用于企业内部自建VPN的主要技术有两种——IPSec VPN和（ B )

A、SLL VPN B、SSL VPN C、IPSL VPN D、LAN VPN

9、用公钥加密，用私钥解密，主是为了保证信息的（ A ）。

A 保密性 B 完整性 C身份确认性 D 不可否认性

10、实现有线网络与移动通信网络互连的协议是（ B ）.

A、IP B、WAP C、WWW D、HTTP

11、一般地，可以从三个层次实施恶意代码的防范，分别为:网络边界防护、集群服务器/邮件系统防护、（ B ）

A、文件病毒防护 B、主机病毒防护 C、文件木马防护 D、主机木马防护

12、从逻辑上来看,密钥管理系统又由密钥生成子系统、密钥库子系统、( A ）、密钥管理子系统和管理终端组成。

A、密钥恢复子系统 B、密钥存储子系统 C、密钥销毁子系统 D、密钥加密子系统

13、目前，防火墙的类型或者实现形式主要有四类：嵌入式防火墙、（ D )、硬件防火墙和应用程序防火墙。

A、终端防火墙 B、主机防火墙 C、网关防火墙 D、软件防火墙

14、能够隐藏内部网络IP地址的技术是( C）.

A、防火墙 B、VPN C、代理服务 D、入侵检测系统

15、关于网关杀毒的主要实现方式下列说法中不正确的是（ D ）

A、基于代理服务器的方式 B、基于防火墙协议还原的方式

C、基于邮件服务器的方式 D、基于解析服务器的方式

16、目前主要有两种不同的PKI开发模式，分别是（ A )

A、面向产品的开发模式和面向服务的开发模式 B、面向产品的开发模式和面向技术的开发模式

C、面向技术的开发模式和面向服务的开发模式 D、面向企业的开发模式和面向服务的开发模式

17、风险评估指的是对信息和信息处理设施的威胁、( B ）和脆弱性这三个因子及三者发生的可能性进行评估。

A、攻击 B、影响 C、风险 D、漏洞

18、在进行风险评估时，应考虑的对应关系主要是（ A ）

A、资产与威胁的对应关系 A、资产与影响的对应关系 A、资产与可能性的对应关系 A、价值与威胁的对应关系

19、人员能力成熟度模型将人员能力成熟度划分为（ D)个级别

A、3 B、7 C、22 D、5

20、数据安全的目的是实现数据的机密性、( C ）、可控性、不可否认性,并进行数据备份和恢复。

A、唯一性 B、不可替代性 C、完整性 D、可确认性

二、填空题

1、国际标准化组织中，最重要的两个组织是 ISO 和 IEC 。

2、信息安全保障的三个要素是 人 、 技术 和 管理 。

3、 网桥 是连接两个协议差别很大的计算机网络时使用的设备。

4、远程证明技术主要包括 语义 、 属性 和 软件 三种。

5、借鉴软件工程中的相关知识，对体系结构的描述经常采用 视图 的方法，并且主要有三类视图，即 物理 视图、 逻辑 视图和 概念 视图。

6、可以将安全策略分为 管理性 安全策略和 技术性 安全策略。

7、认证体系的核心是 CA 。

8、 安全运营管理 是面向信息系统运行阶段的安全服务产品。

9、访问OCSP服务器查询用户证书状态时，OCSP会返回 有效 、 无效 和 未知 三种状态。

三、名词解释题

写出下列英文缩写的含义。

1、ISO：国际标准化组织

2、CIDF：通用入侵检测框架 3、CA：数字证书认证机构

4、DOS：拒绝服务 5、P-CMM：人员能力成熟度模型

四、简答题

1、 简述进行风险评估的五个步骤.P155

答：按照组织商务动作流程进行资产识别、并根据估价原则对资产进行评估。

根据资产所处的环境进行威胁识别与评价.

对应每一威胁，对资产或组织存在的脆弱性进行识别与评价。

对已采取的安全控制进行确认。

建立风险测量的方法及风险等级评价原则,确定风险的大小与等级。

2、 简述人员能力成熟度模型将人员能力划分的五个级别。P200

答:初始级，可管理级,可定义级,可预知级，优化级。

3、 依据防火墙的实现形式，它可以分为哪几类？p107

答：嵌入式防火墙，软件防火墙，硬件防火墙，应用程序防火墙。

4、 下一代入侵检测产品可能涉及哪些关键技术？p105

答：智能关联，告警泛滥抑制，告警融合.

5、 简述网关杀毒的四种实现方式。P124

答:基于代理服务器的方式,基于防火墙协议还原的方法，基于邮件服务器的方法,基于信息渡轮产品的方法。

6、简述授权体系的基本结构.P69

五、论述题

1、 简述PKI/CA两种开发模式的不同之处。P128

2、 可信计算平台的可信机制通过哪三个方面来体现?简述这三个方面的作用。P133

三

信息安全技术

第1章 计算机信息安全概述

1．填空题

1．数据源点鉴别服务是开发系统互连第N层向\_N+1\_\_\_\_\_\_\_\_层提供的服务.

2．对等实体鉴别服务是数据传输阶段对对方实体的\_\_\_合法性\_\_\_\_\_进行判断。

3．计算机信息安全技术研究的内容应该包括三个方面：计算机外部安全、计算机信息在存储介质上的安全、 计算机网络安全 。

4．影响计算机信息安全的因素大至可分为四个方面： 人为恶意破坏 、自然灾害、人为疏忽、软件设计等不完善等。

5．我们将计算机信息安全策略分为三个层次：政策法规层、 安全管理层 、安全技术层。

6．信息资源的典型特点是:一旦被一人占有，就 不能 被其他人占有。

3．简答题

1．什么是TEMPEST技术？答：TEMPEST技术（美国国家安全局和国防部联合研究开发）的主要目的是防止计算机系统中因电磁辐射而产生的信息泄密

2．信息的完整性 答:完整性技术是保护计算机系统内软件和数据不被偶然或人为蓄意地破坏、篡改、伪造等

3．信息的可用性 答：可用性技术是在用户授权的条件下，信息必须是可用的

4．信息的保密性 答：保密性技术是防止信息失窃和泄露的技术，信息必须按照信息拥有者的要求保持一定的秘密性。

4．问答题

1．对计算机信息系统安全构成威胁的主要因素有哪些?

(1)直接对计算机系统的硬件设备进行破坏

（2）对存放在系统存储介质上的信息进行非法获取、篡改和破坏等

（3)在信息传输过程中对信息非法获取、篡改和破坏等 从信息源到信息传输

2．从技术角度分析引起计算机信息系统安全问题的根本原因是什么?

3．计算机信息安全研究的主要内容有哪些？（１）计算机外部安全

（２）计算机信息在存储介质上的安全，也称计算机内部安全

（３）计算机信息在传输过程中的安全，即计算机网络安全

4．什么是信息的完整性、可用性、保密性?答：(1）完整性技术是保护计算机系统内软件和数据不被偶然或人为蓄意地破坏、篡改、伪造等 .（2） 可用性技术是在用户授权的条件下，信息必须是可用的 。（3）保密性技术是防止信息失窃和泄露的技术，信息必须按照信息拥有者的要求保持一定的秘密性。

5．安全体系结构ISO7498-2标准包括哪些内容？

鉴别(authentication）

访问控制（access control)

数据保密（data confidentiality）

数据完整性(data integrity）

抗否认（non—reputation)

6．计算机系统的安全策略内容有哪些？答:计算机系统的安全策略是指在特定的环境下,为保证一定级别的安全要求所提出的一系列条例、规则和方法。安全策略可分为政策法规层、安全管理层、安全技术层三个层次。（1）政策法规层是为建立安全规章制度和合理使用安全技术提供的法律保护,同时通过立法和政策导向来提高人的职业道德，对人进行伦理教育，净化社会环境。(2)安全管理层将涉及到具体单位和个人，为实施安全技术提供具体保护。包括组织管理机构、人事管理和计算机系统管理。（3）安全技术层可以通过物理方法和逻辑方法（或软件方法)来实现。1）物理安全策略是保护计算机等硬件实体免受破坏和攻击；2）逻辑方法是通过访问控制、加密、防火墙、安全操作系统等方法以阻挡非法侵入。

7．在计算机安全系统中人、制度和技术的关系如何?答：规章制度是计算机安全体系的基础，是安全的最重要的因素。第二个重要因素就是人,任何保护措施没有人的参与都是毫无意义的。从这个意义上来说，人是对计算机信息安全最大的威胁。安全技术实际上是用来帮助人们实现安全防护的手段，提高安全防护的能力.强化规章制度执行，提高人们的安全防范意识，提高人们的道德水准比安全技术更重要。

8．什么是计算机系统的可靠性？计算机可靠性包含哪些内容？

答:计算机系统的可靠性是指在给定的时间内，在一定的条件下，计算机系统能完成应的能力。从宏观上来说可靠性可以分为硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。就硬件来说，使用时间越长，“磨损”越大，就越容易出故障。软件则相反，使用时间越长越可靠，软件没有“磨损”等问题

9．提高计算机系统的可靠性可以采取哪两项措施?答：提高计算机系统的可靠性可以采取避错和容错两项措施。

10．容错系统工作过程包括哪些部分？每个部分是如何工作的？答：容错系统工作过程包括自动检测、自动切换和自动恢复部分

11．容错设计技术有哪些？答:（1）硬件冗余设计通过增加硬件资源来获得容错能力的.（2）信息冗余设计在数据中外加一部分信息位来检测或纠正信息在运算或传输中的错误而达到容错功能。（3)软件冗余设计用多个不同软件，采用不同的算法,执行同一功能，及时发现程序设计错误,提高系统的可靠性

12． 故障恢复策略有哪两种?答:故障恢复策略有前向恢复和后向恢复两种。前向恢复是指在发生故障时,当前的任务继续进行,同时把系统恢复成连贯的正确状态，弥补当前状态的不连贯情况，这种方法适合实时处理。后向恢复是指在发生故障时,系统恢复到前一个正确状态,再继续执行，这种方法不能用于实时处理。

13．什么是恢复块方法、N—版本程序设计和防卫式程序设计?

5．选择题

1．\_\_D\_\_\_\_\_\_是防止发送方在发送数据后又否认自己行为，接收方接到数据后又否认自己接收到数据。

A。 数据保密服务 B。 数据完整性服务

C。 数据源点服务 D. 禁止否认服务

2．鉴别交换机制是以\_\_\_\_A\_\_\_\_的方式来确认实体身份的机制。

A. 交换信息 B。 口令

C。 密码技术 D。 实体特征

3．数据源点鉴别服务是开发系统互连第N层向 \_\_A\_\_\_\_\_层提供的服务

A . N+1 B。 N—1 C . N+2 B. N-2

4．从技术上说，网络容易受到攻击的原因主要是由于网络软件不完善和 (C) 本身存在安全漏洞造成的。

A．人为破坏 B．硬件设备

C．操作系统 D．网络协议

5．对等实体鉴别服务是数据传输阶段对 (A） 合法性进行判断。

A．对方实体 　　　 B．对本系统用户

C．系统之间　　　　　 D．发送实体

6．在无信息传输时，发送伪随机序列信号，使非法监听者无法知道哪些是有用信息，哪些是无用信息.(A ）

A．公证机制　　　　　　　　　B．鉴别交换机制

C．业务流量填充机制　 　　 D．路由控制机制

7.在系统之间交换数据时，防止数据被截获.（C )

A．数据源点服务 B． 数据完整性服务

C．数据保密服务 D． 禁止否认服务

8．以交换信息的方式来确认对方身份的机制.（B）

A．公证机制　　　　　　　　　 B．鉴别交换机制

C．业务流量填充机制　 　　 D．路由控制机制

第2章 密码与隐藏技术

1．填空题

1．如果当明文字母集与密文字母集是一对一映射时，则密钥长度是\_\_\_\_\_\_\_。

2．DES算法是对称或传统的加密体制,算法的最后一步是\_\_\_\_\_\_\_\_\_\_\_\_。

3．公开密钥体制中每个成员有一对密钥，它们是公开密钥和\_\_\_\_\_\_\_\_\_\_。

4．在RSA算法中已知公开模数r = p?q，则欧拉函数 （r) = \_\_\_\_\_\_\_\_\_\_\_\_。

5．代替密码体制加密时是用字母表中的另一个字母\_\_\_\_\_\_\_明文中的字母。

6．如果a?b ≡ b mod r成立，则称a与b对模r是\_\_\_\_\_\_\_的.

7．换位密码体制加密时是将改变明文中的字母\_\_\_\_\_\_\_\_\_，本身不变。

8．DES算法加密明文时，首先将明文64位分成左右两个部分，每部分为\_\_\_\_\_\_位。

9．在密码学中明文是指可懂的信息原文；密文是指明文经变换后成为 识别的信息。

10．在密码学中加密是指用某种方法伪装明文以隐藏它的内容过程；解密是指将密文变成 的过程.

11．DES 是分组加密算法，它以 位二进制为一组，对称数据加密,64位明文输出.

12．DES是对称算法，第一步是 最后一步是逆初始变换IP 。

13．利用欧几里德算法，求最大公约数算法时，即重复使用带余数除法,直到余数为 时，则上次余数为最大公约数。

14．公开密钥算法知道了加密过程不能推导出解密过程，即不能从 或从pk推导出sk。

15．传统加密算法知道了加密过程可以 出解密过程.

16．欧拉函数 用来计算1、2、3，?？？，r 中有多个数与 互质。

17．AES算法的每轮变换由四种不同的变换组合而成，它们分别是 、行位移变换、列混合变换和圈密钥加法变换.

18．设两个整数a、b分别被m除，如果所得余数相同，则称a与b对模m是 。

19．鲁棒性（robustness）指嵌入有水印的数字信息经过某种改动或变换之后，数字水印 破坏，仍能从数字信息中提取出水印信息。

20． RSA算法的安全性取决于p、q保密性和已知r=p？q分解出p、q的 。

21．AES算法是一种 密码体制,其明文分组长度、密钥长度可以是128比特、192比特、256比特中的任意一个。

22．水印容量是指在数字信息中加入的 。

23．现代密码学两个主要研究方向是对称密码体制和公开密钥体制，其中公开密钥体制典型代表是 。

24．DES 是分组加密算法，它以64位为一组，对称数据加密，64位明文输入, 密文输出。

25．古典移位密码是将明文字符集循环向前或向后移动一个或多个 位置。

26．当AES的输入明文分组长度为128位时，经AES加密处理后,得到的输出是 。

27． AES算法中，有限域GF（28)中的两个元素相加可以定义为其系数是两个多项式对应系数的 .

27．AES算法处理的基本单位是 和字。

29．求乘逆时可以利用欧几里德算法，即重复使用带余数除法，每次的余数为除数除上一次的除数，直到余数为 时为止。

30． 是DES算法的核心部分，它提供很好的混乱数据效果，提供了更好的安全性.

31．换位密码体制思想是改变明文中字母的位置,明文中的字母 。

32．在密码学中加密E是指用某种方法伪装明文以隐藏它的内容过程；解密是指将密文变成 的过程。

33．当AES算法输入为 位，输出为128位。

34．目前计算机密码学有两个研究方向，其中传统方法的计算机加密体制(或对称密码体制）,典型代表有 算法等.

35．在公开密钥体制中，每个成员都有一对密钥.其中一个密钥如个人电话号码一样可查找,这个密钥通常称为公开密钥。另一个密钥是保密的，不可让其他人知道，这个密钥通常称为 .

3．简答题

1．解释AES算法中的数据块长Nb

2．AES算法中的密钥长Nk

3．AES算法中的变换轮数N

4．AES算法中的状态state

5．AES算法中的圈密钥

6．AES算法中的扩展密钥

7．数字水印

4．问答题

1．请说明研究密码学的意义以及密码学研究的内容。

2．古典代替密码体制和换位密码体制有什么特点?

3。 请比较代替密码中移位密码、单表替代密码和多表替代密码哪种方法安全性好，为什么？

4．写出DES算法步骤。

5．仔细观察DES的初始置换表，找出规律，并用数学表达式表示。

6．DES加密过程与解密过程有什么区别？

7．AES与DES相比较有哪些特点？

8．请设计AES算法加密过程的流程图.。

9．画出AES的扩展密钥生成流程图。

10．写出AES扩展密钥程序涉及三个RotWord（）、SubWord（）和Rcon［]模块的工作方式。

11．AES加密和解密时使用圈密钥有什么区别？

12．对称加密体制与公开密钥加密体制有什么特点？

13．请设计RSA算法流程图。

14．使用RSA算法时选择有关参数应注意哪些问题？

15．在一个使用RSA的公开密钥系统中，假设用户的私人密钥被泄露了,他还使用原来的模数,重新产生一对密钥，这样做安全吗?

16．NTRU算法密钥是如何产生的？

17．写出NTRU算法加密与解密方程。

18．什么是信息隐藏术？什么是数字水印?

19．画出数字水印的通用模型？

20．数字水印有哪些主要特性？

21．典型数字水印算法有哪些？

22．请设计AES算法解密过程的流程图。

6．选择题

1．在DES算法中扩展置换后的E(R)与子密钥k异或后输入\_\_\_\_\_\_\_到S盒代替。

A。 64位 B. 54位　　　C. 48位 D. 32位

2．RSA算法的安全性取决于r = p？q中\_\_\_\_\_\_\_\_\_和p、q的保密性。

A。 r 大小 B。 p ， q的分解难度

C. 与p、q无关 D 与p、q有关

3．求最大公约数时依然使用重复带余数除法，直到余数为\_\_\_\_\_\_\_\_时为止。

A。 0 B. 1 C。 2 D。 3

4．在DES算法中，需要将明文分组右半部扩展置换,扩展置换是实现明文换位和\_\_\_\_\_\_扩展.

A。 24位到48位 B. 32位到48 位

C。 64位到128位 D. 16位到32位

5．求乘逆时采用欧几里德算法,即重复使用带余数除法直到余数为\_\_\_\_\_\_\_\_时为止。

A。 0 B。 1 　C。 2 D。 3

6．用DES算法生成子密钥时,需要将原密钥\_\_\_\_\_\_\_压缩置换.

A。 56位 B. 48位

C。 64位 D. 28位

7．在RSA算法中需要选择一个与 （ r ）互质的量k，k值的大小与r关系是\_\_\_\_\_。

A。 无关 B. k > r

C。 k = r D. k < r

8．在RSA算法中需要选择一个与 （r) 互质的量k，k值的大小与 (r)关系是\_\_\_\_\_。

A。 无关 B. k 〉 (r)

C。 k = （r） D。 　k 〈 （r)

9．使用S盒时如S盒的输入为a a a a a a ，则取a a 作为S盒的列号j 取a a a a 作为S盒的列号i，对应S盒的\_\_\_\_\_\_\_元素为S盒输出。

A．(1，i） B． （i,1) C．（i,j) D．（j， i）

10．设a?b 1（mod r) 已知a，求b，称求a对于模r的乘逆b，称a、b对r \_\_\_\_\_。

A、互为乘逆 B、互为乘法

C、互为余数 D、互为质数

11．在DES算法中，使用S盒时要将48位输入按顺序每\_\_\_\_\_\_位分为一组。

A．4 B．6 C．8 D．16

12．AES中将一个4字节的字可以看成是系数在GF（28）中并且次数小于 的多项式。

A．2 B．3 C．4 D．5

13．是DES算法的核心部分，它提供很好的混乱数据效果，提供了更好的安全性。

A．S盒代替 B．P盒置换

C．压缩置换 D．扩展置换

14．DES算法进行将置换后的明文,即新的64位二进制序列，按顺序分为左、右两组L 和 R , 每组都是 。

A．16位 B．32位 C．64位 D．128位

15．AES算法是一种分组密码体制，其明文分组长度、密钥长度可以是128比特、192比特、256比特中的任意一个，其中AES—128表示 。

A．明文长度 B． 密钥长度

C．密文长度 D．算法位数

16．在开始进入一轮DES时先要对密钥进行分组、移位。 56位密钥被分成左右两个部分，每部分为28位。根据轮数，这两部分分别循环左移 .

A．1位或2位 B．2位或3位

C．3位或4位 D．4位或5位

17．AES算法的每轮变换由四种不同的变换组合而成，它们分别是S-盒变换、行位移变换、列混合变换和圈密钥加法变换。

A．S-盒变换 B．Y-盒变换

C．X-盒变换 D．Z-盒变换

18．AES中的状态可以用二维字节数组表示，它有 、Nb列，其中数组中元素单位为字节，Nb的单位为字。

A. 2行 B. 4行 C. 8行 D. 16行

19．在对称加密体制中，如果有n个用户，则需要密钥个数为

A．n(n+1）/2 B．2n C．n(n—1)/2 D．n(n—1)

20．DES 是分组加密算法,它以 二进制为一组，对称数据加密.

A． 32位 B．64位 C．128位 D．256位

21．DES算法是分组加密算法，它利用密钥，通过传统的换位、替换和 运算等变换实现二进制明文的加密与解密。

A．异或 B．或 C．与 D．非

22．AES算法利用外部输入字数为Nk的密钥串K，通过扩展密钥程序得到共 字的扩展密钥串。

A．Nb \* （Nr + l） B．Nb ＊ Nr

C．Nb ＊ (Nk + l） D．Nb ＊ Nk

23．RSA算法需要计算m mod r等值,由于m 值巨大，可以使用 来计算m mod r。

A．压缩算法 B．平方—乘算法

C．扩展算法 D．置换算法

24．AES算法的每轮变换由四种不同的变换组合而成，它们分别是 、行位移变换、列混合变换和圈密钥加法变换。

A．X-盒变换 B．F-盒变换 C． S-盒变换 D．D-盒变换

第3章 数字签名与认证

2．填空题

1．对输入任意长度明文,经MD5算法后，输出为 。

2．DSA的安全性主要是依赖于有限域上离散对数问题求解的 性。

3．单向散列函数，也称hash函数,它可以为我们提供电子信息完整性的判断依据，是防止信息被 的一种有效方法。

4．生物特征识别技术是根据人体本身所固有的生理特征、行为特征的 性，利用图像处理技术和模式识别的方法来达到身份鉴别或验证目的的一门科学。

5．人体本身的生理特征包括面像、 、掌纹、视网膜、虹膜和基因等。

6． 技术是通过分析指纹的全局特征和局部特征从指纹中抽取的特征值，从而通过指纹来确认一个人的身份。

7． 就是主要用于对数字信息进行的签名，以防止信息被伪造或篡改等。

8．hash函数的作用是当向hash函数输入一任意长度的的信息M时,hash函数将输出一 为m的散列值h。

9．为了提高数字签名的安全性和效率，通常是先对明文信息M作 变换,然后再对变换后的信息进行签名。

10．DSS (Digital Signature Standard）是利用了安全散列函数(SHA）提出的一种 技术。

11．MD5是以512位分组来处理输入的信息，每一分组又被划分为 个32位子分组

3．简答题

1．数字签名

2．Kerberos 身份验证系统由

3．公开密钥基础设施PKI

4．数字证书

5．解释X.509

6．解释PKCS

7．解释OCSP含义

8．解释LDAP含义

9．解释PKIX含义

4．问答题

1．什么是数字签名？在网络通信中数字签名能够解决哪些问题？

2．写出基于公开密钥的数字签名方案。

3．写出DSA算法过程。

4． DSA算法指出如果签名过程导致 s = 0时,就应该选择一个新的k值,并重新计算签名，为什么？如果k值被泄露，将会发生什么情况？

5．安全的散列函数有哪些特征？

6．简述数字签名的过程.

