

7 网络信息类安全题

7.1 判断题

以下说法是否正确？正确的打“√”，错误的打“×”

1、信息安全的层次化特点决定了应用系统的安全不仅取决于应用层安全机制，同样依赖于底层的物理、网络 and 系统等层面的安全状况。（ ）

2、企业事业单位及其工作人员协助机关、单位逃避、妨碍保密检查或者泄露保密检查或者泄露国家秘密案件查处的，由有关主管部门依法予以处罚。（ ）

3、对本机关产生的仍在保密期限内的国家秘密文件、资料，如果认为符合提前解密条件的，可以不需要办理解密手续，直接删去密级标志后就予以公开。（ ）

4、连接互联网的计算机必须与处理涉密信息的计算机严格区分，做到专机专用，不得既用于上互联网又用于处理国家秘密信息。（ ）

5、涉密人员可以私自到境外机构、组织或者外商独资企业工作，为其提供服务。（ ）

6、涉密人员被解聘或者本人提出辞职的，应先调离涉密岗位，在本单位履行脱密期后再行办理解聘、辞职或调离手续。（ ）

7、国家秘密载体以及属于国家秘密的设备、产品的明显部位应当标注国家秘密标志。（ ）

8、复制国家秘密载体或者摘录、引用、汇编属于国家秘密的内容，应当按照规定报批，不得擅自改变原件的密级、保密期限和知悉范围，复制件应当加盖复制机关、单位戳记，并视同原件进行管理。（ ）

9、机关单位制作本单位保密承诺书，可以结合实际补充相关内容，也可以适当删减规定的基本内容。（ ）

10、中央国家机关、省级机关及其授权的机关、单位可能确定绝密级、机密级和秘密级国家秘密；设区的市、自治州一级的