7．分析SHA 安全散列算法过程。

8．比较在MD5中四个初始变量A、B、C、D的值（小数在前的存储方式）与SHA-1中五个初始变量A、B、C、D、E的值（大数在前的存储方式）的关系。

9．什么是PGP加密软件？

10．Kerberos 身份验证系统由哪几部分组成?写出Kerberos鉴别协议步骤。

11．什么是公开密钥基础设施PKI？PKI由哪几部分基本组成?

12．什么是数字证书？X。509数字证书包含哪些内容?

13．对PKI的性能有哪些要求？

14．你是如何为自己的存折选密码的？为什么？

15．我们在选用密码时，应该注意哪些问题？

16．生物特征识别技术的基本原理是什么?

17．一个生物识别系统包括哪些内容？

18．指纹的总体特征和局部特征有哪些？指纹采集常用的设备有哪些？

19．虹膜的生物特征识别技术的基本依据是什么？

20．你还知道哪些生物识别方法？

21．智能卡是由哪几部分组成的?有什么特点？

6．选择题

1．MD5算法将输入信息M按顺序每组 长度分组，即：M1，M2,…，Mn—1，Mn。

A．64位 B．128位

C．256位 D。 512位

2．PGP加密算法是混合使用 算法和IDEA算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件.

A．DES B．RSA C．IDEA D．AES

3． 就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A．公开密钥体制 B． 对称加密体制

C．PKI（公开密钥基础设施） D．数字签名

4．在为计算机设置使用密码时，下面 密码是最安全。

A．12345678 B．66666666

C．20061001 D．72096415

5．PGP加密算法是混合使用RSA算法和IDEA等算法，它能够提供数据加密和 服务，主要用于邮件加密软件.

A．DES B．RSA C．IDEA D．数字签名

6．MD5是按每组512位为一组来处理输入的信息，经过一系列变换后,生成一个 位散列值。

A．64 B．128 C．256 D．512

7．MD5是以512位分组来处理输入的信息，每一分组又被划分为 32位子分组.

A．16个 B．32个

C．64个 D．128个

8．整个 系统由认证服务器AS、票据许可服务器TGS、客户机和应用服务器四部分组成。

A ．PKI B．Kerberos C ．NTUR B．AES

9． 是由权威机构CA发行的一种权威性的电子文档,是网络环境中的一种身份证.

A．认证机构 B．密码 C．票据 D．数字证书

第4章 计算机病毒与黑客

2．填空题

1．计算机病毒的破坏性、 、传染性是计算机病毒的基本特征。

2．计算机病毒是一种能自我复制，破坏计算机系统、破坏数据的\_\_\_\_\_\_\_\_\_。

3．文件型病毒主要是以感染COM、EXE等可执行文件为主，文件型病毒大多数是常驻

的.

4．TCP/IP协议规定计算机的端口有 65536 个，木马可以打开一个或者几个端口，黑客所使用的控制器就能进入木马打开的端口。

5．计算机病毒能通过自身复制来感染正常文件，达到破坏计算机正常运行的目的，称为 .（传染性）

6．目前大多数新式病毒都是通过 进行传播的,破坏性很大。（网络）

7．计算机 是一种寄存于微软Office的文档或模板的宏中的计算机病毒。（宏病毒）

8．计算机 一般也是使用脚本语言将有害代码直接写在网页上，当浏览网页时会立即破坏本地计算机系统。（网页病毒）

9．技术人员从病毒程序中抽取一段独一无二、足以代表该病毒特征的二进制程序代码，并将这段代码作为判断该病毒的依据，这就是所谓的 .(病毒特征代码)

10．将一个程序捆绑到另一个程序可以通过自己 来实现，也可以从网上下载类似DAMS文件捆绑器来实现。（编写程序)

3．简答题

1．什么是病毒特征代码？

2．什么是校验和法？

4．问答题

1．简述计算机病毒的定义和特征.

2．产生病毒的根本原因是什么？

3．计算机病毒的传播途径有哪些？

4．你知道计算机病毒有哪几种类型？

5． 计算机感染病毒后会有哪些表现？

6． 简述计算机病毒程序的一般构成。

7． 计算机病毒制作技术有哪些？

8． 目前使用的反计算机病毒技术有哪些？

9． 蠕虫病毒的主要特性有哪些?

10．什么是特洛伊木马？黑客程序一般由哪几个部分组成？

11．黑客如何利用特洛伊木马程序窥测他人的计算机工作？

12．你知道哪些黑客程序自启动的方法?

13．你在使用计算机时遇到计算机病毒或黑客吗？它们的表现现象如何?如何使自己的计算机尽可能避免计算机病毒的破坏？

5。．选择题

1．蠕虫病毒的主要特性有：自我复制能力、很强的传播性、潜伏性，很大的破坏性等。与其它病毒不同，蠕虫\_\_\_\_\_\_\_\_将其自身附着到宿主程序上。

A．需要， B．不需要， C．可以不需要 D．不一定

2．TCP/IP协议规定计算机的端口有 个，木马可以打开一个或者几个端口，黑客所使用的控制器就可进入木马打开的端口.

A．32768 B．32787 C．1024 D．65536

3．目前计算机病毒的主要传播途径是 。

A．软盘　　　B．硬盘　　 C．可移动式磁盘　　D．网络

4．下面正确的说法是 .

A．购买原版的杀毒软件后可以直接使用，不需要升级

B．安装实时杀毒软件计算机就会绝对安全

C．安装实时杀毒软件可以有效防止计算机病毒的攻击

D．在一台计算机中非常有必要同时使用两个杀毒软件

5．蠕虫病毒可以用VBScript脚本语言编写的，而VBScript代码是通过 来解释执行的。

A．VBScript脚本语言 B．Visual Studio语言

C．Windows Script Host D．Visual Basic语言

6． 是将病毒中比较特殊的共同行为归纳起来，当程序运行时监视其行为,若发现类似病毒的行为，立即报警.

A. 特征代码法 B。 行为监测法

C. 校验和法 D. 虚拟机技术

7．软件产品的脆弱性是产生计算机病毒的 。

A．技术原因 B．社会原因

C．自然原因 D．人为原因

8．主动型木马是一种基于远程控制的黑客工具，黑客使用的程序和在你电脑上安装的程序分别是\_\_\_\_\_\_\_\_\_\_\_\_.

A．服务程序/控制程序 B．控制程序/服务程序

C．驱动程序/木马程序 D．木马程序/驱动程序

9．TCP/IP协议规定计算机的端口有 个,木马可以打开一个或者几个端口，黑客所使用的控制器就进入木马打开的端口.

A．32768 B．32787 C．1024 D．65536

10．软件产品的脆弱性是产生计算机病毒的 。

A．技术原因 B．社会原因

C．自然原因 D．人为原因

第5章 网络攻击与防范

2．填空题

1． 是一种破坏网络服务的技术方式，其根本目的是使受害主机或网络失去及时接受处理外界请求,或无法及时回应外界请求的能力。

2．当网络攻击者向某个应用程序发送超出其 最大容量的数据，使数据量超出缓冲区的长度，多出来的数据溢出堆栈，引起应用程序或整个系统的崩溃。

3． 攻击是向操作系统或应用程序发送超长字符串，导致程序在缓冲区溢出时意外出错，甚至使黑客获得到系统管理员的权限.

4．你知道的常用端口扫描软件有 。

5．及早发现系统存在的攻击漏洞，及时安装系统补丁程序,可以防止 攻击。

6． 是一种自动检测远程或本地主机安全性的程序。

7．目标探测（或踩点)是通过自动或人工查询方法，获得与目标网络相关的 的参数.（物理和逻辑)

8．基于主机的检测技术是采用 、非破坏性的办法对系统进行检测.通常,它涉及到系统的内核、文件的属性、操作系统的补丁等问题。（）

9．基于网络的检测技术是采用 、非破坏性的办法来检验系统是否有可能被攻击。（ ）

10．利用 查询得到目标主机的IP地址分配、机构地址位置和接入服务商等重要信息。（ ）

11．所谓 欺骗就是伪造某台主机的IP地址的技术，让一台主机来扮演另一台主机。（）

12．扫描程序是一种自动检测远程或本地主机 的程序。

3．简答题

1．“混杂"模式

2．电子交易SET

3．安全通道协议SSH

4．安全套接层协议SSL

5．分布式拒绝服务DDoS

6．拒绝服务DoS攻击

7．缓冲区溢出

8．IP欺骗攻击

9．IP地址盗用

10．DNS欺骗

11．Web欺骗

4．问答题

1．查阅有关资料，了解目前操作系统和网络协议中还存在哪些漏洞.

2．什么是目标探测？目标探测的方法有哪些?

3．从整个信息安全角度来看的话，目前扫描器有哪几种类型？

4．请写出你所知道的常见扫描器软件名称。

5．写出FTP端口扫描步骤。

6．如何防止端口扫描？

7．网络监听的原理是什么？

8．如何检测网络监听?如何防范网络监听？

9．Sniffer工作原理是什么？什么是“混杂”模式？

10．如何防范Sniffer？

11．缓冲区溢出原理是什么?请举例说明。

12．缓冲区溢出攻击方法有哪些？

13．如何防范缓冲区溢出?

14．什么是拒绝服务DoS攻击？什么是分布式拒绝服务DDoS

15．写出DDoS攻击的步骤.

16．如何防范DDoS攻击?

17．调查你学校或单位局域网使用的网络拓扑结构，该网络提供了哪些服务?采用哪些安全保护措施？

18．什么是IP欺骗攻击？如何防止IP地址欺骗?

19．IP地址盗用常用方法有哪些？如何防范IP盗用？

20．写出DNS欺骗的工作原理,如何防范DNS欺骗?

21。 什么是Web欺骗？Web欺骗方有哪些法？

22．安全套接层协议SSL主要提供哪些服务？ 是如何实现的？

23．什么是安全通道协议SSH ?它主要由哪几个部分组成？

24．什么是安全电子交易SET?它的主要作用是什么？

27．IPsec通过哪些服务来保护通过公共IP网络传送的机密数据的?

28．IPSec安全体系结构中包括了哪3个最基本的协议？

29．什么是有线等效加密WEP？

30．WPA标准安全特性有哪些?

31．写出802.1x认证过程.

32．WAPI安全协议由哪两部分组成？

33．什么是扩展频谱技术。

6．选择题

1． 是使计算机疲于响应这些经过伪装的不可到达客户的请求，从而使计算机不能响应正常的客户请求等,从而达到切断正常连接的目的。

A．包攻击　　　　　　　　 B．拒绝服务攻击

C．缓冲区溢出攻击　　　　 D．口令攻击

2． 一般是依据一个包含常用单词的字典文件、程序进行大量的猜测，直到猜对口令并获得访问权为止。

A．包攻击　　　　　　　　 B．服务型攻击

C．缓冲区溢出攻击　　 　　　 D．口令攻击

3． 就是要确定你的IP地址是否可以到达，运行哪种操作系统,运行哪些服务器程序，是否有后门存在。

A．对各种软件漏洞的攻击 B．缓冲区溢出攻击

C．IP 地址和端口扫描 D．服务型攻击

4．分布式拒绝服务DDoS攻击分为3层： 、主控端、代理端,三者在攻击中扮演着不同的角色。

A．其它 B．防火墙 C．攻击者 D．受害主机

5．有一种称为嗅探器 的软件，它是通过捕获网络上传送的数据包来收集敏感数据,这些数据可能是用户的账号和密码，或者一些机密数据等等.

A．softice Ｂ．Unicode Ｃ．W32Dasm Ｄ．Sniffer

6．攻击者在攻击之前的首要任务就是要明确攻击目标，这个过程通常称 .

A．安全扫描 B．目标探测

C．网络监听 D．缓冲区溢出

7．下面是一些常用的工具软件,其中 是端口扫描软件。

A．Softice Ｂ．W32Dasm Ｃ．SuperScan Ｄ．Sniffer

8．从技术上说，网络容易受到攻击的原因主要是由于网络软件不完善和 本身存在安全缺陷造成的。

A．网络协议 B．硬件设备

C．操作系统 D．人为破坏

9． 是一种自动检测远程或本地主机安全性弱点的程序。

A．杀毒程序　　　　　　 B．扫描器程序

C．防火墙　　　　　　　 D． 操作系统

10．每当新的操作系统、服务器程序等软件发布之后，黑客就会利用 寻找软件漏洞，从而达到导致计算机泄密、被非法使用，甚至崩溃等目的。

A．IP 地址和端口扫描 B．口令攻击

C．各种软件漏洞攻击程序 D．服务型攻击

11． 攻击是指借助于客户机/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击,从而成倍地提高拒绝服务攻击的威力。

A．分布式拒绝服务 B．拒绝服务

C．缓冲区溢出攻击　　　　 D．口令攻击

12． B 是一种破坏网络服务的技术，其根本目的是使受害主机或网络失去及时接受处理外界请求，或无法及时回应外界请求的能力。

A．包攻击　　　　　　　　 B．拒绝服务

C．缓冲区溢出攻击　　　　　 D．口令攻击

13．下面是一些常用的工具软件,其中 是分析网络路由软件。

A．Softice Ｂ．W32Dasm Ｃ．江民杀毒 Ｄ．TraceRoute

第6章 防火墙技术

2．填空题

1．可以将防火墙分成 和应用层防火墙两种基本类型的防火墙。

2．屏蔽主机网关是将筛选路由器作为第一道防线，而把\_\_\_\_\_\_\_\_\_作为第二道防线。

3．屏蔽子网网关有一台主机和两台路由器组成，两台路由器分别连接到\_\_\_\_\_\_\_和Internet。

4．包头信息中包括 、IP目标地址、内装协议、TCP/UDP目标端口、ICMP消息类型、TCP包头中的ACK位。

5．应用层防火墙也称为代理防火墙,它作用于 层，一般是运行代理服务器的主机。

6．安全、 、速度是防火墙的三大要素。（管理)

7． 是作用于网络层的，一般根据源、目的地址做出决策,输入单个的IP包。（网络层防火墙）

8． 防火墙就是将防火墙功能嵌入到路由器或交换机中.（嵌入式）

9．防火墙中的 技术是基于IP地址来监视并过滤网络上流入和流出的IP包，它只允许与指定的IP地址通信。（包过滤)

10．防火墙设计策略有拒绝访问除明确许可以外的任何一种服务,即没有被列为允许的服务都是 的。

11．防火墙设计策略有允许访问除明确拒绝以外的任何一种服务，即没有被列为禁止的服务都是 的。

3．简答题

1．防火墙

2．嵌入式防火

3．网络层防火墙

4．应用层防火墙

5．智能防火墙

6．包过滤技术

7．代理服务技术

8．电路层网关技术

9．状态检测技术

10．分布式防火墙

4．问答题

1．什么是防火墙？一个防火墙至少提供哪两个基本的服务？

2．硬件防火墙与软件防火墙有什么区别?

3．防火墙有哪些主要功能?

4．网络层防火墙和应用层防火墙有什么特点？

5．嵌入式防火有什么特点？

6．智能防火墙有什么特点？

7．画出防火墙的筛选路由器结构、双宿主主机结构、屏蔽主机网关结构和屏蔽子网结构图。

8．什么是包过滤技术？请写包过滤规则的制定过程.

9．什么是代理服务技术？请举例说明。

10．什么是电路层网关技术？请写出电路层网关的工作过程。

11．什么是状态检测技术?请写状态检测技术防火墙的工作过程。

12． 什么是分布式防火墙？与传统防火墙相比分布式防火墙有什么优点？

13．一个完整的分布式防火墙系统应该包含哪几个部分？

14．请写出防火墙设计策略.

15．选购防火墙时应注意哪些问题？

16．什么是个人防火墙？个人防火墙一般由哪几个模块组成？

6．选择题

1．防火墙中包过滤规则是以IP的包头信息为基础，包头信息包括：\_\_\_\_\_IP源地址、封装协议、TCP/UDP端口等.

A。 IP目的地址 B。 数据地址

C. 总线地址 D. 控制端口

2．在防火墙双穴网关中，堡垒机充当网关，装有\_\_\_\_\_\_\_\_\_\_块网卡。

A．1 B。 2 C。 3 D。 4

3．防火墙原型分为双穴网关，屏蔽主机网关，屏蔽子网网关三种网关,从安全性方面考虑\_\_\_\_\_\_\_\_\_\_网关最安全

A. 双穴网关 B。 屏蔽主机网关

C. 屏蔽子网网关 D。 屏蔽主机子网网关

4．在防火墙屏蔽主机网关中\_\_\_\_\_\_\_作为第一道防线与Internet相连。

A．筛选路由器 B．堡垒机

C．局域网 D．内部专用网

5．在防火墙屏蔽子网网关中,至少使用\_\_\_\_\_\_\_个路由器

A．1 　 B．2 C．3 Ｄ．4

6．对于一个要求安全性很高的大型企业，应选择 防火墙的体系结构.

A．双穴网关 B．屏蔽主机网关

C．屏蔽子网网关 D．个人防火墙

7．状态分析技术不需要把客户机／服务器模型一分为二,状态分技术在 截获数据包的。

A．应用层 B．传输层

C．网络层 D．物理层

8．下面正确的说法是 。

A．防火墙可以防范一切黑客入侵

B．防火墙增加杀毒功能后可以提高防火墙工作速度

C． 在一个安全体系中不能同时使用两个防火墙

D．防火墙可以实现网络地址翻译功能

9．目前防火墙可以分成两大类，它们是网络层防火墙和 。

A．应用层防火墙 B．表示层防火墙

C．会话层防火墙 D．传输层防火墙

10．防火墙中的状态分析技术是数据包过滤技术的延伸，通常被称为 。

A．固定数据包过滤 B．静态数据包过滤

C． 随机数据包过滤 D．动态数据包过滤

11．在个人计算机中安装防火墙系统的目的是 。

A．保护硬盘 B．使计算机绝对安全

C．防止计算机病毒和黑客 D．保护文件

12．目前防火墙技术中主要有三种：数据包过滤、代理服务和 技术。

A．杀毒 B．防黑客 C．修补漏洞 D．状态分析

13．数据包过滤独立于任何应用软件,它在 上对每一个数据包进行检查。

A．应用层 B．传输层 C．网络层 D．物理层

14．代理服务位于内部用户和外部服务之间.代理在 和因特网服务之间的通信以代替相互间的直接交谈.

A．幕前处理所有用户 B．幕前处理个别用户

C．幕后处理所有用户 D．幕后处理个别用户

第7章 入侵检测技术

2．填空题

1．入侵检测系统能够通过对网络中的数据或主机的日志等信息进行提取和分析，发现 行为。

2． 系统能够通过对网络中的数据或主机的日志等信息进行提取和分析，发现入侵和攻击行为，并可通过和防火墙联动，对入侵或攻击做出响应.（入侵检测)

3． 的目标是识别系统内部人员和外部入侵者的非法使用、滥用计算机系统的行为。

4．一般可将入侵检测系统粗略分为三大模块：即入侵数据提取模块、 和入侵事件响应模块.(入侵数据分析模块）

5．入侵检测的正确性 于收集信息的可靠性和准确性。（依赖）

6．入侵数据分析是整个入侵检测系统的 模块。（核心）

7．入侵检测响应方式分为主动响应和 响应。（被动）

8． 安装在被保护的主机上，通常用于保护运行关键应用的服务器.（基于主机的IDS）

9． 一般安装在需要保护的网段中，利用网络侦听技术实时监视网段中传输的各种数据包等。（基于网络的IDS）

10．入侵行为的属性可分为异常（Anomaly）和 两种。（误用）

11．异常检测是假定所有的入侵行为都与正常行为 。（不同)

12． 检测是假定所有的入侵行为都与正常行为不同。(异常）

13． 是假定所有入侵行为、手段及其变种都能够表达为一种模式或特征。(误用检测）

14．误用检测是假定所有入侵行为、手段及其变种都能够表达为一种 。(模式或特征)

3．简答题

1．什么是入侵检测。

4．问答题

1．在网络安全中，什么入侵检测?入侵检测一般步骤是什么？

2．根据系统所检测的对象分类，入侵检测系统有哪些类型？

3．根据数据分析方法分类，入侵检测系统有哪些类型？

4．目前，入侵检测系统使用哪些关键技术？

5．入侵检测统计分析模型有那些?

6．分布式入侵检测系统有什么特点？

7．写出基于移动代理的入侵检测系统工作过程。

8. 通用入侵检测框架CIDF文档由哪几部分组成?

9．Snort主要功能有哪些？由哪几部分组成？

10．选购入侵检测产品时要注意哪些问题？

6．选择题

1．的目标是识别系统内部人员和外部入侵者的非法使用、滥用计算机系统的行为。

A．入侵检测 B．杀毒软件

C．防火墙 D．网络扫描

2．一般可将入侵检测系统粗略分为三大模块：即 、入侵数据分析模块和入侵事件响应模块。

A. 入侵数据输出模块 B. 入侵数据提取模块

C。 入侵数据输入模块 D. 入侵数据破坏模块

3．数据分析模块主要作用在于对数据进行深入分析,发现攻击并根据分析的结果产生事件，传递给 D 。

A. 入侵数据输出模块 B。 入侵数据提取模块

C. 入侵数据输入模块 D。 事件响应模块

4主要作用在于对数据进行深入分析，发现攻击并根据分析的结果产生事件,传递给事件响应模块。

A. 入侵数据输出模块 B. 入侵数据提取模块

C。 入侵数据输入模块 D。 入侵数据破坏模块

5安装在被保护的主机上，通常用于保护运行关键应用的服务器。

A．基于网络的IDS Ｂ．基于应用的AIDS

Ｃ．基于主机的防火墙 Ｄ．基于主机的IDS

6． 一般安装在需要保护的网段中，利用网络侦听技术实时监视网段中传输的各种数据包等。

A．基于网络的IDS Ｂ．基于应用的AIDS

Ｃ．基于主机的防火墙 Ｄ．基于主机的IDS

7．入侵行为的属性可分为异常（Anomaly）和 两种。

A．误用 Ｂ．统计 Ｃ．分析 Ｄ．匹配

8．下面是一些常用的工具软件，其中 软件是一中典型的入侵检测软件.

A．softice Ｂ．Snort

Ｃ．Superscan Ｄ．ASPack

9．是假定所有入侵行为、手段及其变种都能够表达为一种模式或特征。

A．病毒检测 Ｂ．误用检测

Ｃ．文件检测 Ｄ．异常检测

10。检测是假定所有的入侵行为都与正常行为不同。

A．病毒检测 Ｂ．误用检测

Ｃ．文件检测 Ｄ．异常检测

11．入侵检测的目标是识别系统内部人员和外部入侵者的非法使用、滥用计算机系统的行为.

A．防火墙 B．杀毒软件 C．入侵检测 D．数据取证

第8章 数字取证技术

2．填空题

1． 技术将计算机调查和分析技术应用于对潜在的、有法律效力的电子证据的确定与获取。（数字取证）

2．网络取证的数据主要来源于网络数据流，同样要求是对潜在的、有法律效力的证据的确定与 。（获取)

3． 是要保存计算机系统的状态，避免无意识破坏现场,同时不给犯罪者破坏证据提供机会，以供日后分析.(电子证据的确定和收集)

4． 阶段将使用原始数据的精确副本，应保证证据必须是安全的，有非常严格的访问控制。（电子证据的保护）

5． 是指在已经获取的数据流或信息流中寻找数字证据.

6．模糊专家系统取证技术中 是确定每个语义变量的模糊集所定义的隶属函数和每个模糊集中输入值的隶属度。

3．简答题

1．计算机取证

2．电子证据

4．问答题

1。 什么是计算机取证？电子证据有什么特点?

2．在各类存储介质中有哪些数据可以作为证据?

3．数字取证原则有哪些?写出数字取证过程。

4．网络取证有什么特点？请画出网络取证模型.

5．写出IDS取证的具体步骤。

6．利用蜜阱技术进行取证分析时,一般遵循哪些原则？

7．模糊专家取证系统包含哪几个组件?

8．你知道哪些数字取证工具?

5．选择题

1． 将计算机调查和分析技术应用于对潜在的、有法律效力的电子证据的确定与获取。

Ａ．防病毒技术 Ｂ．防黑客技术

Ｃ．数字取证技术 Ｄ．防盗版技术

2． 的主要方法有对文件的复制、被删除文件的恢复、缓冲区内容获取、系统日志分析等，。Ａ．网络取证 Ｂ．文字取证

Ｃ．盗版取证 Ｄ．计算机取证

3． 的数据主要来源于网络数据流,同样要求是对潜在的、有法律效力的证据的确定与获取。

Ａ．网络取证 Ｂ．文字取证

Ｃ．盗版取证 Ｄ．计算机取证

4． 是要保存计算机系统的状态，避免无意识破坏现场，同时不给犯罪者破坏证据提供机会，以供日后分析.

A．电子证据的保护 Ｂ．电子证据的分析

Ｃ．电子证据的备份 Ｄ．电子证据的确定和收集

5． 阶段将使用原始数据的精确副本，应保证证据必须是安全的，有非常严格的访问控制。

A．电子证据的保护 Ｂ．电子证据的分析

Ｃ．电子证据的备份 Ｄ．电子证据的确定和收集

6． 是指在已经获取的数据流或信息流中寻找数字证据。

A．电子证据的保护 Ｂ．电子证据的分析

Ｃ．电子证据的备份 Ｄ．电子证据的确定和收集

7．模糊专家系统取证技术中 是确定每个语义变量的模糊集所定义的隶属函数和每个模糊集中输入值的隶属度。

A．取证分析器 Ｂ．模糊推理引擎组件

Ｃ．模糊化组件 Ｄ．反模糊化组件

8．下面是一些常用的工具软件，其中 软件是一中典型的数字取证软件。

A．softice Ｂ．W32Dasm

Ｃ．Superscan Ｄ．Encase

第9章 操作系统安全

2．填空题

1．操作系统的安全是计算机系统安全的 .（核心）

2．有选择的访问控制包括使用多种不同的方式来限制计算机环境下对 对象的访问。(特定)

3．安全系统应该具备 ，以便测试其完整性，并可追踪任何可能的安全破坏活动。(审计能力)

4．每个用户及程序应使用尽可能 的权限工作,这样，由攻击者恶意攻击造成的破坏程度会降低到最小（小）

5．操作系统访问控制权限的合理设置主要是指利用操作系统的访问控制功能，为用户和文件系统建立恰当的 控制.（访问权限)

6．从技术管理的角度考虑，可以从 和审计日志两个方面提高系统的安全性。（）

7． 是安全系统的一个重要组成部分，它记录了计算机系统所发生的情况，如何时由谁做了一件什么样的事，结果如何等。（日志文件）

8．Windows安全服务的核心功能包括了活动 目录AD。服务、对公钥基础设施PKI等。()

9．Windows系统活动目录包括目录和与目录相关的 两个部分。（)

10．Windows系统的安全模型正是建立 结构之上，提供域间信任关系、组策略安全管理等安全性服务。（ ）

3．简答题

1．Linux 安全模块LSM

2．Linux的PAM机制

3．Windows系统的活动目录

4．问答题

1．操作系统安全功能有哪些?

2．操作系统安全设计原则有哪些？

3．操作系统的安全配置指导思想是什么？

4．操作系统的安全性包括哪些内容？

5。 你知道Windows 2000/XP/2003中有哪些安全机制?

6．什么是活动目录？活动目录能够提供哪些服务？

7．什么是Windows安全设置模板?

8．Windows的安全账号管理器作用是什么？

9．硬盘的NTFS分区格式有何特点?

10．Windows 2000/XP/2003安全配置时要注意哪些事项？

11．Unix的安全机制有哪些？

12 Linux的安全机制有哪些?

13．什么是Linux的PAM机制？什么是Linux 安全模块LSM？

14．进行Linux安全设置时要注意哪些事项？

15．磁盘的NTFS文件格式有什么特点？

6．选择题

1． 控制包括使用多种不同的方式来限制计算机环境下对特定对象的访问。

Ａ．内存管理与对象重用 Ｂ．有选择的访问

Ｃ．审计能力 Ｄ．加密数据传送

2．安全系统应该具备 ，以便测试其完整性，并可追踪任何可能的安全破坏活动.

Ａ．内存管理与对象重用 Ｂ．有选择的访问

Ｃ．审计能力 Ｄ．加密数据传送

3． 保证了在网络传送时所截获的信息不能被未经身份认证代理所访问.

Ａ．内存管理与对象重用 Ｂ．有选择的访问

Ｃ．审计能力 Ｄ．加密数据传送

4．操作系统访问控制权限的合理设置主要是指利用操作系统的访问控制功能，为用户和文件系统建立恰当的 控制。

A．访问权限 Ｂ．合理设置

Ｃ．即使更新 Ｄ．攻击防范

5．从技术管理的角度考虑，可以从 和审计日志两个方面来提高操作系统的安全性。

A．备份 Ｂ．监控 Ｃ．运行 Ｄ．删除

6． 是安全系统的一个重要组成部分，它记录了计算机系统所发生的情况,如何时由谁做了一件什么样的事，结果如何等。

A．备份文件 Ｂ．日志文件

Ｃ．加密文件 Ｄ．注册文件

7．Windows安全服务的核心功能包括了 B 服务、对公钥基础设施PKI(Public Key Infrastructure）的集成支持、对Kerberos V5鉴别协议的支持等。

A．固定目录AD Ｂ．活动目录AD

Ｃ．备份目录AD Ｄ．存储目录AD

8．Windows系统活动目录包括目录和与目录相关的 A 两个部分。

A．服务 Ｂ．备份 Ｃ．存储 Ｄ．压缩

9．Windows系统的安全模型正是建立在 结构之上，提供域间信任关系等安全性服务。

A．管理委派 Ｂ．鉴别与访问控制

Ｃ．活动目录 Ｄ．组策略安全管理

第10章 数据备份与恢复

2．填空题

1．你知道的系统备份软件有 。

2．为了防止重要数据丢失或操作系统被破坏的最有效的方法是对数据和系统进行　　　　。

3．防止计算机系统中重要数据丢失的最简单、最有效的方法是 。

4．数据备份包括 和用户数据备份.

5．你知道的数据恢复软件有 。

6． 只备份上次完全备份以后有变化的数据.

7．将数据备份到可读写的存储介质上称为 。（可更新备份）

8．将数据备份到只读存储介质上称为 。（不可更新备份）

9．通过网络将文件备份到与本地计算机物理上相分离的存储介质上称为 .（异地备份）

10．在单机的特定存储介质上进行的备份称为 .（本地备份）

11． 只备份上次备份以后有变化的数据.（增量备份）

12．SAN简称为 ，是一个独立于服务器网络系统之外的，几乎拥有无限信息存储能力的高速信息存储网络。

3．简答题

1．本地备份、异地备份

2．可更新备份、不可更新备份

3．完全备份、、差分备份

4．增量备份、按需备份

5．动态备份、镜像备份

6．系统数据

7．用户数据

8．DAS直接存储

9．NAS网络存储

10．SAN存储网络

11．IP存储

12．数据迁移技术

4．问答题

1．为什么要进行数据备份？

2．如果你是系统管理员，为了提高系统的可靠性,你将如何制订备份方案？准备使用哪些备份手段?

3．有下面的一个说法：“我们的数据库软件有容错和自动恢复功能，服务器主机已经作了双机热备份,而且以后还要建立群集系统，所以，我们不需要进行数据设备和备份软件了。”你认为这种说法对吗？为什么？

4．什么是系统数据备份?

5．什么是 磁盘阵列RAID技术？常用的RAID模式有哪些特点?

6．系统还原卡基本原理是什么？在安装还原卡之前要注意哪些问题？，

7．Ghost软件有哪些功能?

8．什么是用户数据备份？Second Copy2000软件有哪些功能？

9．网络备份系统由哪几部分组成?制订备份管理计划内容有哪些？

10．数据恢复之前应该注意哪些问题？

11．硬盘数据恢复基本原理是什么？

12．修复硬盘综合工具PC-3000有哪些功能？

13．EasyRecovery恢复数据软件有哪些功能？

6．选择题

1． 只备份上次完全备份以后有变化的数据。

A．差分备份 B．增量备份

C．本地备份 D．异地备份

2．下面是一些常用的工具软件,其中 是数据备份软件。

A．Hiew Ｂ．Second Copy2000

Ｃ．Resource Hacker Ｄ．EasyRecovery

3． 备份到可读写的存储介质上.

A．差分备份 Ｂ．可更新备份

Ｃ．不可更新备份 Ｄ．静态备份

4．将数据备份到只读存储介质上称为 。

A．差分备份 Ｂ．可更新备份

Ｃ．不可更新备份 Ｄ．静态备份

5．通过网络将文件备份到与本地计算机物理上相分离的存储介质上称为 。

A．差分备份 Ｂ．可更新备份

Ｃ．不可更新备份 Ｄ．异地备份

6．在单机的特定存储介质上进行的备份称为 。

A．本地备份 Ｂ．可更新备份

Ｃ．不可更新备份 Ｄ．异地备份

7． 只备份上次备份以后有变化的数据。

A．差分备份 Ｂ．可更新备份

Ｃ．不可更新备份 Ｄ．增量备份

8．系统数据备份主要是针对计算机系统中的操作系统、 、系统应用软件及常用软件工具等。

A．办公软件 Ｂ．杀毒软件

Ｃ．系统驱动程序 Ｄ．设备驱动程序

9． 主要是针对计算机系统中的操作系统、设备驱动程序、系统应用软件及常用软件工具等。

A．系统数据备份 Ｂ．可更新备份

Ｃ．不可更新备份 Ｄ．用户数据备份

10．SAN简称为 ，是一个独立于服务器网络系统之外的，几乎拥有无限信息存储能力的高速信息存储网络。

A．网络存储 Ｂ．存储网络 Ｃ．直接存储 Ｄ．数据存储

11．下面 可以用来实现用户数据恢复.

A．softice Ｂ．Ghost Ｃ．W32Dasm Ｄ．EasyRecovery

一、单选题

1.在网络纠纷案件中,网络游戏客户的号码被盗了，应采取的合理措施是（）

A。向网站客服投诉请求解决

B.拨打 120

C.拨打 119

D。找网络黑客再盗回来

2。下列情形中,不构成侵权的是（）

A.未经他人同意擅自在网络上公布他人隐私

B.下载网络小说供离线阅读

C。伪造、篡改个人信息

D。非法侵入他人电脑窃取资料

3。网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序.为了防止受 到网络蠕虫的侵害，应当注意对()进行升级更新。

A。计算机操作系统

B.计算机硬件

C。文字处理软件

D.视频播放软件

4.甲冒充新闻工作者,以在新闻网站上发布隐私为要挟,向乙、丙、丁等人索取了数十万财物。 甲的行为应当认定为()

A.敲诈勒索罪

B.诈骗罪

C.招摇撞骗罪

D。寻衅滋事罪

5。某公司未经授权,擅自在其经营的网站提供某电影供在线观看，该公司侵犯了制作该电影的 电影公司的（)

A。专利权

B.商标权

C.信息网络传播权

D。发明权

6。以下关于非对称密钥加密的表述，正确的是(）

A.加密方和解密方使用的是不同的算法

B.加密密钥和解密密钥是不同的

C.加密密钥和解密密钥匙相同的

D。加密密钥和解密密钥没有任何关系

7.国内第一家网上银行是（）

A。招商银行网上银行

B。中国农业银行网上银行

C。中国银行网上银行

D.中国建设银行网上银行

8。下列密码，相对而言最安全的是（）

A。123456.0

B.888888.0

C.666abc

D。2h4l5k

9。采用一种或多种传播手段，使大量主机感染病毒，从而在控制者和被感染主机之间形成一个 可一对多控制的网络。该网络通常称为(）

A.钓鱼网络

B。游戏网络

C。僵尸网络

D。互联网络

10。以下关于宏病毒的表述，正确的是（）

A.宏病毒主要感染可执行文件

B.宏病毒仅向办公自动化程序编制的文档进行传染

C。宏病毒主要感染 U 盘、硬盘的引导扇区或主引导扇区

D.CIH 病毒属于宏病毒

11。下列程序能修改高级语言源程序的是()

A.调试程序

B.解释程序

C。编译程序

D。编辑程序

12。互联网上网服务营业场所不得允许未成年人进入，经营者应当在显著位置设置未成年人 禁入标志;对难以判明是否已成年的，应当要求其出示（)

A.学生证

B.身份证

C.工作证

D。借书证

13.在网络环境下,权利管理信息专指以(）出现的信息，它们被嵌在电子文档里，附加于作品的 每件复制品上或作品中向公众传播时显示出来。

A.数字化形式

B.纸面化形式

C.图像形式

D。声音形式

14.下列选项中,使用身份认证双因素法的是（)

A。电话卡

B.交通卡

C。校园饭卡

D。银行卡

15。非法获取计算机信息系统数据、非法控制计算机信息系统罪的犯罪主体是年满()周岁并 具有刑事责任能力的自然人.

A。10。0

B。14.0

C.16.0

D.18。0

二、多选题

1.下列关于密码安全的描述,正确的是()

A.容易被他人记住的密码不安全

B.相对而言,密码越长越安全

C.密码要定期更换

D。密码中使用的字符种类越多越不容易被猜中

2.甲创作并演唱了《两只麻雀》，乙公司擅自将该歌曲制成彩铃在网络上供免费下载。乙公 司侵犯了甲的（)

A.信息网络传播权

B。广播权

C。表演者权

D。汇编权

3.下列不属于侵犯网络隐私权的情形有()

A。用户在注册邮箱的时候，要求填写其个人联系方式和真实姓名

B.根据相关法律,在网络游戏进行注册的时候需要填写个人身份证号码以验证用户是否 为成年人

C.张某想要开一家淘宝商店,淘宝要求商户注册的时候实名认证

D。商家收集消费者的购物倾向,制定针对个别消费者的营销策略追求商业利益

4.下列行为中，侵犯软件著作权的有()

A。使用著作权人已公开发行的软件的

B.未经著作权人许可,修改、翻译其软件的

C。故意避开或者破坏著作权人为保护其软件著作权而采取的技术措施的

D。故意删除或者改变软件权利管理电子信息的

5。下列表述中，不正确的有(）

A。显示器和打印机都是输出设备

B。显示器只能显示字符

C.通常的彩色显示器都只有 7 种颜色

D.打印机只能打印字符和表格

6.通过信息网络提供他人作品，在下列情形中，可以不经著作权人许可、不向其支付报酬的是 ()

A。为介绍、评定某一作品或者说明某一问题,在向公众提供的作品中适当引用已经发表 的作品

B。国家机关执行公务，在合理范围内向公众提供已经发表的作品

C.向公众提供在公众集会上发表的讲话

D。向公众提供在信息网络上已发表的关于政治、经济问题的时事性文章

7。网络服务提供者在业务活动中收集、使用公民个人电子信息，应当遵循的原则有(）

A。合法原则

B.正当原则

C。必要原则

D。公开原则

8.可以作为身份认证依据的人的生物特征有()

A。指纹

B。虹膜

C。脸部

D。掌纹

9。以下属于计算机病毒防治策略的是（)

A。防毒能力

B。查毒能力

C.解毒能力

D.禁毒能力

10.要做好计算机信息系统安全保护工作,必须明确（）

A.安全是一个过程,是动态的，没有一劳永逸安全措施，要警钟常鸣

B。安全是个管理的概念,只有加强管理才能保障安全

C。要不断根据计算机信息网络系统出现的新情况、新问题,加强安全管理

D。安全是相对的，没有绝对的安全

11。国家机关及其工作人员在对履行职责中知晓的公民个人电子信息，应当(）

A.予以封存

B。予以保密

C。不得泄露、篡改、毁损

D.可以提供给第三人

12。网络抄袭与剽窃是指单位或者个人剽窃使用网络及其他媒体上已经发表的文字、图片、 影音等资源用于非公益目的,即大段抄袭或者剽窃著作权人的作品，在网络上以自己的名义发 表、传播。这种行为侵犯了著作权人的（)

A.署名权

B。信息网络传播权

C.获得报酬权

D.肖像权

13。网络侵权和传统侵权的区别有（）

A。网络侵权中的证据比传统侵权具有不稳定性

B.网络侵权的主体比传统侵权具有隐秘性

C.网络侵权造成的后果比传统侵权更易传播、扩散

D.网络侵权比传统侵权的司法管辖更不好定位

14。计算机病毒按传染方式分为()

A.良性病毒

B.引导型病毒

C.文件型病毒

D。复合型病毒

15。互联网增值服务主要以网络社区为基础平台，通过用户之间的沟通和互动,激发用户自我 表现和娱乐的需求,从而给个人用户提供各类通过付费才可获得的个性化增值服务和虚拟物 品消费服务。互联网增值服务主要包括(）

A。会员特权

B。网络虚拟形象

C.个人空间装饰

D.个人信息获取

16。威胁网络安全的主要因素有（)

A。自然灾害

B.意外事故

C.计算机犯罪

D.“黑客”行为

17.根据我国《电信条例》的规定，电信业务分为（)

A.基础电信业务

B。增值电信业务

C.营利电信业务

D。非营利电信业务

18.计算机网络的资源共享功能包括(）

A。安全共享

B.硬件资源共享

C。软件资源共享

D.数据资源共享

19。有关电子商务的参与者，下列选项正确的是()

A。政府是市场经济活动的宏观调控者

B。企业是是电子商务的主力军

C。消费者是电子商务最终的服务对象

D。电子商务的发展是政府、企业和消费者等各类主体协同努力的结果

20。网络游戏虚拟货币交易服务企业应当遵守的规定有（)

A.不得为未成年人提供交易服务

B。不得为未经审查或者备案的网络游戏提供交易服务

C。提供服务时,应保证用户使用有效身份证件进行注册

D.接到利害关系人通知后，应当协助核实交易行为的合法性

三、判断题

1。访问控制不能阻止人们利用系统脆弱点以管理员身份获得对系统的访问并查看系统文件。

对

错

2。雇佣、组织、教唆或者帮助他人发布、转发网络信息侵害他人人身权益，被侵权人不得请 求行为人承担连带责任。

对

错

3.确认电子签名的法律效力，关键在于解决两个问题:一是通过立法确认电子签名的合法性、 有效性;二是明确满足什么条件的电子签名才是合法的、有效的。

对

错

4。利用互联网技术向近亲属发送诈骗信息,诈骗到数额较大的财物，即使近亲属谅解,也不能从 宽处理.

对

错

5。为了防御网络监听，最常用的方法是信息加密.

对

错

6。互联网信息服务提供者发现其网站传输的信息明显属于宣扬封建迷信信息的，应当立即停 止传输,保存有关记录，并向国家有关机关报告。

对

错

7.互联网是通过网络适配器将各个网络互联起来.

对

错

8.欧盟早在 1995 年就在相关数据保护法律中提出了“被遗忘权”概念,任何公民可以在其个 人数据不再需要时提出删除要求.

对

错

9.薄弱点扫描本身并不会保护计算机系统，需在找出薄弱点后采取安全措施。

对

错

10。可能给电脑网络系统造成影响或者破坏的人只有黑客。

对

错

11.网络侵权主体只能是自然人。

对

错

12。《信息交换用汉字编码字符集基本集》国家标准规定:一个汉字用 4 个字节表示。

对

错

13。个人电子邮箱不属于个人信息。

对

错

14。某网站为促进社会公共利益，在一定的范围内公开他人的病历资料，此行为受法律的保护。

对

错

15.域名争议解决机构作出的裁决只涉及争议域名持有者信息的变更。

对

错

交卷

### 一、单选题

1. （容易）2014年2月27日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平2月27日下午主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。他强调，\_\_\_\_\_\_\_和\_\_\_\_\_是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题.
2. 信息安全、信息化
3. 网络安全、信息化
4. 网络安全、信息安全
5. 安全、发展

答案:B

1. （容易）2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上指出，网络空间的竞争，归根结底是\_\_\_\_竞争。
2. 人才
3. 技术
4. 资金投入
5. 安全制度

答案：A

1. （容易）2014年2月，我国成立了（ ），习近平总书记担任领导小组组长。
2. 中央网络技术和信息化领导小组
3. 中央网络安全和信息化领导小组
4. 中央网络安全和信息技术领导小组
5. 中央网络信息和安全领导小组

答案：B

1. （容易)首届世界互联网大会的主题是\_\_\_\_\_\_。
2. 互相共赢
3. 共筑安全互相共赢
4. 互联互通，共享共治
5. 共同构建和平、安全、开放、合作的网络空间

答案:C

1. （容易）2016年4月19日,习近平总书记在网络安全和信息化工作座谈会上指出,“互联网核心技术是我们最大的‘命门’，\_\_\_\_\_\_是我们最大的隐患"。
2. 核心技术受制于人
3. 核心技术没有完全掌握
4. 网络安全技术受制于人
5. 网络安全技术没有完全掌握

答案：A

1. （中等）2016年4月19日,习近平总书记在网络安全和信息化工作座谈会上指出：“互联网主要是年轻人的事业，要不拘一格降人才。要解放思想，慧眼识才，爱才惜才。培养网信人才,要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的\_\_\_\_。”
2. 网络空间安全学院
3. 信息安全学院
4. 电子信息工程学院
5. 网络安全学院

答案：A

1. （容易）2016年04月19日，习近平总书记在网络安全和信息化工作座谈会上的讲话强调,要建立\_\_\_\_\_\_网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制.
2. 政府和企业
3. 企业和企业
4. 企业和院校
5. 公安和企业

答案：A

1. （容易)2016年04月19日,习近平总书记在网络安全和信息化工作座谈会上的讲话强调，要加快网络立法进程,完善依法监管措施，化解网络风险。前段时间发生的e租宝、中晋系案件，打着（ ）旗号非法集资,给有关群众带来严重财产损失，社会影响十分恶劣。
2. “网络购物”
3. “网络投资”
4. “网络金融”
5. “网络集资”

答案：C

1. （困难)2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上指出：“要正确处理开放和自主的关系",对此的理解错误的是（）
2. 互联网让世界变成了地球村，推动国际社会越来越成为你中有我、我中有你的命运共同体
3. 关起门来,另起炉灶，彻底摆脱对外国技术的依赖，靠自主创新谋发展，否则总跟在别人后面跑，永远追不上
4. 市场换不来核心技术,有钱也买不来核心技术，必须靠自己研发、自己发展.
5. 强调自主创新，不是关起门来搞研发，一定要坚持开放创新，只有跟高手过招才知道差距，不能夜郎自大

答案：B

1. （中等）2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上指出，维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险,正所谓“聪者听于无声，明者见于未形”。（ ）是最基本最基础的工作。（)
2. 感知网络安全态势
3. 实施风险评估
4. 加强安全策略
5. 实行总体防御

答案：A

1. （中等）2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上指出，网信事业要发展，必须贯彻\_\_的发展思想.
2. 以法律法规为中心
3. 以安全为中心
4. 以人民为中心
5. 以防御为中心

答案:C

1. （中等)习近平总书记在第二届世界互联网大会上指出“各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体"，为此提出了五点主张，以下哪一项不属于五点主张范围（)
2. 加快全球网络基础设施建设，促进互联互通
3. 打造网上文化交流共享平台，促进交流互鉴
4. 构建互联网治理体系，促进公平正义
5. 尊重网络知识产权，共筑网络文化

答案:D

1. （容易）2016年04月19日,习近平总书记在网络安全和信息化工作座谈会上的讲话强调，我们提出了全球互联网发展治理的（ ）,特别是我们倡导尊重网络主权、构建网络空间命运共同体,赢得了世界绝大多数国家赞同.
2. “四项原则”、“四点主张”
3. “四项原则"、“五点主张”
4. “五项原则"、“四点主张”
5. “五项原则”、“五点主张”

答案：B

1. （中等）习近平总书记在第二届世界互联网大会上指出“各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体”,为此提出了五点主张，以下哪一项不属于五点主张范围（)
   1. 加快全球网络基础设施建设，促进互联互通
   2. 打造网上文化交流共享平台，促进交流互鉴
   3. 构建互联网治理体系,促进公平正义
   4. 尊重网络知识产权，共筑网络文化

答案：D

1. （容易）2010年7月，某网站在网上公开了数十万份有关阿富汗战争、伊拉克战争、美国外交部相关文件，引起轩然大波,称为（）:
2. 维基解密;
3. icloud泄密;
4. 越狱；
5. 社会工程

答案：A

1. （容易）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。
2. 拖库;
3. 撞库;
4. 木马；
5. 信息明文存储

答案:B

1. （容易)棱镜门的主要曝光了对互联网的什么活动?
2. 监听;
3. 看管;
4. 羁押;
5. 受贿;

答案：A

1. （容易）棱镜门事件的发起者是谁？
2. 俄罗斯克格勃；
3. 美国国家安全局；
4. 英国军情六处;
5. 斯诺登;

答案：B

1. （容易)2016年国家网络安全宣传周主题是(）
2. 网络安全为人民，网络安全靠人民
3. 共建网络安全,共享网络文明
4. 网络安全同担，网络生活共享
5. 我身边的网络安全

答案：A

1. （中等）某网站”网站吸纳会员时要求交纳相应会费，交纳后网站就会给购买者一个会员编号和一个会员“昵称”,该购买者就正式成为网站会员。成为会员后，就可自由发展下线，收取提成，形成五五复制的上下级关系。这种行为属于\_\_\_\_\_\_.
2. 网络传销
3. 网络钓鱼
4. 网络攻击
5. 网络诈骗

答案: A

1. （中等）某同学的以下行为中不属于侵犯知识产权的是()。
2. 把自己从音像店购买的《美妙生活》原版CD转录，然后传给同学试听
3. 将购买的正版游戏上网到网盘中，供网友下载使用
4. 下载了网络上的一个具有试用期限的软件,安装使用
5. 把从微软公司购买的原版Windows 7系统光盘复制了一份备份，并提供给同学

答案：C

1. （容易）物联网就是物物相连的网络，物联网的核心和基础仍然是\_\_\_\_,是在其基础上的延伸和扩展的网络。
2. 城域网
3. 互联网
4. 局域网
5. 内部办公网

答案:B

1. （容易）下列有关隐私权的表述,错误的是( ）
2. 网络时代,隐私权的保护受到较大冲击
3. 虽然网络世界不同于现实世界，但也需要保护个人隐私
4. 由于网络是虚拟世界,所以在网上不需要保护个人的隐私
5. 可以借助法律来保护网络隐私权

答案：C

1. (中等）我们常提到的”在Windows操作系统中安装VMware，运行Linux虚拟机"属于( )。
2. 存储虚拟化
3. 内存虚拟化
4. 系统虚拟化
5. 网络虚拟化

答案：C

1. （容易）好友的QQ突然发来一个网站链接要求投票,最合理的做法是（ ）
2. 因为是其好友信息,直接打开链接投票
3. 可能是好友QQ被盗，发来的是恶意链接，先通过手机跟朋友确认链接无异常后，再酌情考虑是否投票
4. 不参与任何投票.
5. 把好友加入黑名单

答案：B

1. （容易）使用微信时可能存在安全隐患的行为是?( )
2. 允许“回复陌生人自动添加为朋友"
3. 取消“允许陌生人查看10张照片”功能
4. 设置微信独立帐号和密码，不共用其他帐号和密码
5. 安装防病毒软件，从官方网站下载正版微信

答案：A

1. （容易）微信收到“微信团队”的安全提示：“您的微信账号在16：46尝试在另一个设备登录。登录设备：XX品牌XX型号”。这时我们应该怎么做( ）
2. 有可能是误报，不用理睬
3. 确认是否是自己的设备登录,如果不是，则尽快修改密码
4. 自己的密码足够复杂，不可能被破解,坚决不修改密码
5. 拨打110报警，让警察来解决

答案：B

1. （中等）小强接到电话，对方称他的快递没有及时领取，请联系XXXX电话,小强拨打该电话后提供自己的私人信息后，对方告知小强并没有快递.过了一个月之后，小强的多个账号都无法登录。在这个事件当中，请问小强最有可能遇到了什么情况？（ ）
2. 快递信息错误而已，小强网站账号丢失与快递这件事情无关
3. 小强遭到了社会工程学诈骗，得到小强的信息从而反推出各种网站的账号密码
4. 小强遭到了电话诈骗，想欺骗小强财产
5. 小强的多个网站账号使用了弱口令，所以被盗。

答案：B

1. （中等） 注册或者浏览社交类网站时，不恰当的做法是:（ ）
2. 尽量不要填写过于详细的个人资料
3. 不要轻易加社交网站好友
4. 充分利用社交网站的安全机制
5. 信任他人转载的信息

答案：D

1. （容易）在某电子商务网站购物时,卖家突然说交易出现异常，并推荐处理异常的客服人员。以下最恰当的做法是？
2. 直接和推荐的客服人员联系
3. 如果对方是信用比较好的卖家，可以相信
4. 通过电子商务官网上寻找正规的客服电话或联系方式，并进行核实
5. 如果对方是经常交易的老卖家，可以相信

答案：C

1. （容易)你收到一条10086发来的短信,短信内容是这样的：“尊敬的用户,您好.您的手机号码实名制认证不通过,请到XXXX网站进行实名制验证，否则您的手机号码将会在24小时之内被停机”，请问,这可能是遇到了什么情况？
2. 手机号码没有实名制认证
3. 实名制信息与本人信息不对称，没有被审核通过
4. 手机号码之前被其他人使用过
5. 伪基站诈骗

答案:D

1. (容易)刘同学喜欢玩网络游戏。某天他正玩游戏，突然弹出一个窗口，提示:特大优惠！1元可购买10000元游戏币！点击链接后，在此网站输入银行卡账号和密码,网上支付后发现自己银行卡里的钱都没了。结合本实例，对发生问题的原因描述正确的是？
2. 电脑被植入木马
3. 用钱买游戏币
4. 轻信网上的类似“特大优惠”的欺骗链接，并透露了自己的银行卡号、密码等私密信息导致银行卡被盗刷
5. 使用网银进行交易

答案：C

1. （容易)李同学浏览网页时弹出 “新版游戏，免费玩，点击就送大礼包”的广告,李同学点了之后发现是个网页游戏，提示：“请安装插件"，请问，这种情况李同学应该怎么办最合适？（ ）
2. 为了领取大礼包，安装插件之后玩游戏
3. 网页游戏一般是不需要安装插件的，这种情况骗局的可能性非常大，不建议打开
4. 询问朋友是否玩过这个游戏，朋友如果说玩过，那应该没事.
5. 先将操作系统做备份，如果安装插件之后有异常，大不了恢复系统

答案:B

1. （容易）ATM机是我们日常存取现金都会接触的设备，以下关于ATM机的说法正确的是？
2. 所有ATM机运行的都是专业操作系统，无法利用公开漏洞进行攻击，非常安全，
3. ATM机可能遭遇病毒侵袭
4. ATM机无法被黑客通过网络进行攻击
5. ATM机只有在进行系统升级时才无法运行，其他时间不会出现蓝屏等问题。

答案:B

1. (中等）互联网世界中有一个著名的说法：“你永远不知道网络的对面是一个人还是一条狗！”，这段话表明，网络安全中\_\_\_\_\_\_.
2. 身份认证的重要性和迫切性
3. 网络上所有的活动都是不可见的
4. 网络应用中存在不严肃性
5. 计算机网络中不存在真实信息

答案：A

1. （困难）对于青少年而言,日常上网过程中,下列选项，存在安全风险的行为是?
2. 将电脑开机密码设置成复杂的15位强密码
3. 安装盗版的操作系统
4. 在QQ聊天过程中不点击任何不明链接
5. 避免在不同网站使用相同的用户名和口令

答案：B

1. （容易）青少年在使用网络中，正确的行为是\_\_\_\_\_\_。
2. 把网络作为生活的全部
3. 善于运用网络帮助学习和工作，学会抵御网络上的不良诱惑
4. 利用网络技术窃取别人的信息。
5. 沉迷网络游戏

答案：B

1. (容易)我们经常从网站上下载文件、软件,为了确保系统安全,以下哪个处理措施最正确\_\_\_\_\_\_
2. 直接打开或使用
3. 先查杀病毒，再使用
4. 习惯于下载完成自动安装
5. 下载之后先做操作系统备份，如有异常恢复系统

答案：B

1. （容易）我们在日常生活和工作中，为什么需要定期修改电脑、邮箱、网站的各类密码？(）
2. 遵循国家的安全法律
3. 降低电脑受损的几率
4. 确保不会忘掉密码
5. 确保个人数据和隐私安全

答案:D

1. (中等）浏览网页时，弹出“最热门的视频聊天室”的页面，遇到这种情况，一般怎么办？\_\_\_\_\_\_
2. 现在网络主播很流行，很多网站都有，可以点开看看
3. 安装流行杀毒软件，然后再打开这个页面
4. 访问完这个页面之后,全盘做病毒扫描
5. 弹出的广告页面,风险太大，不应该去点击

答案：D

1. (容易）U盘里有重要资料,同事临时借用，如何做更安全？
2. 同事关系较好可以借用
3. 删除文件之后再借
4. 同事使用U盘的过程中，全程查看
5. 将U盘中的文件备份到电脑之后，使用杀毒软件提供的“文件粉碎”功能将文件粉碎，然后再借给同事

答案：D

1. （容易）家明在网上购买iphone4,结果收到4个水果。家明自觉受骗,联系电商，电商客服告诉家明，可能是订单有误，让家明重新下单,店家将给家明2个iphone。如果家明报警，店家也无任何法律责任，因为家明已经在签收单上签字了。为维护自身合法权益，家明应该怎么做？
2. 为了买到IPHONE,再次交钱下单
3. 拉黑网店，再也不来这里买了
4. 向网站管理人员申诉，向网警报案
5. 和网店理论,索要货款

答案：C

1. （容易）随着网络时代的来临,网络购物进入我们每一个人的生活，快捷便利，价格低廉。网购时应该注意( ）
2. 网络购物不安全，远离网购
3. 在标有网上销售经营许可证号码和工商行政管理机关标志的大型购物网站网购更有保障
4. 不管什么网站，只要卖的便宜就好
5. 查看购物评价再决定

答案:B

1. （困难）信息安全的主要目的是为了保证信息的（ ）
2. 完整性、机密性、可用性
3. 安全性、可用性、机密性
4. 完整性、安全性、机密性
5. 可用性、传播性、整体性

答案:A

1. （中等）赵女士的一个正在国外进修的朋友，晚上用QQ联系赵女士，聊了些近况并谈及国外信用卡的便利,问该女士用的什么信用卡,并好奇地让其发信用卡正反面的照片给他，要比较下国内外信用卡的差别。该女士有点犹豫，就拨通了朋友的电话，结果朋友说QQ被盗了。那么不法分子为什么要信用卡的正反面照片呢？( )
2. 对比国内外信用卡的区别
3. 复制该信用卡卡片
4. 可获得卡号、有效期和CVV（末三位数）该三项信息已可以进行网络支付
5. 收藏不同图案的信用卡图片

答案：(C）

1. （容易) 你的QQ好友给你在QQ留言，说他最近通过网络兼职赚了不少钱，让你也去一个网站注册申请兼职。但你打开该网站后发现注册需要提交手机号码并发送验证短信。以下做法中最合理的是？(）
2. 提交手机号码并且发送验证短信
3. 在QQ上询问朋友事情的具体情况
4. 不予理会,提交手机号码泄露个人隐私，发送验证短信可能会被诈骗高额话费
5. 多手段核实事情真实性之后,再决定是否提交手机号码和发送验证码

答案:D

1. （容易）下列关于计算机木马的说法错误的是\_\_\_\_。
2. Word文档也会感染木马
3. 尽量访问知名网站能减少感染木马的概率
4. 杀毒软件对防止木马病毒泛滥具有重要作用
5. 只要不访问互联网，就能避免受到木马侵害

答案:D

1. （容易）网盘是非常方便的电子资料存储流转工具。不仅不占用空间，而且在任何电脑上都能访问，下面这些使用网盘的做法中，哪一项会造成个人隐私信息泄露的风险？
2. 将自己的信息分类，不重要的信息例如游戏文件、视频文件上传到云盘,个人身份证等信息存放在自己的电脑上
3. 自己的照片等信息加密后再存储到云盘，或者使用云盘的保密文件夹功能
4. 将所有信息保存在云盘，设置一个复杂的云盘密码，然后将密码信息保存在电脑D盘的文件夹中
5. 认真研究云盘的功能，设置云盘的强密码，谨慎使用分享功能

答案:C

1. （容易）当前网络中的鉴别技术正在快速发展,以前我们主要通过账号密码的方式验证用户身份，现在我们会用到U盾识别、指纹识别、面部识别、虹膜识别等多种鉴别方式。请问下列哪种说法是正确的。
2. 面部识别依靠每个人的脸型作为鉴别依据，面部识别无法伪造
3. 指纹识别相对传统的密码识别更加安全
4. 使用多种鉴别方式比单一的鉴别方式相对安全
5. U盾由于具有实体唯一性,被银行广泛使用，使用U盾没有安全风险

答案：C

1. （容易）以下对使用云计算服务的理解哪一个是正确的？
2. 云计算是高科技，XX是大公司，所以XX云上的虚拟机肯定安全，可以放心存放用户的各种信息
3. 云计算里的虚拟机不是自己的主机，可以随便折腾，安装各种恶意软件
4. 云中的主机也需要考虑安全性，云服务商应该定期打补丁，安装杀毒软件
5. 云计算中的数据存放在别人的电脑中，不安全，不要使用

答案：C

1. （容易）电脑中安装哪种软件，可以减少病毒、特洛伊木马程序和蠕虫的侵害？（ ）
2. VPN软件
3. 杀毒软件
4. 备份软件
5. 安全风险预测软件

答案：B

1. (容易）“短信轰炸机”软件 会对我们的手机造成怎样的危害( )
2. 短时内大量收到垃圾短信，造成手机死机
3. 会使手机发送带有恶意链接的短信
4. 会损害手机中的SIM卡
5. 会大量发送垃圾短信，永久损害手机的短信收发功能

答案：A

1. （容易)iPhone手机“越狱”是指( ）
2. 带着手机逃出去
3. 通过不正常手段获得苹果手机操作系统的最高权限
4. 对操作系统升级
5. 修补苹果手机的漏洞

答案：B

1. （中等)位置信息和个人隐私之间的关系，以下说法正确的是\_\_\_\_\_\_
2. 我就是普通人，位置隐私不重要，可随意查看
3. 位置隐私太危险，不使用苹果手机，以及所有有位置服务的电子产品
4. 需要平衡位置服务和隐私的关系，认真学习软件的使用方法，确保位置信息不泄露
5. 通过网络搜集别人的位置信息，可以研究行为规律

答案:C

1. （容易）关于适度玩网络游戏的相关安全建议,以下哪项是最不妥当的行为（)？
2. 选择网络游戏运营商时，要选择合法正规的运营商
3. 保留有关凭证，如充值记录、协议内容、网上转账记录等,以便日后维权使用
4. 在网吧玩游戏的时候，登录网银购买游戏币
5. 不要轻易购买大金额的网游道具

答案：C

1. （中等）电子邮件地址上的@是\_\_\_\_\_\_的意思
2. 互联网
3. 邮件服务器
4. 在……上
5. 发送……上

答案:C

1. （中等）韩同学收到一封邮件，说自己的QQ号码存在异常,需要紧急处理，点开网站后需要输入QQ号、密码，以下最合理的做法是？
2. QQ号码存在异常，应立即按邮件要求处理
3. QQ密码设置复杂，没有安全问题,不予理睬
4. 检查邮件标题是否为蓝色，如果不是蓝色标题,则可确定这封邮件为仿冒官方的盗号邮件,可直接举报
5. 冻结此QQ，不再使用

答案：C

1. （容易）为了确保电子邮件中邮件内容的安全，应该采用以下哪种方式比较恰当（）
2. 电子邮件发送时要加密，并注意不要错发
3. 电子邮件不需要加密码
4. 只要向接收者正常发送就可以了
5. 使用移动终端发送邮件

答案:A

1. （容易）家明发现某网站可以观看“XX魔盗团2”，但是必须下载专用播放器，家明应该怎么做？
2. 安装播放器观看
3. 打开杀毒软件，扫描后再安装
4. 先安装，看完电影后再杀毒
5. 不安装，等待正规视频网站上线后再看

答案:D

1. （容易）下面关于我们使用的网络是否安全的正确表述是\_\_\_\_\_\_
2. 安装了防火墙,网络是安全的
3. 设置了复杂的密码，网络是安全的
4. 安装了防火墙和杀毒软件,网络是安全的
5. 没有绝对安全的网络，使用者要时刻提高警惕，谨慎操作

答案:D

1. （容易)以下不属于电脑病毒特点的是?
2. 寄生性
3. 传染性
4. 潜伏性
5. 唯一性

答案：D

1. (容易）网络安全领域，把已经被发现,但相关软件厂商还没有进行修复的漏洞叫什么漏洞？
2. 0day漏洞
3. DDAY漏洞
4. 无痕漏洞
5. 黑客漏洞

答案：A

1. （中等）通过电脑病毒甚至可以对核电站、水电站进行攻击导致其无法正常运转,对这一说法你认为以下哪个选项是准确的？
2. 理论上可行，但没有实际发生过
3. 病毒只能对电脑攻击,无法对物理环境造成影响
4. 不认为能做到,危言耸听
5. 绝对可行，已有在现实中实际发生的案例

答案：D

1. （容易）家明使用安装了Windows操作系统的电脑，同学建议他电脑中重要的资料最好不要保存在C盘中。下列哪个观点最合理？
2. 这种说法没有根据
3. 文件存储在C盘容易被系统文件覆盖
4. C盘是默认系统盘，不能存储其他文件
5. C盘最容易遭到木马病毒的攻击，而且重装系统时会删除C盘上的所有文件，如果备份不及时会造成严重影响

答案：D

1. （容易)我们应当及时修复计算机操作系统和软件的漏洞，是因为（ ）
2. 操作系漏洞补丁及时升级,软件漏洞补丁就没有必要及时修复
3. 以前经常感染病毒的机器,现在就不存在什么漏洞了
4. 漏洞就是计算机系统或者软件系统的缺陷，病毒和恶意软件可以通过这个缺陷趁虚而入
5. 手动更新后,玩游戏时操作系统就不会自动更新,不会占用网络带宽了

答案:C

1. （容易)张同学发现安全软件提醒自己的电脑有系统漏洞，如果你是张同学，最恰当的做法是？()
2. 立即更新补丁，修复漏洞
3. 不与理睬，继续使用电脑
4. 暂时搁置，一天之后再提醒修复漏洞
5. 重启电脑

答案：A

1. （中等)世界上首例通过网络攻击瘫痪物理核设施的事件是？
2. 巴基斯坦核电站震荡波事件
3. 以色列核电站冲击波事件
4. 伊朗核电站震荡波事件
5. 伊朗核电站震网(stuxnet）事件

答案：D

1. （中等）1988年美国一名大学生编写了一个程序，这是史上第一个通过Internet传播的计算机病毒.你知道这个病毒叫什么吗？
2. 小球病毒
3. 莫里斯蠕虫病毒
4. 红色代码
5. 震荡波

答案：B

1. （容易）对于人肉搜索,应持有什么样的态度？
2. 主动参加
3. 关注进程
4. 积极转发
5. 不转发，不参与

答案:D

1. (容易）Windows操作系统每个月都会发布一些漏洞更新修复程序，也被称为系统补丁.请问，微软公司通常在哪一天发布最新的系统漏洞补丁？
2. 美国当地时间，每个月的星期二
3. 看比尔盖茨心情
4. 美国时间周一早八点
5. 美国当地时间，每个月第二个星期的星期二

答案：D

1. （中等)发现个人电脑感染病毒，断开网络的目的是（）
2. 影响上网速度
3. 担心数据被泄露电脑被损坏
4. 控制病毒向外传播
5. 防止计算机被病毒进一步感染

答案:B

1. （容易）打电话诈骗密码属于\_\_\_\_\_\_\_\_攻击方式。
2. 木马
3. 社会工程学
4. 电话系统漏洞
5. 拒绝服务

答案：B

1. （容易）提倡文明上网，健康生活，我们不应该有下列哪种行为？
2. 在网上对其他网友进行人身攻击
3. 自觉抵制网上的虚假、低俗内容，让有害信息无处藏身
4. 浏览合法网站，玩健康网络游戏,并用自己的行动影响周围的朋友
5. 不信谣，不传谣，不造谣

答案：A

1. (容易）以下选项属于《文明上网自律公约》内容的是：。①自觉遵纪守法,倡导社会公德，促进绿色网络建设;②提倡自主创新，摒弃盗版剽窃，促进网络应用繁荣；③提倡诚实守信，摒弃弄虚作假，促进网络安全可信；④提倡人人受益,消除数字鸿沟，促进信息资源共享.
2. ②③④
3. ①②④
4. ①②③
5. ①②③④

答案：D

1. (中等）关于比特币敲诈者的说法不正确的是
2. 流行于2015年初
3. 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
4. 病毒作者波格挈夫来自俄罗斯
5. 主要通过网页传播

答案：D

1. (中等）浏览某些网站时，网站为了辨别用户身份进行session跟踪，而储存在本地终端上的数据是（ ）
2. 收藏夹
3. 书签
4. COOKIE
5. https

答案:C

1. （容易)下列关于密码安全的描述，不正确的是( ）
2. 容易被记住的密码不一定不安全
3. 超过12位的密码很安全
4. 密码定期更换
5. 密码中使用的字符种类越多越不易被猜中

答案：B

1. （困难)当一个发往目的地的主机IP包经过多个路由器转发时，以下说法正确的是（ )
2. 当IP包在每跳段中传输时,目的地址改为下一个路由器的IP地址。
3. 当一个路由器将IP包分发到广域网WAN时，目的的IP地址经常发生改变。
4. 目的的IP地址将永远是第一个路由器的IP地址。
5. 目的的IP地址固定不变

答案:D

1. （中等）当访问web网站的某个资源时,请求无法被服务器理解将会出现的HTTP状态码是( )
2. 200
3. 401
4. 302
5. 303

答案:B

1. （中等)对网络系统进行渗透测试,通常是按什么顺序来进行的：（ ）
2. 控制阶段、侦查阶段、入侵阶段
3. 入侵阶段、侦查阶段、控制阶段
4. 侦查阶段、入侵阶段、控制阶段
5. 侦查阶段、控制阶段、入侵阶段

答案:C

1. (容易）李欣打算从自己计算机保存的动画中挑选喜欢的发送给表姐欣赏，她应该从扩展名为( )的文件中进行查找。
2. 。mp3
3. 。swf
4. 。txt
5. .xls

答案：B

1. （中等）下图是一张图书销售系统数据库的图书表，其中包含（ ）个字段.



A、5 B、6 C、7 D、8

答案:C

1. （中等）当Windows系统出现某些错误而不能正常启动或运行时,为了提高系统自身的安全性，在启动时可以进入模式。
2. 异常
3. 安全
4. 命令提示符
5. 单步启动

答案:B

1. （中等）数据被非法篡改破坏了信息安全的（ ）属性.
2. 保密性
3. 完整性
4. 不可否认性
5. 可用性

答案：B

1. （困难）下列算法中属于非对称密码算法的是（   ）
2. IDEA
3. RSA
4. DES
5. 3DES

答案：B

1. （容易）量子[密码学](http://baike。baidu.com/view/25311。htm)的理论基础是\_\_\_\_\_\_
2. 量子力学
3. 数学
4. 传统密码学
5. 天体物理学

答案： A

1. (容易)传统密码学的理论基础是
2. 数学
3. 物理学
4. 计算机学科
5. 力学

答案：A

1. (实事类）（中等)我国首个城域量子通信试验示范网于2010年在（）启动建设
2. 北京
3. 上海
4. 合肥
5. 深圳

答案：C

1. （实事）(中等)世界首个量子卫星,中科院量子科学实验卫星（简称量子卫星）于（)发射
2. 2016年7月
3. 2015年10月
4. 2015年11月
5. 2016年 5月

答案：A

1. (中等）以下哪个选项是目前利用大数据分析技术无法进行有效支持的?
2. 新型病毒的分析判断
3. 天气情况预测
4. 个人消费习惯分析及预测
5. 精确预测股票价格

答案：D

1. （容易）关于物联网的说法，错误的是：
2. 万物互联将为我们的生活带来极大便利,节约沟通成本，提升资源利用效率
3. 物联网与互联网存在本质区别，黑客很难攻击到诸如网络摄像头之类的物理设备
4. 物联网是Internet of Things的意思，意即万物互联，是互联网的一部分
5. 物联网中很多设备都是使用着安卓操作系统

答案:B

1. (中等）电子商务的交易过程中,通常采用的抗抵赖措施是( )
2. 信息加密和解密
3. 信息隐匿
4. 数字签名和身份认证技术
5. 数字水印

答案：C

1. (困难）以下哪一项不在数字证书数据的组成中? ( ）
2. 版本信息
3. 有效使用期限
4. 签名算法
5. 版权信息

答案：D

1. （中等)以下对Windows 系统账号的描述,正确的是\_\_\_\_\_\_。
2. Windows系统默认不允许修改administrator管理员账号为其它名称
3. Windows 系统默认生成administrator 和guest 两个账号，两个账号都不可以改名
4. Windows 系统默认会生成administrator 和guest 两个账号,不允许修改guest账号名称
5. Windows 系统默认生成administrator 和guest 两个账号,两个账号都可以改名

答案：D

1. （困难）常见的密码系统包含的元素是\_\_\_\_\_\_？
2. 明文空间、密文空间、信道、加密算法、解密算法
3. 明文空间、摘要、信道、加密算法、解密算法
4. 明文空间、密文空间、密钥空间、加密算法、解密算法
5. 消息、密文空间、信道、加密算法、解密算法

答案：C

1. （困难）电子邮件客户端通常需要使用（ ）协议来发送邮件？
2. 仅SMTP
3. 仅POP
4. SMTP 和POP
5. 以上都不正确

答案：A

1. （中等）Windows操作系统从哪个版本开始引入安全中心的概念（ ）?
2. WinNT SP6
3. Win2000 SP4
4. WinXP SP2
5. Win2003 SP1

答案：C

1. （困难）：下面对于cookie的说法错误的是（ )？
2. cookie 是一小段存储在浏览器端文本信息,web 应用程序可以读取cookie 包含的信息
3. cookie 可以存储一些敏感的用户信息,从而造成一定的安全风险
4. 通过cookie 提交精妙构造的移动代码，绕过身份验证的攻击叫做cookie 欺骗
5. 防范cookie 欺骗的一个有效方法是不使用cookie 验证方法,而使用session 验证方法

答案：C

1. （困难）为了增强电子邮件的安全性，人们经常使用PGP软件，它是（ ）？
2. 一种基于RSA 的邮件加密软件
3. 一种基于白名单的反垃圾邮件软件
4. 基于SSL 的VPN 技术
5. 安全的电子邮箱

答案:A

1. （中等）以下关于Https 协议与Http 协议相比的优势说明，哪个是正确的：（ ）?
2. Https 协议对传输的数据进行了加密，可以避免嗅探等攻击行为
3. Https 使用的端口与Http 不同,让攻击者不容易找到端口，具有较高的安全性
4. Https 协议是Http 协议的补充,不能独立运行，因此需要更高的系统性能
5. Https 协议使用了挑战机制，在会话过程中不传输用户名和密码，因此具有较高的安全性

答案：A

1. （容易）王女士经常通过计算机网络进行购物，从安全角度看，下面哪项是不好的操作习惯( )？
2. 在使用网络浏览器时，设置不在计算机中保留网络历史记录和表单数据
3. 为计算机安装具有良好声誉的安全防护软件，包括病毒查杀、安全检查和安全加固方面的软件
4. 在IE 的配置中,设置只能下载和安装经过签名的、安全的ActiveX 控件
5. 采用专用的计算机进行网上购物，安装好软件后不对该计算机上的系统软件、应用软件进行升级

答案:D

1. （容易）小刘在某电器城购买了一台冰箱，并留下了个人姓名、电话和电子邮件地址等信息,第二天他收到了一封来自电器城提示他中奖的邮件，查看该邮件后他按照提示缴纳中奖税款后并没有得到中奖奖金，再打电话询问电器城才得知电器城并没有举办中奖活动。根据上面的描述，由此可以推断的是（ ）?
2. 小刘在电器城登记个人信息时,使用了加密手段
3. 小刘遭受了钓鱼邮件攻击，钱被骗走了
4. 小刘的计算机中了木马,被远程控制
5. 小刘购买的冰箱是智能冰箱，可以连网

答案:B

1. (容易）张三将微信个人头像换成微信群中某好友头像，并将昵称改为该好友的昵称，然后向该好友的其他好友发送一些欺骗信息。该攻击行为属于以下哪类攻击( ）？
2. 口令攻击
3. 暴力破解
4. 拒绝服务攻击
5. 社会工程学攻击

答案：D

1. （中等）管理员在审查入侵检测日志过程中，管理员注意到来自互联网的通信信息，从中显示了公司内部的薪酬服务器IP地址。下面哪个恶意的活动最可能造成这类结果（ ）?
2. 拒绝服务攻击
3. 地址欺骗
4. 端口扫描
5. 中间人攻击

答案:B

1. (中等)防范特洛伊木马软件进入学校网络最好的选择是（ )？
2. 部署击键监控程序
3. 部署病毒扫描应用软件
4. 部署状态检测防火墙
5. 部署调试器应用程序

答案：B

1. （中等）下面选项属于社会工程学攻击选项的是（ ）？
2. 逻辑炸弹
3. 木马
4. 包重放
5. 网络钓鱼

答案：D

1. (容易）没有自拍，也没有视频聊天，但电脑摄像头的灯总是亮着,这是什么原因（ ）
2. 可能中了木马，正在被黑客偷窥
3. 电脑坏了
4. 本来就该亮着
5. 摄像头坏了

答案：A

1. （容易）文件型病毒传染的对象主要是\_\_\_\_。
2. 。DOE和.EXE
3. 。DBF
4. 。WPS
5. 。EXE和。DOC

答案：A

1. (容易)电脑安装多款安全软件会有什么危害（）？
2. 可能大量消耗系统资源，相互之间产生冲突
3. 不影响电脑运行速度
4. 影响电脑的正常运行
5. 更加放心的使用电脑

答案：A

1. (容易）有一种网站,只要打开它,电脑就有可能感染木马病毒。这种网站的专业名称是什么?
2. 钓鱼网站
3. 挂马网站
4. 游戏网站
5. 门户网站

答案：B

1. （容易）如果你家里的电话或者手机只响一声就挂了，最佳的处理方式是
2. 立刻报警，一定是诈骗电话
3. “响一声"电话多数为吸费电话，如果是陌生号码，就不要理睬
4. 立刻报警，一定是诈骗电话
5. 不管是谁，拨回去把对方大骂一顿

答案:B

1. （困难）以下哪一项是DOS攻击的一个实例？
2. SQL注入
3. IP 地址欺骗
4. Smurf攻击
5. 字典破解

答案:C

1. （困难）以下哪一项是在兼顾可用性的基础上,防范SQL注入攻击最有效的手段:
2. 删除存在注入点的网页
3. 对数据库系统的管理
4. 对权限进行严格的控制，对web用户输入的数据进行严格的过滤
5. 通过网络防火墙严格限制Internet用户对web服务器的访问

答案：C

1. （中等）下列哪个漏洞不是由于未对输入做过滤造成的？
2. DOS攻击
3. SQL注入
4. 日志注入
5. 命令行注入

答案：A

1. （中等）POP服务器使用的端口号是\_\_\_\_.
2. tcp端口25
3. tcp端口110
4. tcp端口143
5. tcp端口23

答案：B

1. （中等）下列哪个选项是不能执行木马脚本的后缀（）？
2. asp
3. php
4. cer
5. htm

答案：D

1. （困难)ASP木马不具有的功能是\_\_\_\_.
2. 上传功能
3. 远程溢出提权功能
4. 下载功能
5. 浏览目录功能

答案：B

1. （困难）命令注入的危害不包括下列哪项?
2. 获取服务器信息
3. 构造一句话木马
4. 盗取当前用户cookie
5. 更改网站主页

答案：D

1. (中等)以下哪项不属于防止口令被猜测的措施？
2. 严格限定从一个给定的终端进行认证的次数
3. 确保口令不在终端上再现
4. 防止用户使用太短的口令
5. 使用机器产生的口令

答案：B

1. （容易）如果某天你在Windows系统下观察到，U盘中多出了一个原来并不存在的“回收站"图标或文件夹，则最可能的原因是:
2. U盘损坏
3. 感染了病毒
4. 磁盘碎片所致
5. U盘中有垃圾文件没有彻底清理

答案：B

1. （困难）利用FTP进行文件传输时的主要安全问题存在于：
2. 匿名登录不需要密码
3. 破坏程序能够在客户端运行
4. 破坏程序能够在服务器端运行
5. 登录的用户名和密码会明文传输到服务器端

答案；D

1. （中等)域名服务系统(DNS）的功能是：
2. 完成域名和IP地址之间的转换
3. 完成域名和网卡地址之间的转换
4. 完成主机名和IP地址之间的转换
5. 完成域名和电子邮件地址之间的转换

答案:A

1. （容易)小李既属于“一般用户”组，又属于“高级用户”组，现要访问“工作文档”目录，已知“一般用户”组对于此文件夹的操作权限是“只读"，“高级用户”组对此文件夹的操作权限是“可写"，那么小李现在可对“工作文档”目录进行什么操作？
2. 仅可读
3. 仅可写
4. 既可读又可写
5. 权限冲突，无法做任何操作

答案：C

1. （中等)王先生近期收到了一封电子邮件，发件人显示是某同事，但该邮件十分可疑，没有任何与工作相关内容，邮件中带有一个陌生的网站链接，要求他访问并使用真实姓名注册,这可能属于哪种攻击手段（ ）
2. 缓冲区溢出攻击
3. 钓鱼攻击
4. 水坑攻击
5. DDOS攻击

答案：B

1. (容易）网络安全领域，VPN通常用于建立\_\_\_\_\_\_之间的安全访问通道。
2. 总部与分支机构、与合作伙伴、与移动办公用户、远程用户；
3. 客户与客户、与合作伙伴、远程用户;
4. 同一个局域网用户；
5. 仅限于家庭成员；

答案：A

1. （容易)驻留在网页上的恶意代码通常利用（ )来实现植入并进行攻击.
2. 口令攻击
3. U盘工具
4. 浏览器软件的漏洞
5. 拒绝服务攻击

答案：C

1. （中等）用户暂时离开时,锁定Windows系统以免其他人非法使用。锁定系统的快捷方式为同时按住（ ) 。
2. WIN键和Z键
3. F1键和L键
4. WIN键和L键
5. F1键和Z键

答案：C

1. （容易）要安全浏览网页，不应该( ）。
2. 在公用计算机上使用“自动登录”和“记住密码”功能
3. 禁止开启ActiveX控件和Java脚本
4. 定期清理浏览器Cookies
5. 定期清理浏览器缓存和上网历史记录

答案：A

1. （中等)王同学喜欢在不同的购物和社交网站进行登录和注册，但他习惯于在不同的网站使用相同的用户名和密码进行注册登录，某天，他突然发现，自己在微博和很多网站的账号同时都不能登录了，这些网站使用了同样的用户名和密码，请问,王同学可能遭遇了以下哪类行为攻击:（ )。
2. 拖库
3. 撞库
4. 建库
5. 洗库

答案 : B

1. （容易)在连接互联网的计算机上( ）处理、存储涉及国家秘密和企业秘密信息。
2. 可以
3. 严禁
4. 不确定
5. 只要网络环境是安全的，就可以

答案：B

1. (容易）重要数据要及时进行（ ）,以防出现意外情况导致数据丢失。
2. 杀毒
3. 加密
4. 备份
5. 格式化

答案:C

1. （容易）下面哪个口令的安全性最高（ )
2. integrity1234567890
3. ！＠7es6RFE,,,d195ds＠@SDa
4. passW@odassW@odassW＠od
5. ichunqiuadmin123456

答案：B

1. （容易）主要用于通信加密机制的协议是( ）
2. HTTP
3. FTP
4. TELNET
5. SSL

答案：D

1. （容易）在网络访问过程中，为了防御网络监听，最常用的方法是 ( )
2. 采用物理传输（非网络）
3. 对信息传输进行加密
4. 进行网络伪装
5. 进行网络压制

答案:B

1. （中等）属于操作系统自身的安全漏洞的是:（ ）.
2. 操作系统自身存在的“后门"
3. QQ木马病毒
4. 管理员账户设置弱口令
5. 电脑中防火墙未作任何访问限制

答案 : A

1. （中等）Windows 操作系统提供的完成注册表操作的工具是：（)。
2. syskey
3. msconfig
4. ipconfig
5. regedit

答案 ： D

1. (中等）使用不同的密钥进地加解密，这样的加密算法叫（ ）。
2. 对称式加密算法
3. 非对称式加密算法
4. MD5
5. HASH算法

答案 : B

1. （容易)有一类木马程序，它们主要记录用户在操作计算机时敲击键盘的按键情况,并通过邮件发送到控制者的邮箱。这类木马程序属于：（ ）。
2. 破坏型
3. 密码发送型
4. 远程访问型
5. 键盘记录型

答案 ： D

1. （容易)关于暴力破解密码，以下表述正确的是？（ ）
2. 就是使用计算机不断尝试密码的所有排列组合，直到找出正确的密码
3. 指通过木马等侵入用户系统,然后盗取用户密码
4. 指入侵者通过电子邮件哄骗等方法，使得被攻击者提供密码
5. 通过暴力威胁,让用户主动透露密码

答案：A

1. （中等)关于黑客的主要攻击手段,以下描述不正确的是？（ ）
2. 包括社会工程学攻击
3. 包括暴力破解攻击
4. 直接渗透攻击
5. 不盗窃系统资料

答案：D

1. （中等）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（）
2. 对称加密技术
3. 分组密码技术
4. 公钥加密技术
5. 单向函数密码技术

答案：A

1. （容易）在使用网络和计算机时，我们最常用的认证方式是:
2. 用户名／口令认证
3. 指纹认证
4. CA认证
5. 动态口令认证

答案：A

1. （中等）许多黑客都利用系统和软件中的漏洞进行攻击,对此，以下最有效的解决方案是什么？（ ）
2. 安装防火墙
3. 安装入侵检测系统
4. 给系统和软件更新安装最新的补丁
5. 安装防病毒软件

答案：C

1. （中等)邮件炸弹攻击主要是( )
2. 破坏被攻击者邮件服务器
3. 恶意利用垃圾数据塞满被攻击者邮箱
4. 破坏被攻击者邮件客户端
5. 猜解受害者的邮箱口令

答案:B

1. (容易）网络扫描工具( ）
2. 只能作为攻击工具
3. 只能作为防范工具
4. 既可作为攻击工具也可以作为防范工具
5. 不能用于网络攻击

答案：C

1. （中等)操作系统中\_\_\_\_文件系统支持加密功能（ ）
2. NTFS
3. FAT32
4. FAT
5. EFS

答案：A

1. （容易）某网站的用户登录需要输入4位数字的验证码，假设该网站不设置对验证码输入错误次数的限制，如果对验证短信进行暴力破解，最多尝试多少次就可以完成破解？
2. 1000次
3. 10000次
4. 1000000次
5. 20000次

答案：B

1. （容易)一般来说，个人计算机中的防病毒软件无法防御以下哪类威胁？
2. Word病毒
3. DDoS攻击
4. 电子邮件病毒
5. 木马

答案：B

1. (中等）IPv6是由互联网工程任务组（Internet Engineering Task Force，IETF）设计的下一代IP协议,IPv6采用的地址长度是:\_\_\_\_\_\_\_\_\_
2. 256位
3. 128位
4. 64位
5. 512位

答案：B

1. （容易)近年来，电子邮件用户和公司面临的安全性风险日益严重,以下不属于电子邮件安全威胁的是：\_\_\_\_\_\_\_\_\_
2. SMTP的安全漏洞
3. 电子邮件群发
4. 邮件炸弹
5. 垃圾邮件

答案：B

1. （中等）宏病毒是一种寄存在文档或模板宏中的计算机病毒,以下那种类型的文件不会被宏病毒感染：\_\_\_\_\_\_\_\_\_
2. doc
3. xls
4. exe
5. ppt

答案：C

1. (中等）《保守国家秘密法》中规定,机密级国家秘密保密期限一般不超过\_\_\_\_\_\_\_\_\_年：
2. 五十年
3. 二十年
4. 十年
5. 三十年

答案：B

1. （中等）释放计算机当前获得的IP地址,使用的命令是：\_\_\_\_\_\_\_\_\_
2. ipconfig
3. ipconfig /all
4. ipconfig /renew
5. ipconfig /release

答案：D

1. (中等）以下关于Windows服务描述说法错误的是：\_\_\_\_\_\_\_\_\_
2. Windows服务通常是以管理员身份运行
3. 可以作为独立的进程运行或通过DLL的形式依附在svchost进程
4. 为提升系统的安全性，管理员应尽量关闭不需要的系统服务
5. Windows服务需要用户交互登录才能运行

答案:D

1. (中等） 以下关于风险，说法错误的是:\_\_\_\_\_\_\_\_\_
2. 风险是客观存在的
3. 任何措施都无法完全清除风险
4. 可以采取适当措施，彻底清除风险
5. 风险是指一种可能性

答案：C

1. （中等）如果希望通过防火墙禁止QQ工具联网，应该修改Windows防火墙以下哪项设置：\_\_\_\_\_\_\_\_\_
2. 入站规则
3. 出站规则
4. 连接安全规则
5. 监视

答案:B

1. （中等）Windows server来宾用户登录主机时,用户名为：\_\_\_\_\_\_\_\_\_
2. anonymous
3. admin
4. root
5. guest

答案：D

1. （容易）DHCP可以用来为每台设备自动分配\_\_\_\_\_\_\_\_\_
2. IP地址
3. MAC地址
4. URL
5. 服务器名称

答案:A

1. （中等）网页病毒(又称网页恶意代码）是利用网页来进行破坏的病毒，它是使用一些SCRIPT语言编写的恶意代码。攻击者通常利用什么植入网页病毒：\_\_\_\_\_\_\_\_\_
2. 拒绝服务攻击
3. 口令攻击
4. 平台漏洞
5. U盘工具

答案：C

1. (中等）可以被数据完整性机制防止的攻击方式是\_\_\_\_\_\_
2. 假冒源地址或用户的地址欺骗攻击;
3. 抵赖做过信息的递交行为;
4. 数据中途被攻击者窃听获取；
5. 数据在途中被攻击者篡改或破坏

答案:D

1. (中等）“进不来” “拿不走” “看不懂" “改不了” “走不脱”是网络信息安全建设的目的.其中,“看不懂”是指下面那种安全服务：
2. 数据加密
3. 身份认证
4. 数据完整性
5. 访问控制

答案:A

1. (困难）DES算法密钥是 64 位，因为其中一些位是用作校验的，密钥的实际有效位是\_\_\_\_\_\_\_\_位。
2. 60
3. 56
4. 54
5. 48

答案：B

1. （容易）下面哪一是基于一个大的整数很难分解成两个素数因数？
2. ECC
3. RSA
4. DES
5. Diffie—Hellman

答案：B

1. （中等）若A给B发送一封邮件，并想让B能验证邮件是由A发出的,则A应该选用\_\_\_\_\_\_\_\_对邮件加密。
2. A的公钥
3. A的私钥
4. B的公钥
5. B的私钥

答案：B

1. （容易）数据加密标准DES采用的密码类型是？
2. 序列密码
3. 分组密码
4. 散列码
5. 随机码

答案：B

1. （容易）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？
2. 散列算法
3. 随机数生成算法
4. 对称密钥算法
5. 非对称密钥算法

答案：C

1. (容易）非对称密码算法具有很多优点,其中不包括：
2. 可提供数字签名、零知识证明等额外服务；
3. 加密/解密速度快,不需占用较多资源；
4. 通信双方事先不需要通过保密信道交换密钥；
5. 密钥持有量大大减少

答案：B

1. （容易）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：
2. C 1级
3. D级
4. B 1级
5. A 1级

答案：D

1. （容易）密码分析的目的是什么？
2. 确定加密算法的强度
3. 增加加密算法的代替功能
4. 减少加密算法的换位功能
5. 确定所使用的换位

答案:A

1. (容易）CA认证中心的主要作用是：
2. 加密数据；
3. 发放数字证书;
4. 安全管理;
5. 解密数据

答案：B

1. （容易）哪种访问控制技术方便访问权限的频繁更改？
2. 自主访问控制；
3. 强制访问控制；
4. 基于角色的访问控制;
5. 基于格的访问控制

答案:C

1. （容易)\_\_\_\_\_\_\_\_是以文件为中心建立的访问权限表。
2. 访问控制矩阵 ;
3. 访问控制表；
4. 访问控制能力表 ;
5. 角色权限表

答案：B

1. （容易）文件的拥有者可以决定其他用户对于相应的文件有怎样的访问权限,这种访问控制是
2. 自主访问控制 ;
3. 强制访问控制 ；
4. 主体访问控制 ;
5. 基于角色的访问控制策略

答案:A

1. （容易)以下哪一项是伪装成有用程序的恶意软件？
2. 计算机病毒;
3. 特洛伊木马;
4. 逻辑炸弹;
5. 蠕虫程序

答案:B

1. （中等）下列不属于网络蠕虫的恶意代码是
2. 冲击波;
3. SQL SLAMMER；
4. 熊猫烧香 ;
5. 红色代码

答案:C

1. (容易)近年来黑客的网络攻击行为模式发生了很大的变化，并且呈现愈演愈烈的趋势,其中的根本原因是什么？
2. 黑客热衷制造轰动效应；
3. 黑客受到利益驱动；
4. 系统安全缺陷越来越多；
5. 黑客技术突飞猛进

答案:B

1. （容易)\_\_\_\_\_\_\_\_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。
2. 蜜网
3. 鸟饵
4. 鸟巢
5. 玻璃鱼缸

答案：A

1. （中等）下列哪种病毒能对计算机硬件产生破坏？
2. CIH ；
3. CODE RED；
4. 维金
5. 熊猫烧香

答案：A

1. （容易）以下哪一项不属于恶意代码？
   * 1. 病毒；
     2. 蠕虫;
     3. 远程管理软件;
     4. 木马

答案:C

1. (容易）攻击者截获并记录了从A到B的数据,然后又从早些时候所截获的数据中提取出信息重新发往B，称为
2. 中间人攻击 ；
3. 强力攻击 ;
4. 重放攻击；
5. 注入攻击

答案：C

1. (容易）以下不可以防范口令攻击的是:
2. 设置的口令要尽量复杂些，最好由字母、数字、特殊字符混合组成；
3. 在输入口令时应确认无他人在身边；
4. 定期改变口令;
5. 选择一个安全性强复杂度高的口令，所有系统都使用其作为认证手段

答案：D

1. (中等）向有限的空间输入超长的字符串是哪一种攻击手段？
2. 缓冲区溢出;
3. 网络监听；
4. 拒绝服务 ;
5. IP欺骗

答案:A

1. （容易)下列哪一项信息不包含在X.509规定的数字证书中？
2. 证书有效期；
3. 证书持有者的公钥；
4. 证书颁发机构的签名;
5. 证书颁发机构的私钥

答案：D

1. （容易）以下那种生物鉴定设备具有最低的误报率?
2. 指纹识别;
3. 语音识别;
4. 掌纹识别；
5. 签名识别

答案：A

1. （容易）以下哪一项鉴别机制不属于强鉴别机制？
2. 令牌+口令；
3. PIN码+口令;
4. 签名+指纹；
5. 签名+口令

答案:B

1. (中等）对称密钥密码体制的主要缺点是；
2. 加、解密速度慢;
3. 密钥的分配和管理问题;
4. 应用局限性;
5. 加密密钥与解密密钥不同

答案:B

1. （容易）以下哪一项不属于入侵检测系统的功能；
2. 监视网络上的通信数据流；
3. 捕捉可疑的网络活动;
4. 提供安全审计报告;
5. 过滤非法的数据包

答案:D

1. （容易）关闭系统多余的服务有什么安全方面的好处？
2. 使黑客选择攻击的余地更小;
3. 关闭多余的服务以节省系统资源;
4. 使系统进程信息简单，易于管理;
5. 没有任何好处

答案：A

1. （容易)一台计算机可以有\_\_\_\_\_\_\_\_个不同的IP地址。
2. 只能1个;
3. 只能2个;
4. 最多3个；
5. 多个

答案：D

1. （容易）黑客搭线窃听属于哪一类风险？
2. 信息存储安全；
3. 信息传输安全；
4. 信息访问安全；
5. 以上都不正确

答案：B

1. （容易)有些计算机病毒每感染一个EXE文件就会演变成为另一种病毒，这种特性称为计算机病毒的\_\_\_\_\_.
2. 激发性;
3. 传播性;
4. 衍生性;
5. 隐蔽性

答案：C

1. （中等）以下\_\_\_\_\_\_\_\_不属于渗透测试。
2. 白盒测试；
3. 黑盒测试;
4. 灰盒测试;
5. 红盒测试

答案：D

1. （容易）网络安全中的“木桶原理"通常是指；
2. 整体安全水平由安全级别最低的部分所决定;
3. 整体安全水平由安全级别最高的部分所决定；
4. 整体安全水平由各组成部分的安全级别平均值所决定；
5. 以上都不对

答案：A

1. （容易)在生物特征认证中,不适宜于作为认证特征的是;
2. 指纹;
3. 虹膜；
4. 脸像;
5. 体重

答案：D

1. (容易）访问以下哪个网址将可能遭受钓鱼攻击：
2. www.1cbc.com。cn;
3. www.qq.com;
4. www。taobao。com；
5. www.sina。com

答案：A

1. （容易)关于“肉鸡"以下哪种说法正确?
2. 发起主动攻击的机器;
3. 被黑客植入木马的机器，黑客通过木马控制端控制肉鸡参与攻击;
4. 用户通常自愿成为肉鸡；
5. 肉鸡不能发动攻击

答案:B

1. （容易)“心脏出血”漏洞会导致以下哪类信息被泄露？
2. 存储在客户端的重要信息；
3. 邮件附件中的重要信息；
4. 存储在网站服务器内存中的重要信息；
5. 正在网络中传输的重要信息;

答案：C

1. （容易)逻辑炸弹通常是通过\_\_\_\_\_\_\_\_。
2. 必须远程控制启动执行，实施破坏;
3. 指定条件或外来触发启动执行，实施破坏 ;
4. 通过管理员控制启动执行，实施破坏;
5. 通过物理机执行破坏

答案：B

1. （容易）一台需要与互联网通信的 WEB 服务器放在以下哪个位置最安全? ( ）
2. 在 DMZ 区
3. 在内网中
4. 和防火墙在同一台计算机上
5. 在互联网防火墙外

答案：A

1. (容易）下面哪一个选项能用来描述隐含在网页代码指令中的恶意代码，该恶意代码可以修改 IE 首页、弹窗等 ：
2. 主引导区病毒 主引导区病毒
3. 宏病毒
4. 木马
5. 脚本病毒

答案：D

1. （容易）防火墙一般都具有网络地址转换功能（ Network Address Translation,NAT)，NAT允许多台计算机使用一个( )连接网络:
2. Web 浏览器
3. IP 地址
4. 代理服务器
5. 服务器名

答案:B

1. （容易)云计算是通过使计算分布在大量的分布式计算机上，而非本地计算机或远程服务器中，使个人和企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。目前已经有很多云计算相关的服务可供普通用户使用，家明就在XX云上申请了一个虚拟机，在上面部署了自己的个人网站.请问下列家明对云计算的理解哪一个是正确的？”
2. 云计算是高科技，XX是大公司，所以XX云上的虚拟机肯定安全，可以存放用户的各种信息
3. 云计算里的虚拟机不是自己的主机，可以随便折腾，安装各种恶意软件
4. 云中的主机也需要考虑安全性，云服务商应该定期打补丁,安装杀毒软件
5. 云计算中的数据存放在别人的电脑中，不安全，不要使用

答案：C

1. （中等)下列哪个算法属于非对称算法（)。

A、SSF33  
B、DES  
C、SM3  
D、M2

答案:D

1. （困难)根据我国《电子签名法》第2条的规定，电子签名,是指数据电文中以电子形式所含、所附用于(?)，并标明签名人认可其中内容的数据。  
   A、识别签名人  
   B、识别签名人行为能力  
   C、识别签名人权利能力  
   D、识别签名人的具体身份  
   答案：A
2. （中等)根据我国《电子签名法》的规定，数据电文是以电子、光学、磁或者类似手段（ )的信息。  
   A、生成、发送  
   B、生产、接收  
   C、生成、接收、储存  
   D、生成、发送、接收、储存  
   答案:D
3. (中等）我国《电子签名法》第三条规定：“当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否认其效力”。这一确认数据电文法律效力的原则是（？）。  
   A、公平原则  
   B、歧视性原则  
   C、功能等同原则  
   D、非歧视性原则  
   答案:C
4. （中等）《电子签名法》既注意与国际接轨，又兼顾我国国情，下列不属于《电子签名法》所采用的原则或制度是（）。  
   A:技术中立原则  
   B：无过错责任原则  
   C：当事人意思自治原则  
   D：举证责任倒置原则  
   答案:B
5. （中等）身份认证的要素不包括（）  
   A：你拥有什么(What you have)  
   B：你知道什么（What you know）  
   C：你是什么（What you are)  
   D：用户名  
   答案：D
6. （容易）下面不属于网络钓鱼行为的是（）  
   A:以银行升级为诱饵，欺骗客户点击金融之家进行系统升级  
   B:黑客利用各种手段，可以将用户的访问引导到假冒的网站上  
   C:用户在假冒的网站上输入的信用卡号都进入了黑客的银行  
   D：网购信息泄露，财产损失  
   答案:D
7. （困难)电子合同的法律依据是《电子签名法》、《合同法》和以下的(）。  
   A：民事诉讼法  
   B:刑法  
   C:会计法  
   D:公司法  
   答案：A
8. (中等）Morris蠕虫病毒，是利用（）  
   A：缓冲区溢出漏洞  
   B：整数溢出漏洞  
   C：格式化字符串漏洞  
   D:指针覆盖漏洞  
   答案:A
9. （容易）某网站的流程突然激增，访问该网站响应慢,则该网站最有可能受到的攻击是？（)  
   A：SQL注入攻击  
   B：特洛伊木马  
   C：端口扫描  
   D：DOS攻击  
   答案:D
10. （容易）个人用户之间利用互联网进行交易的电子商务模式是(）  
    A:B2B  
    B:P2P  
    C：C2C  
    D：O2O  
    答案：C
11. （容易）门禁系统属于（)系统中的一种安防系统。  
    A:智能强电  
    B:智能弱电  
    C:非智能强电  
    D：非智能弱电  
    答案:B
12. （容易）手机发送的短信被让人截获，破坏了信息的（)  
    A：机密性  
    B:完整性  
    C：可用性  
    D:真实性  
    答案:A
13. （容易）光盘被划伤无法读取数据，破坏了载体的（)  
    A：机密性  
    B:完整性  
    C：可用性  
    D：真实性

答案:C

1. （中等）网络不良与垃圾信息举报受理中心的热线电话是？（）
2. 12301
3. 12315
4. 12321
5. 12110

答案:C

1. (容易）根据《中华人民共和国保守国家秘密法》规定，国家秘密包括三个级别,他们是：(）
2. 一般秘密、秘密、绝密
3. 秘密、机密、绝密
4. 秘密、机密、高级机密
5. 机密、高级机密、绝密

答案：B

1. （中等）根据《计算机软件保护条例》，法人或者其他组织的软件著作权，保护期为（）年。

A. 100年 B。 50年 C。 30年 D。 10年

答案:B

1. (中等）账户为用户或计算机提供安全凭证,以便用户和计算机能够登录到网络，并拥有响应访问域资源的权利和权限。下列关于账户设置安全，说法错误的是：
2. 为常用文档添加everyone用户
3. 禁用guest账户
4. 限制用户数量
5. 删除未用用户

答案：A

1. （中等）以下关于数字签名，说法正确的是：
2. 数字签名能保证机密性
3. 可以随意复制数字签名
4. 签名可以被提取出来重复使用,但附加在别的消息后面,验证签名会失败
5. 修改的数字签名可以被识别

答案：D

1. （中等)用ipconfig命令查看计算机当前的网络配置信息等，如需释放计算机当前获得的IP地址，则需要使用的命令是：
2. ipconfig
3. ipconfig/all
4. inconfig/renew
5. ipconfig/release

答案：D

1. （中等）设置复杂的口令，并安全管理和使用口令，其最终目的是：
2. 攻击者不能非法获得口令
3. 规范用户操作行为
4. 增加攻击者破解口令的难度
5. 防止攻击者非法获得访问和操作权限

答案：D

1. （中等)信息安全应急响应,是指一个组织为了应对各种安全意外事件的发生所采取的防范措施,既包括预防性措施，也包括事件发生后的应对措施。应急响应方法和过程并不是唯一的，通常应急响应管理过程为:
2. 准备、检测、遏制、根除、恢复和跟踪总结
3. 准备、检测、遏制、根除、跟踪总结和恢复
4. 准备、检测、遏制、跟踪总结、恢复和根除
5. 准备、检测、遏制、恢复、跟踪总结和根除

答案：A

1. (中等）以下操作系统补丁的说法，错误的是:
2. 按照其影响的大小可分为“高危漏洞”的补丁，软件安全更新的补丁，可选的高危漏洞补丁,其他功能更新补丁,无效补丁
3. 给操作系统打补丁，不是打得越多越安全
4. 补丁安装可能失败
5. 补丁程序向下兼容,比如能安装在Windows操作系统的补丁一定可以安装在Windows XP系统上

答案：D

1. （中等）数据被破坏的原因不包括哪个方面()。
2. 计算机正常关机
3. 自然灾害
4. 系统管理员或维护人员误操作
5. 病毒感染或“黑客”攻击

答案:A

1. (中等）信息安全管理中最关键也是最薄弱的一环是:
2. 技术
3. 人
4. 策略
5. 管理制度

答案：B

（案例一）228-231。小王毕业后进入A公司，现在需要协助领导完成一项关于网络安全方面的项目的研究,在研究过程中遇到如下问题，请选择正确答案进行解答：

（1）（中等）计算机网络是地理上分散的多台\_\_\_\_\_\_遵循约定的通信协议，通过软硬件互联的系统。

A。计算机

B.主从计算机

C。自主计算机

D.数字设备

答案:C

（2）（中等)大部分网络接口有一个硬件地址,如以太网的硬件地址是一个\_\_\_\_\_\_\_位的十六进制数。

A.32

B。48

C。24

D.64

答案：B

（3）（中等)拒绝服务攻击具有极大的危害,其后果一般是：

A.大量木马在网络中传播

B。被攻击目标无法正常服务甚至瘫痪

C。能远程控制目标主机

D。黑客进入被攻击目标进行破坏

答案:B

（4）（中等)WWW(World Wide Web）是由许多互相链接的超文本组成的系统，通过互联网进行访问.WWW服务对应的网络端口号是：

A。22

B。21

C.79

D。80

答案：D

（案例2）232-233小王是A单位信息安全部门的员工，现在需要为单位的电子邮件系统进行相关的加密保护工作,遇到如下问题，请选择正确答案进行解答：

（1）(中等）电子邮件系统中使用加密算法若按照密钥的类型划分可分为\_\_\_\_\_\_\_\_两种.

A。公开密钥加密算法和对称密钥加密算法

B。公开密钥加密算法和算法分组密码

C.序列密码和分组密码

D.序列密码和公开密钥加密算法

答案：A

（2）（中等）以下不属于电子邮件安全威胁的是：

A。点击未知电子邮件中的附件

B。电子邮件群发

C。使用公共wifi连接无线网络收发邮件

D.SWTP的安全漏洞

答案：B

1. (简单）关闭WIFI的自动连接功能可以防范\_\_\_\_\_\_\_\_。

A、 所有恶意攻击

B、 假冒热点攻击

C、 恶意代码

D、 拒绝服务攻击

答案：B

1. （简单）关于如何防范摆渡攻击以下哪种说法正确？

A、安装杀毒软件

B、安装防火墙

C、禁止在两个信息系统之间交叉使用U盘

D、加密

答案：C

1. （中等）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

答案:B

1. （中等）黑客hacker源于20世纪60年代末期的\_\_\_\_\_\_\_\_计算机科学中心。

A、哈佛大学

B、麻省理工学院

C、剑桥大学

D、清华大学

答案：B

1. （简单)以下\_\_\_\_\_\_\_\_可能携带病毒或木马.

A．二维码

B．IP地址

C．微信用户名

D．微信群

答案：A

1. （中等)造成广泛影响的1988年Morris蠕虫事件，是\_\_\_\_\_\_\_\_作为其入侵的最初突破点.

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

答案：C

1. （容易）谁破解了英格玛机?

A、牛顿

B、图灵

C、比尔盖茨

D、赫敏

答案：B

1. （中等)计算机网络中防火墙，在内网和外网之间构建一道保护屏障.以下关于一般防火墙说法错误的是：

A.过滤进、出网络的数据

B。管理进、出网络的访问行为

C.能有效记录因特网上的活动

D.对网络攻击检测和告警

答案:C

1. （难）VPN的加密手段为：

A。具有加密功能的防火墙

B。具有加密功能的路由器

C。VPN内的各台主机对各自的信息进行相应的加密

D。单独的加密设备

答案:C

1. (简单）“熊猫烧香”的作者是？

A、波格契夫

B、朱利安。阿桑奇

C、格蕾丝.赫帕

D、李俊

答案：D

1. （简单）病毒和逻辑炸弹相比，特点是？

A、破坏性

B、传染性

C、隐蔽性

D、攻击性

答案：B

1. (中等）网站的安全协议是https时,该网站浏览时会进行\_\_\_\_\_\_\_\_处理。

A、 口令验证

B、 增加访问标记

C、 身份验证

D、 加密

答案:D

二、多选题

1. （容易）习近平在中央网络安全和信息化领导小组第一次会议上旗帜鲜明的提出了\_\_\_\_\_\_。
2. 没有网络安全就没有现代化
3. 没有信息化就没有国家安全
4. 没有网络安全就没有国家安全
5. 没有信息化就没有现代化

答案：CD

1. （中等）2016年4月19日，习主席在网络安全和信息化工作座谈会上的讲话提到核心技术从3个方面把握。以下哪些是习主席提到的核心技术.( ）
2. 基础技术、通用技术
3. 非对称技术、“杀手锏”技术
4. 前沿技术、颠覆性技术
5. 云计算、大数据技术

答案：ABC

1. (中等)第二届互联网大会于2015年12月16日在浙江乌镇开幕，习近平总书记出席大会开幕式并发表讲话，介绍我国互联网发展情况，并就推进全球互联网治理体系变革提出应坚持哪几项原则？（ ）。
2. 尊重网络主权
3. 维护和平安全
4. 促进开放合作
5. 构建良好秩序

答案（ABCD）

1. （中等）常用的保护计算机系统的方法有：
2. 禁用不必要的服务
3. 安装补丁程序
4. 安装安全防护产品
5. 及时备份数据

答案：ABCD

1. （容易）现在的智能设备能直接收集到身体相应信息，比如我们佩戴的手环收集个人健康数据。以下哪些行为可能造成个人信息泄露？( ）
2. 将手环外借他人
3. 接入陌生网络
4. 手环电量低
5. 分享跑步时的路径信息

答案：ABD

1. （容易）越来越多的人习惯于用手机里的支付宝、微信等付账，因为很方便，但这也对个人财产的安全产生了威胁。以下哪些选项可以有效保护我们的个人财产?（）
2. 使用手机里的支付宝、微信付款输入密码时避免别人看到.
3. 支付宝、微信支付密码不设置常用密码
4. 支付宝、微信不设置自动登录.
5. 不在陌生网络中使用.

答案：ABCD

1. (容易）下列哪些选项可以有效保护我们上传到云平台的数据安全?( ）
2. 上传到云平台中的数据设置密码
3. 定期整理清除上传到云平台的数据
4. 在网吧等不确定网络连接安全性的地点使用云平台
5. 使用免费或者公共场合WIFI上传数据到云平台

答案：AB

1. （容易）2014年7月,国内安全团队研究了特斯拉 Model S型汽车，发现利用汽车软件里的某个漏洞，可以远程控制车辆，实现开锁、鸣笛、闪灯，可以在汽车行进的过程中远程开启天窗。这个事例告诉我们接入到网络中的设备都存在被黑客攻击的可能性，以下哪些措施可以有效避免接入网络的硬件设备免受网络攻击？（)
2. 硬件设备不接入到陌生的网络
3. 对自身网络设置密码验证
4. 硬件设备中安装安全防护软件
5. 及时清洁网络设备

答案：ABC

1. （困难）公开密钥基础设施(PKl)由以下哪几部分组成：（ )。
2. 认证中心;注册中心
3. 质检中心
4. 咨询服务
5. 证书持有者；用户；证书库

答案：AD

1. （容易）现在网络购物越来越多，以下哪些措施可以防范网络购物的风险
2. 核实网站资质及网站联系方式的真伪
3. 尽量到知名、权威的网上商城购物
4. 注意保护个人隐私
5. 不要轻信网上低价推销广告

答案：ABCD

1. （容易）在日常生活中，以下哪些选项容易造成我们的敏感信息被非法窃取？
2. 随意丢弃快递单或包裹
3. 在网上注册网站会员后详细填写真实姓名、电话、身份证号、住址等信息
4. 电脑不设置锁屏密码
5. 定期更新各类平台的密码，密码中涵盖数字、大小写字母和特殊符号

答案：ABC

1. （中等）以下哪些选项是关于浏览网页时存在的安全风险：()
2. 网络钓鱼
3. 隐私跟踪
4. 数据劫持
5. 网页挂马

答案：ABCD

1. （容易）网购已经在我们的生活中无处不在，下列哪些行为有诈骗嫌疑？（)
2. 拍下商品,付款成功后,告诉其在20天后才能到货
3. 买家拍货之后不付款要求卖家发货，卖家不发货就以投诉差评威胁新手卖家
4. 有自称为“淘宝客服"的人索要账户密码
5. 卖家推荐买家使用支付宝担保交易，保证交易中的安全性。

答案：ABC

1. （容易）我们在日常生活中网上支付时，应该采取哪些安全防范措施？（）
2. 保护好自身信息、财产安全，不要相信任何套取账号、USBkey和密码的行为
3. 网购时到正规、知名的网上商店进行网上支付，交易时确认地址栏内网址是否正确
4. 从银行官方网站下载安装网上银行、手机银行、安全控件和客户端软件；开通短信口令时,务必确认接收短信手机号为本人手机号
5. 避免在公共场所或者他人计算机上登录和使用网上银行，退出网上银行时一定要将USBkey拔出

答案：ABCD

1. （容易）某网站的用户数据库泄露，影响数据总共数亿条，泄露信息包括用户名、MD5密码、密码提示问题/答案（hash)、注册IP、生日等。该网站邮箱绑定的其他账户也受到波及，如iPhone用户的Apple ID等.发生此类问题我们应该进行下列哪种措施，避免受到更大损失（）？
2. 立即登录该网站更改密码
3. 投诉该网站
4. 更改与该网站相关的一系列账号密码
5. 不再使用该网站的邮箱

答案:AC

1. （容易)以下防范智能手机信息泄露的措施有哪几个( ）
2. 禁用 Wi-Fi 自动连接到网络功能，使用公共 Wi—Fi 有可能被盗用资料
3. 下载软件或游戏时，仔细审核该软件,防止将木马带到手机中
4. 经常为手机做数据同步备份
5. 勿见二维码就扫.

答案：ABD

1. （容易)以下哪些属于数据线连接到电脑上的安全风险？( ）
2. 不法分子可能在电脑上看到手机当中的短信内容；
3. 木马或病毒可在手机与电脑中相互感染；
4. 不法分子可通过远控电脑来操作、读取手机敏感信息;
5. 损坏手机使用寿命。

答案：（ABC)

1. (困难）请分析哪些是病毒、木马，在电子邮件的传播方式？( ）
2. 邮件主题及内容伪造成各式各样（好友的回复邮件、管理员的提醒、热点事件等)
3. 病毒副本存在邮件附件中,伪装成各种格式的文件引诱用户点击执行,如jpg、doc、zip、rar等，但有些时候实际上是exe文件
4. 将木马代码通过邮件的正文发送过去
5. 将病毒源文件直接发送给用户。

答案：（AB）

1. （中等 ） 为了防治垃圾邮件，常用的方法有：（ )。
2. 避免随意泄露邮件地址.
3. 定期对邮件进行备份。
4. 借助反垃圾邮件的专门软件。
5. 使用邮件管理、过滤功能.

答案 ： ACD

1. （容易)不要打开来历不明的网页、电子邮件链接或附件是因为\_\_\_\_\_\_。
2. 互联网上充斥着各种钓鱼网站、病毒、木马程序
3. 不明来历的网页、电子邮件链接、附件中，很可能隐藏着大量的病毒、木马
4. 可能含有的病毒、木马会自动进入电脑并隐藏在电脑中，会造成文件丢失损坏
5. 可能含有的病毒、木马会自动进入电脑并隐藏在电脑中，会导致系统瘫痪

答案：（ABCD)

1. (困难）网页挂马指的是，不法分子把一个木马程序上传到一个网站里面，然后用木马生成器生成一个网页木马，再加代码使得木马在打开网页时运行！完整过程如下：上传木马—-生成网页木马—-修改代码使用能自动运行-—加载到网站程序中.请分析一下受害者被网页挂马攻击的几个要素？（ )
2. 用户访问了存在挂马链接的网页(主动或被动);
3. 用户系统上存在漏洞、并且被攻击程序攻击成功；
4. 用户系统上的安全软件没有起作用；
5. 用户清理了电脑中的缓存网页文件

答案：（ABC)

1. （困难）请分析，以下哪些是高级持续性威胁(APT）的特点?( )
2. 此类威胁，攻击者通常长期潜伏
3. 有目的、有针对性全程人为参与的攻击
4. 一般都有特殊目的（盗号、骗钱财、窃取保密文档等）
5. 不易被发现

答案：（ABCD）

1. （中等）以下哪项属于防范假冒网站的措施（)
2. 直接输入所要登录网站的网址,不通过其他链接进入
3. 登录网站后留意核对所登录的网址与官方公布的网址是否相符
4. 登录官方发布的相关网站辨识真伪
5. 安装防范ARP攻击的软件

答案：ABC

1. （容易）关于网络安全技术学习相关方式，以下说法正确的是？( ）
2. 出于学习的角度，可以未经许可对某网站进行渗透测试
3. 可搭建虚拟仿真环境来学习一些入侵与防御的技术
4. 可以参加一些技术学习类比赛来锻炼自己的能力
5. 可以学习基础知识的同时，关注一些安全事件，分析问题原因

答案：BCD

1. （容易)以下哪些关于网络安全的认识是错误的?（ )
2. 电脑病毒防治主要靠软件查杀
3. 文件删除后信息就不会恢复
4. 网络共享文件是安全的
5. 防病毒软件要定期升级

答案:ABC

1. （容易)如何防范钓鱼网站？
2. 通过查询网站备案信息等方式核实网站资质的真伪
3. 安装安全防护软件
4. 警惕中奖、修改网银密码的通知邮件、短信,不轻意点击未经核实的陌  
   生链接
5. 不在多人共用的电脑上进行金融业务操作，如网吧等。

答案:(ABCD)

1. (容易）青少年安全使用网络的一些说法，哪些是正确的( ）?
2. 不要随意下载“破解版”、“绿色版”等软件，下载软件从正规的官方网站下载
3. 养成不打开陌生链接的习惯
4. 尽量不使用聊天工具
5. 玩游戏不使用外挂

答案：ABD

1. （中等）U盘病毒通过( ）,（ )，（ ）三个途径来实现对计算机及其系统和网络的攻击的。
2. 隐藏
3. 复制
4. 传播
5. 破解

答案：ABC

1. （中等）web安全是一个系统问题，包括服务器安全、web应用服务器安全、web应用程序安全、数据传输安全和应用客户端安全.然而,网络的规模和复杂性使web安全问题比通常意义上的Internet安全问题更为复杂。目前的web安全主要分为以下几个方面？（ ）
2. 保护服务器及其数据的安全;
3. 保护服务器和用户之间传递的信息的安全;
4. 保护web应用客户端及其环境安全；
5. 保证有足够的空间和内存，来确保用户的正常使用。

答案:ABC

1. （中等）拥有安全软件和安全的配置是安全网站必要的条件。web服务器负责提供内容，调用产生内容的应用程序应用服务器为应用程序提供多种服务，包括数据存储、目录服务、邮件、消息等.而网站的服务器配置中往往存在很多安全问题，攻击者可以使用扫描工具检测到这些问题并加以利用，导致后端系统的攻陷,包括数据库和企业内部网络。常见的安全问题有?( ）
2. 服务器软件未做安全补丁,有缺省密码的缺省的账号；
3. 服务器软件漏洞和错误配置允许列出目录和目录遍历攻击；
4. 不必要的缺省、备份或例子文件，包括 脚本、应用程序、配置文件和网页；
5. 不正确的文件和目录权限，不必要的服务被运行，包括内容管理和远程系统管理.

答案：ABCD

1. （容易）下列算法属于Hash算法的有( ）
2. RSA
3. DES
4. SHA1
5. MD5

答案：CD

1. （中等）由于TCP/IP协议的缺陷,可能导致的风险有(       )
2. 拒绝服务攻击
3. 顺序号预测攻击
4. 物理层攻击
5. TCP协议劫持入侵

答案:ABD

1. （困难)CA能提供以下哪种证书？ (   ）
2. 个人数字证书
3. SET服务器证书
4. SSL服务器证书
5. 安全电子邮件证书

答案:ACD

1. （容易)如何防范操作系统安全风险？( ）
2. 给所有用户设置严格的口令
3. 使用默认账户设置
4. 及时安装最新的安全补丁
5. 删除多余的系统组件

答案：ACD

1. (容易）网络安全攻击的主要表现方式有（  ）。
2. 中断
3. 截获
4. 篡改
5. 伪造

答案:ABCD

1. （困难）CSRF攻击防范的方法有？
2. 使用随机Token
3. 校验referer
4. 过滤文件类型
5. 限制请求频率

答案：AB

1. (中等)[黑盒测试法](”http://baike。baidu。com/view/229014.htm")注重于测试软件的功能需求，主要试图发现下列几类错误
2. 功能不正确或遗漏
3. 输入和输出错误
4. [初始化](”http：//baike。baidu。com/view/872.htm")和[终止](”http：//baike。baidu。com/view/189182.htm")错误
5. 性能错误

答案：ABCD

1. （容易）当短暂离开电脑时，为了确保个人信息安全,良好的使用习惯是对计算机进行锁屏,以下哪些是正确的计算机锁屏方法（ ）
2. 同时按住 windows logo键和s键
3. 同时按住windows logo键和L键
4. 单击windows左下的【开始】按钮,单击【注销】按钮,单击【切换用户】或【锁定】按钮.
5. 同时按住Ctrl键、Alt键和Del键,再点击【锁定计算机】按钮。

答案:BCD

1. (中等）以下哪些关于网络安全的认识是错误的？( ）
2. 电脑病毒的防治只能靠软件查杀；
3. 文件删除后信息就不会恢复;
4. 网络
5. 防病毒软件要定期升级。

答案:ABC（选项A是迷惑选项，病毒防治不仅靠被动查杀，主要靠良好习惯预防)

1. (容易)以下行为中，哪些存在网络安全风险？（ ）
2. 家用的无线路由器使用默认的用户名和密码
3. 在多个网站注册的帐号和密码都一样
4. 在网吧电脑上进行网银转账
5. 使用可以自动连接其它WIFI的手机APP软件

答案：ABCD

1. （容易)VPN在公共网上构建虚拟专用网，进行数据通信，可以保证通信过程中的身份认证、数据保密性和数据完整性。VPN采用的安全技术有:（ ）。
2. 安全隧道技术
3. 密钥管理技术
4. 数据包过滤技术
5. 用户身份认证技术

答案 : ABD

1. （中等）以下选项中，哪些是数字签名机制能够实现的目标:（ )。
2. 接受者能够核实发送者对信息的签名
3. 发送者不能抵赖对信息的签名
4. 接受者不能伪造对信息的签名
5. 发送者能够确定接受者收到信息

答案 : ABC

1. （容易）黑客常用的获取关键账户口令的方法有：（ ）。
2. 通过网络监听非法得到用户口令
3. 暴力破解
4. 社工撞库
5. SSL协议数据包分析

答案 ： ABC

1. （中等)下面是关于常用服务的默认端口的叙述，正确的是：（ ）.
2. FTP：文件传输协议，默认使用21端口。
3. Telnet: 远程登录使用25端口。
4. HTTP:超文本传送协议，默认打开80端口以提供服务。
5. SMTP：邮件传送协议,目标计算机开放的是23端口。

答案 : AC

1. （中等）在网络安全领域,社会工程学常被黑客用于
2. 踩点阶段的信息收集
3. 获得目标webshell
4. 组合密码的爆破
5. 定位目标真实信息

答案：ACD

1. （中等）以下哪些行为可能导致操作系统产生安全漏洞（ )
2. 使用破解版的编程工具
3. 不安全的编程习惯
4. 考虑不周的架构设计
5. 编程计算机未安装杀毒软件

答案:ABC

1. （中等）针对暴力破解攻击，网站后台常用的安全防护措施有哪些？
2. 拒绝多次错误登录请求
3. 修改默认的后台用户名
4. 检测cookie referer的值
5. 过滤特殊字符串

答案：AB

1. (容易）以下关于DDOS攻击的描述，下列哪些是正确的？( ）
2. 无需侵入受攻击的系统，即可导致系统瘫痪
3. 以窃取目标系统上的机密信息为目的
4. 导致目标系统无法处理正常用户的请求
5. 如果目标系统没有漏洞，远程攻击就不可能成功

答案：AC

1. (中等)以下哪些测试属于白盒测试？（）
2. 代码检查法
3. 静态结构分析法
4. 符号测试
5. [逻辑覆盖](”http://baike.baidu。com/view/178784.htm")法

答案：ABCD

1. (中等）网络钓鱼是指攻击者利用伪造的网站或欺骗性的电子邮件进行的网络诈骗活动.以下属于网络钓鱼常见攻击手段的是:
2. 伪造相似域名的网站
3. 显示虚假IP地址而非域名
4. 超链接欺骗
5. 弹出窗口欺骗

答案:ABCD

1. （中等）虚拟专用网络（Virtual Private Network，VPN）是在公用网络上建立专用网络的技术，整个VPN网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台。VPN的特点有：
2. 安全性高
3. 服务质量保证
4. 成本高
5. 可扩展性

答案：ABD

1. (中等）现行重要的信息安全法律法规包括以下：
2. 《计算机信息系统安全保护等级划分准则》
3. 《中华人民共和国电子签名法》
4. 《商用密码管理条例》
5. 《中华人民共和国保守国家秘密法》

答案：BCD

1. （中等)拒绝服务攻击是黑客常用的攻击手段之一，以下属于拒绝服务攻击防范措施的是：
2. 安装防火墙，禁止访问不该访问的服务端口，过滤不正常的畸形数据包
3. 安装先进杀毒软件,抵御攻击行为
4. 安装入侵检测系统，检测拒绝服务攻击行为
5. 安装安全评估系统，先于入侵者进行模拟攻击，以便及早发现问题并解决

答案：ACD

1. （中等）计算机病毒（Computer Virus，CV）是编制者在计算机程序中插入的，破坏计算机系统功能或者数据的代码，能影响计算机系统的使用,并且能够自我复制的一组指令或程序代码，计算机病毒对操作系统的危害主要表现在：
2. 破坏操作系统的处理器管理功能
3. 破坏操作系统的文件管理功能
4. 破坏操作系统的存储管理功能
5. 直接破坏计算机系统的硬件资源

答案:ABCD

1. （中等）访问控制矩阵(Access Control Matrix)是最初实现访问控制机制的概念模型，以二维矩阵规定主体和客体的访问权限。那么明确访问权限是相当重要的工作，在Windows系统对文件的访问权限一般包括：
2. 修改
3. 执行
4. 读取
5. 写入

答案：ABCD

# 2017全民网络安全知识竞赛试题及答案

一、单选题

　　1、网页恶意代码通常利用( C ）来实现植入并进行攻击。

　　A、 口令攻击

　　B、 U盘工具

　　C、 IE浏览器的漏洞

　　D、 拒绝服务攻击

　　2、要安全浏览网页，不应该（ A )。

　　A、 在他人计算机上使用“自动登录”和“记住密码"功能

　　B、 禁止使用Active（错）控件和Java 脚本

　　C、 定期清理浏览器Cookies

　　D、 定期清理浏览器缓存和上网历史记录

　　3、用户暂时离开时，锁定Windows系统以免其他人非法使用.锁定系统的快捷方式为同时按住（ ） 。

　　A、 WIN键和Z键

　　B、 F1键和L键

　　C、 WIN键和L键

　　D、 F1键和Z键

　　4、网站的安全协议是https时，该网站浏览时会进行( D )处理。

　　A、 口令验证B、 增加访问标记C、 身份验证D、 加密

　　5、为了规范互联网电子邮件服务，依法治理垃圾电子邮件问题，保障互联网电子邮件用户的合法权益,信息产业部于2006年2月20日颁布了，自2006年3月30日开始施行。 （ B ）

　　A、《互联网信息服务管理办法》 B、《互联网电子邮件服务管理办法》

　　C、《互联网电子公告服务管理规定》

　　6、为了防范垃圾电子邮件，互联网电子邮件服务提供者应当按照信息产业部制定的技术标准建设互联网电子邮件服务系统,电子邮件服务器( C ）匿名转发功能。

　　A、使用 B、开启 C、关闭

　　7、互联网电子邮件服务提供者对用户的( A )和互联网电子邮件地址负有保密的义务.

　　A、个人注册信息 B、收入信息 C、所在单位的信息

　　8、任何组织或个人不得利用互联网电子邮件从事传播淫秽色情信息、窃取他人信息或者等违法犯罪活动,否则构成犯罪的，依法追究刑事责任，尚不构成犯罪的，由公安机关等依照有关法律、行zd规的规定予以处罚；电信业务提供者从事上述活动的，并由电信管理机构依据( A ）有关行zd规处罚。

　　A、故意传播计算机病毒 B、发送商业广告 C、传播公益信息

　　9、为了鼓励用户对违规电子邮件发送行为进行举报，发动全社会的监督作用,信息产业部委托中国互联网协会设立了互联网电子邮件举报受理中心，其举报电话是010—12321，举报电子邮箱地址为（ A )。

　　A、abuse＠anti-spam、cn B、register@china—cic、org

　　C、member＠china—cic、org

　　10、为了依法加强对通信短信息服务和使用行为的监管，信息产业部和有关部门正在联合制定（ B ）。

　　A、《通信服务管理办法》 B、《通信短信息服务管理规定》

　　C、《短信息管理条例》

　　11、如果您发现自己被手机短信或互联网站上的信息诈骗后，应当及时向（ C ）报案，以查处诈骗者，挽回经济损失.

　　A、消费者协会 B、电信监管机构 C、公安机关

　　12、为了有效抵御网络黑客攻击，可以采用作为安全防御措施。 （ C )

　　A、绿色上网软件 B、杀病毒软件 C、防火墙

　　13、按照《互联网电子公告服务管理规定》，任何人不得在互联网上的电子布告牌(BBS)、电子白板、电子论坛、（ B ）、留言板等电子公告服务系统中发布淫秽、色情、赌博、暴力、恐怖等违法有害信息。

　　A、网站 B、网络聊天室 C、电子邮箱

　　14、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，这属于什么攻击类型？ (A)

　　A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

　　15、为了防御网络监听，最常用的方法是 （ B )

　　A、采用物理传输（非网络） B、信息加密 C、无线网 D、使用专线传输

　　16、向有限的空间输入超长的字符串是哪一种攻击手段?(A）

　　A、缓冲区溢出 B、网络监听 C、拒绝服务 D、IP欺骗

　　17、主要用于加密机制的协议是(D)

　　A、HTTP B、FTP C、TELNET D、SSL

　　18、用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码，这是属于何种攻击手段？ ( B ）

　　A、缓存溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDOS攻击

　　19、在以下认证方式中，最常用的认证方式是:(A)

　　A、基于账户名/口令认证 B、基于摘要算法认证

　　C、基于PKI认证 D、基于数据库认证

　　20、下列不属于系统安全的技术是（ B )

　　A、防火墙 ；B、加密狗 ;C、认证 ; D、防病毒

　　21、抵御电子邮箱入侵措施中，不正确的是（ D )

　　A、不用生日做密码 B、不要使用少于5位的密码 C、不要使用纯数字

　　D、自己做服务器

　　22、不属于常见的危险密码是（ D ）

　　A、跟用户名相同的密码 B、使用生日作为密码 C、只有4位数的密码

　　D、10位的综合型密码

　　23、不属于计算机病毒防治的策略的是（ D )

　　A、

　　B、

　　C、

　　D、 确认您手头常备一张真正“干净"的引导盘 及时、可靠升级反病毒产品 新购置的计算机软件也要进行病毒检测 整理磁盘

　　24、在每天下午5点使用计算机结束时断开终端的连接属于（ A )

　　A、外部终端的物理安全 B、通信线的物理安全 C、窃听数据 D、网络地址欺骗

　　25、当今IT 的发展与安全投入，安全意识和安全手段之间形成（ B ）

　　A、安全风险屏障 B、安全风险缺口

　　C、管理方式的变革 D、管理方式的缺口

　　26、我国的计算机年犯罪率的增长是( C )

　　A、10% B、160% C、60% D、300%

　　27、信息安全风险缺口是指( A ）

　　A、IT 的发展与安全投入，安全意识和安全手段的不平衡

　　B、信息化中，信息不足产生的漏洞

　　C、计算机网络运行，维护的漏洞

　　D、计算中心的火灾隐患

　　28、网络攻击与防御处于不对称状态是因为( C )

　　A、管理的脆弱性 B、应用的脆弱性

　　C、网络软硬件的复杂性 D、软件的脆弱性

　　29、网络攻击的种类（ A )

　　A、物理攻击，语法攻击，语义攻击 B、黑客攻击，病毒攻击

　　C、硬件攻击,软件攻击 D、物理攻击,黑客攻击,病毒攻击

　　30、语义攻击利用的是（ A ）

　　A、信息内容的含义 B、病毒对软件攻击

　　C、黑客对系统攻击 D、黑客和病毒的攻击

　　31、计算机网络最早出现在哪个年代? （ B )

　　A、20世纪50年代 B、20世纪60年代

　　C、20世纪80年代 D、20世纪90年代

　　32、最早研究计算机网络的目的是什么？( C ）

　　A、直接的个人通信； B、共享硬盘空间、打印机等设备;

　　C、共享计算资源; D、大量的数据交换.

　　33、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

　　34、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？（ C )

　　A、安装防火墙 B、安装入侵检测系统

　　C、给系统安装最新的补丁 D、安装防病毒软件

　　35、以网络为本的知识文明人们所关心的主要安全是（ C ）

　　A、人身安全 B、社会安全 C、信息安全

　　47、第一次出现”HACKER"这个词是在（ B ）

　　A、BELL实验室 B、麻省理工AI实验室 C、AT＆T实验室

　　36、可能给系统造成影响或者破坏的人包括( A ）

　　A、所有网络与信息系统使用者 B、只有黑客 C、只有管理员

　　37、黑客的主要攻击手段包括( A )

　　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

　　38、从统计的情况看，造成危害最大的黑客攻击是( C )

　　A、漏洞攻击 B、蠕虫攻击 C、病毒攻击

　　39、第一个计算机病毒出现在（ B ）

　　A、40年代 B、70 年代 C、90年代

　　40、口令攻击的主要目的是（ B )

　　A、获取口令破坏系统 B、获取口令进入系统 C、仅获取口令没有用途

　　41、通过口令使用习惯调查发现有大约\_B的人使用的口令长度低于5个字符的

　　A、50、5％ B、51、 5% C、52、5％

　　42、通常一个三个字符的口令破解需要( B )

　　A、18毫秒 B、18 秒 C、18分钟

　　43、邮件炸弹攻击主要是（ B )

　　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

　　44、逻辑炸弹通常是通过( B ）

　　A、必须远程控制启动执行,实施破坏

　　B、指定条件或外来触发启动执行，实施破坏

　　C、通过管理员控制启动执行，实施破坏

　　45、扫描工具( C ）

　　A、只能作为攻击工具 B、只能作为防范工具

　　C、既可作为攻击工具也可以作为防范工具

　　46、黑客造成的主要安全隐患包括（ A )

　　A、破坏系统、窃取信息及伪造信息

　　B、攻击系统、获取信息及假冒信息

　　C、进入系统、损毁信息及谣传信息

　　47、从统计的资料看，内部攻击是网络攻击的（ B )

　　A、次要攻击 B、最主要攻击 C、不是攻击源

　　48、一般性的计算机安全事故和计算机违法案件可由\_\_\_\_\_受理（ C )

　　A、案发地市级公安机关公共信息网络安全监察部门

　　B、案发地当地县级（区、市)公安机关治安部门。

　　C、案发地当地县级（区、市)公安机关公共信息网络安全监察部门

　　D、案发地当地公安派出所

　　49、计算机刑事案件可由\_\_\_\_\_受理（ A )

　　A、案发地市级公安机关公共信息网络安全监察部门

　　B、案发地市级公安机关治安部门

　　C、案发地当地县级（区、市)公安机关公共信息网络安全监察部门

　　D、案发地当地公安派出所

　　50、计算机信息系统发生安全事故和案件，应当\_\_\_\_\_\_在内报告当地公安机关公

　　共信息网络安全监察部门( D ）

　　A、8小时 B、48小时 C、36小时 D、24小时

　　51、对计算机安全事故的原因的认定或确定由\_\_\_\_\_作出( C ）

　　A、人民法院 B、公安机关 C、发案单位 D、以上都可以

　　52、对发生计算机安全事故和案件的计算机信息系统，如存在安全隐患的， B 应当要求限期整改.

　　A、人民法院 B、公安机关 C、发案单位的主管部门 D、以上都可以

　　53、传入我国的第一例计算机病毒是( B )

　　A、大麻病毒 B、小球病毒 C、1575病毒 D、米开朗基罗病毒

　　54、我国是在\_\_年出现第一例计算机病毒（ C ）

　　A、1980 B、1983 C、1988 D、1977

　　55、计算机病毒是（ A )

　　A、计算机程序 B、数据 C、临时文件 D、应用软件 56、1994年我国颁布的第一个与信息安全有关的法规是（ D )

　　A、国际互联网管理备案规定 B、计算机病毒防治管理办法

　　C、网吧管理规定 D、中华人民共和国计算机信息系统安全保护条例

　　57、网页病毒主要通过以下途径传播（ C )

　　A、邮件 B、文件交换 C、网络浏览 D、光盘

　　58、故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行， 后果严重的,将受到\_\_\_\_处罚（ A )

　　A、处五年以下有期徒刑或者拘役 B、拘留 C、罚款 D、警告

　　59、计算机病毒防治产品根据\_\_\_\_标准进行检验( A ）

　　A、计算机病毒防治产品评级准测 B、计算机病毒防治管理办法

　　C、基于DOS系统的安全评级准则 D、计算机病毒防治产品检验标准

　　60、《计算机病毒防治管理办法》是在哪一年颁布的（ C )

　　A、1994 B、1997 C、2000 D、1998

　　61、VPN是指( A )

　　A、虚拟的专用网络 B、虚拟的协议网络 C、虚拟的包过滤网络

　　62、目前的防火墙防范主要是（ B ）

　　A、主动防范 B、被动防范 C、不一定

　　63、IP地址欺骗通常是（ A )

　　A、黑客的攻击手段 B、防火墙的专门技术 C、IP 通讯的一种模式 黑客在攻击中进行端口扫描可以完成( D )。

　　A、 检测黑客自己计算机已开放哪些端口

　　B、口令破译

　　C、 获知目标主机开放了哪些端口服务

　　D、截获网络流量

　　64、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?(C）

　　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

　　65、木马程序一般是指潜藏在用户电脑中带有恶意性质的 ( A ),利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息.

　　A、远程控制软件 B、计算机操作系统 C、木头做的马

　　66、为了防止各种各样的病毒对计算机系统造成危害，可以在计算机上安装防病毒软件，并注意及时 （ B ），以保证能防止和查杀新近出现的病毒。

　　A、 分析 B、 升级 C、检查

　　67、局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样，则( C ）。

　　A、两台计算机都正常

　　B、两台计算机都无法通讯

　　C、一台正常通讯一台无法通讯

　　68、企业重要数据要及时进行( C )，以防出现以外情况导致数据丢失。 A、杀毒 B、加密 C、备份

　　69、窃听是一种( )攻击,攻击者( ）将自己的系统插入到发送站和接收站之间.截获是一种（ ）攻击，攻击者（ ）将自己的系统插入到发送站和接受站之间。（A)

　　A、 被动，无须，主动，必须

　　B、 主动,必须,被动,无须

　　C、 主动,无须,被动,必须

　　D、 被动,必须,主动,无须

　　70、可以被数据完整性机制防止的攻击方式是(D)。

　　A、 假冒源地址或用户的地址欺骗攻击

　　B、 抵赖做过信息的递交行为

　　C、 数据中途被攻击者窃听获取

　　D、 数据在途中被攻击者篡改或破坏

　　71、王某，未经著作权人许可，以私服营运方式,通过信息网络向公众传播他人网络游戏软件，获利14万余元,其行为均构成（ A )。

　　A、侵犯著作权罪 B、侵犯商业秘密罪

　　C、非法侵入计算机信息系统罪 D、非法经营罪

　　72、任何组织或者个人注册微博客账号，制作、复制、发布、传播信息内容的，应当使用（ A ）,不得以虚假、冒用的居民身份信息、企业注册信息、组织机构代码信息进行注册。网站开展微博客服务，应当保证前款规定的注册用户信息真实。

　　A真实身份信息 B正确的网站信息 C真实的ID D工商注册信息

　　73、2010年年底，熊某偶尔登录到一个境外的淫秽网站,发现该网站有大量的淫秽图片及视频可以观看，便在该网站上注册成为会员。之后，熊某渐渐沉迷于这些淫秽图片和视频,不能自拔。为获得更大的浏览权限，熊某便陆续发了17篇包含淫秽信息的帖子共被点击查看29410次，以不断提高自身的会员等级.熊某的行为（ B )

　　A不构成犯罪 B构成传播淫秽物品罪

　　C构成非法经营罪 D构成制作、复制、出版、贩卖、传播淫秽物品牟利罪

　　74、文艺青年张小五写了一部反映社会现实的小说，发表后引起热烈反响，好评如潮。甲网站觉得有利可图，擅自将该小说发布在网络上,供网民在线阅读。该网站侵犯了张小五的哪种著作权?（ B )

　　A发表权 B信息网络传播权 C复制权 D发行权

　　75、著作权行政管理部门对侵犯互联网信息服务活动中的信息网络传播权的行为实施行政处罚，适用( A )

　　A《著作权行政处罚实施办法》

　　B《互联网著作权行政保护办法》

　　C民法中关于知识产权的相关规定

　　D《商标法》

　　二、判断题

　　1、VPN的主要特点是通过加密使信息能安全的通过Internet传递.（对)

　　2、密码保管不善属于操作失误的安全隐患。(错)

　　3、漏洞是指任何可以造成破坏系统或信息的弱点。(对)

　　4、安全审计就是日志的记录。（错)

　　5、计算机病毒是计算机系统中自动产生的。（错）

　　6、对于一个计算机网络来说，依靠防火墙即可以达到对网络内部和外部的安全防护（错）

　　7、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。(错）

　　8、最小特权、纵深防御是网络安全原则之一。（对)

　　9、安全管理从范畴上讲，涉及物理安全策略、访问控制策略、信息加密策略和网络安全管理策略。（对）

　　10、用户的密码一般应设置为16位以上.(对）

　　11、开放性是UNIX系统的一大特点。（对)

　　12、防止主机丢失属于系统管理员的安全管理范畴。(错）

　　13、我们通常使用SMTP协议用来接收E-MAIL。（错）

　　14、在堡垒主机上建立内部DNS服务器以供外界访问，可以增强DNS服务器的安全性。（错）

　　15、为了防御网络监听，最常用的方法是采用物理传输。(错）

　　16、使用最新版本的网页浏览器软件可以防御黑客攻击。（对）

　　17、通过使用SOCKS5代理服务器可以隐藏QQ的真实IP.（对）

　　18、一但中了IE窗口炸弹马上按下主机面板上的Reset键,重起计算机.（错）

　　19、禁止使用活动脚本可以防范IE执行本地任意程序。(对）

　　20、只要是类型为TXT的文件都没有危险。（错)

　　21、不要打开附件为SHS格式的文件。(对）

　　22、发现木马，首先要在计算机的后台关掉其程序的运行。(对)

　　23、限制网络用户访问和调用cmd的权限可以防范Unicode漏洞。(对)

　　24、解决共享文件夹的安全隐患应该卸载Microsoft网络的文件和打印机共享.(对)

　　25、不要将密码写到纸上。(对）

　　26、屏幕保护的密码是需要分大小写的。（对）

　　27、计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒。（对）

　　28、木马不是病毒。（对)

　　29.复合型防火墙防火墙是内部网与外部网的隔离点,起着监视和隔绝应用层通信流的作用，同时也常结合过滤器的功能.(对）

　　30、非法访问一旦突破数据包过滤型防火墙，即可对主机上的软件和配置漏洞进行攻击。(错)

　　31、ATM 技术领先于TCP/IP技术，即将取代IP技术，实现语音、视频、数据传输网络的三网合一(错）

　　32、Internet设计之初，考虑了核战争的威胁，因此充分考虑到了网络安全问(错）

　　33、我的计算机在网络防火墙之内，所以其他用户不可能对我计算机造成威胁（错）

　　34、Internet没有一个集中的管理权威（对)

　　35、统计表明，网络安全威胁主要来自内部网络，而不是Internet(对)

　　36、只要设置了足够强壮的口令,黑客不可能侵入到计算机中（错)

　　37、路由器在转发IP分组时，一般不检查IP分组的源地址，因此可以伪造IP分组的源地址进行攻击，使得网络管理员无法追踪。(对）

　　38、发起大规模的DDoS攻击通常要控制大量的中间网络或系统(对)

　　39、路由协议如果没有认证功能，就可以伪造路由信息，导致路由表混乱，从而使网络瘫痪(对）

　　40、目前入侵检测系统可以及时的阻止黑客的攻击。(错）

　　41、TCSEC是美国的计算机安全评估机构和安全标准制定机构(对）

　　42、蠕虫、特洛伊木马和病毒其实是一回事(错)

　　43、只要选择一种最安全的操作系统，整个系统就可以保障安全(错）

　　44、在计算机系统安全中，人的作用相对于软件,硬件和网络而言,不是很重要(错)

　　45、在设计系统安全策略时要首先评估可能受到的安全威胁（对)

　　46、安装系统后应当根据厂商或安全咨询机构的建议对系统进行必要的安全配置(对)

　　47、系统安全的责任在于IT技术人员，最终用户不需要了解安全问题（错)

　　48。网络的发展促进了人们的交流,同时带来了相应的安全问题（错）

　　49.具有政治目的的黑客只对政府的网络与信息资源造成危害(错）

　　50、病毒攻击是危害最大、影响最广、发展最快的攻击技术（错）

　　51、黑色星期四"是因有人通过BELL实验室与Internet连接的有漏洞的机器上放置了一个蠕虫程序而引起网络灾难得名的（错）

　　52、邮件的附件如果是带有。exe、.com、.pif、.pl、。src和.vbs为后缀的文件，应确定其安全后再打开 （对）

　　53、在信息战中中立国的体现要比非信息战简单(错)

　　54、信息战的军事目标是指一个国家军队的网络系统、信息系统、数据资源（错)

　　55、计算机病毒是计算机系统中自动产生的(错）

　　56、小球病毒属于引导型病毒（对)

　　57、公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作（对）

　　58、计算机病毒防治产品实行销售许可证制度（对）

　　59、计算机病毒防治产品分为三级，其中三级品为最高级(错）

　　60，删除不必要的网络共享可以提高防范病毒的能力（对）

　　61、带VPN的防火墙一旦设置了VPN 功能，则所有通过防火墙的数据包都将

　　62、通过VPN通道进行通讯(错)

　　63、VPN的所采取的两项关键技术是认证与加密（对）

　　64、要保证一个公司总部与其分支机构的网络通讯安全只有通过VPN来实现(错)

　　65、网络安全工程实施的关键是质量，而质量的关键是服务的长期保障能力（对）

　　66、网络安全服务的开展与网络安全防范是一对矛盾(对)

　　67、网络安全边界防范的不完备性仅指防外不防内（错）

　　68、使用最新版本的网页浏览器软件可以防御黑客攻击.(错)

　　69、不要将密码写到纸上.（对)

　　70、计算机数据恢复在实际生活当中可以百分百恢复。(错)

　　71、违反国家法律、法规的行为，危及计算机信息系统安全的事件，称为计算机案件.(对)

　　72、计算机犯罪是行为人以计算机为工具或以计算机资产为犯罪对象实施的，依照我国刑法应受处罚的，具有社会危害性的行为。（对）

　　73、 计算机信息系统的安全威胁同时来自内、外两个方面。 (对)

　　74、外单位人员如可以随意接入奇瑞公司内网。（错）

　　75、格式化过后的计算机，原来的数据就找不回来了（错）

　　问答题：

　　1、今年我国首届国家网络安全宣传周的主题是什么？

　　答案:共建网络安全,共享网络文明

　　2、罗定职业技术学院的官方网址是什么？

　　答案:www。niubb。net和 www。niubb。net

　　3、罗定职业技术学院政务和公益机构域名是什么?

　　答案：罗定职业技术学院.公益

　　4、首次使用CRP数字校园、校园一卡通等信息系统时,为了保存自已的信息和财产安全应当怎么做?

　　答案：进入信息系统修改密码，并将其设置为一个复杂的密码.

　　5、计算机网络最突出的优点是什么?

　　答案：共享资源

　　6、信息安全有哪些常见的威胁？

　　答案：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。

　　7、解决互联网安全问题的根本条件是什么?

　　答案：提高整个社会网民的互联网道德本质。

　　8、什么是钓鱼网站？

　　答案：“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的URL地址以及页面内容,或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的HTML代码，以此来骗取用户银行或信用卡账号、密码等私人资料。

　　9、什么是网络安全?

　　答案：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露,系统可以连续可靠正常地运行，网络服务不被中断。

　　10、什么是木马？

　　答案：木马是一种带有恶意性质的远程控制软件。木马一般分为客户端

　　（client)和服务器端（server）。客户端就是本地使用的各种命令的控制台，服务器端则是要给别人运行，只有运行过服务器端的计算机才能够完全受控。木马不会像病毒那样去感染文件.

　　11、什么是后门?

　　答案:后门是指一种绕过安全性控制而获取对程序或系统访问权的方法。

　　12、防范网络黑客防措施有哪些?

　　答案：①选用安全的口令②口令不得以明文方式存放在系统中③建立帐号锁定机制④实施存取控制⑤确保数据的安全

　　13、网络病毒的来源有哪些？

　　答案:邮件附件、E—mail 、Web服务器、文件共享。

　　14、局域网内部若出现ARP攻击,会出现哪两种两句现象？

　　答案：1.不断弹出“本机的(错)(错)(错）段地址与网络中的（错)(错)（错)段地址冲突”的对话框.2.计算机不能正常上网,出现网络中断的症状。

　　15、控制USB接口使用的目的？

　　答案：1、网络的安全 2、信息的保密

　　16、什么是IP欺骗?

　　答案：攻击者可通过伪装成被信任源IP地址等方式来骗取目标主机的信任。

　　17、电子邮件存在哪些安全性问题？

　　1、垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷,影响网络传输速度，占用邮件服务器的空间。2、诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜，发信人能迅速让大量受害者上当。3、邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为，信箱不能承受时就会崩溃。4、通过电子邮件传播的病毒，大多数采用附件的形式夹带在电子邮件中.当收信人打开附件后，病毒会查询他的通讯簿,给其上所有或部分人发信,并将自身放入附件中，以此方式继续传播扩散。

　　18、什么是网络蠕虫?

　　答案:网络蠕虫是一种智能化、自动化，综合网络攻击、密码学和计算机病毒技术，无须计算机使用者干预即可运行的攻击程序或代码。

　　19、网络蠕虫有什么特征？

　　答案:具有病毒的特征，传染性，隐蔽性，破坏性;不利用文件寄生，可以主动传播，并且通过网络可快速传播，容易造成网络拥塞；具有智能化、自动化和高技术化；

　　20、防火墙的基本功能有哪些?

　　答案:1过滤进出网络的数据;2管理进出网络的访问行为;3封堵某些禁止的业务；4记录进出网络的信息和活动；5对网络的攻击进行将侧和报警。

　　21、因特网电子商务系统必须保证网络安全的四大要素是什么？

　　答案：1传输数据的保密性;2数据的完整性;3交易各方身份的真实性; 4交易的不可抵赖性；

　　21、对蠕虫病毒和一般病毒进行比较有什么区别？

　　答案：存在形式：普通病毒寄存在文件上，蠕虫病毒寄存在独立程序上； 传染机制：普通病毒在宿主程序上运行,蠕虫病毒会主动攻击；

　　传染目标：普通病毒传染本地文件，蠕虫病毒传染整个网络的计算机。

　　22、黑客攻击的动机都有哪些？

　　答案：1.好奇心理2.挑战性.3.报复心理4，经济利益5，政治目的，6.情报获取

　　23、什么是密码破解，有哪些方法?

　　答案：通过猜解或者直接破坏原密码的密码验证机制来达到和密码分析一样的最终效果，或者是密码对应的权限.

　　一般的密码破解大致分为以下几类。

　　1)使用软件无限次尝试密码。2）绕过密码验证机制。3)如果密码加密，使用替代密码代替原密码

　　24、后门程序与计算机病毒的差别是什么？

　　答案：后门程序又称特洛伊木马,其用途是潜伏在用户的计算机中，进行信息搜集或便于黑客进入。后门程序和计算机病毒最大的差别，在于后门程序不一定有自我复制的动作，即后门程序不一定会“感染"其他计算机。

　　25、黑客技术发展趋势是什么?

　　答案：(1）网络攻击的自动化程度和攻击速度不断提高（2)攻击工具越来越复杂(3）黑客利用安全漏洞的速度越来越快(4)防火墙被攻击者渗透的情况越来越多(5)安全威胁的不对称性在增加(6)攻击网络基础设施产生的破坏效果越来越大

　　26、什么是漏洞？

　　答案:漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

　　27、网络面临的安全威胁主要有哪些方面？

　　网络面临的安全威胁可分为两种：一是对网络数据的威胁；二是对网络设备的威胁。概括起来主要威胁包括以下几个方面：1）由自然力造成的非人为的数据丢失、设备失效、线路阻断。2）人为但属于操作人员无意的失误造成的数据丢失。3）来自外部和内部人员的恶意攻击和入侵。

　　28、IPv6先对IPv4有哪些优势?

　　IPv6优势：首先，IPv6解决了IP地址数量短缺的问题；其次，IPv6对IPv4协议中诸多不完善之处进行了较大的改进，在网络保密性、完整性方面作了更好的改进,在可控性和抗否认性方面有了新的保证。

　　29、计算机病毒传染的一般过程是什么??

　　答案：1)判断传染目标（文件）是否符合感染条件(是否已经被感染)

　　2）若目标符合感染条件,则将病毒链接到传染目标的特点位置，并存入磁盘。

　　3）继续监视系统的运行，寻找新的传染目标

　　30、网络安全服务包括哪些?

　　答案:1、对等实体认证服务2、数据源点认证服务3数据保密服务4数据完整性服务5访问控制服务6可用性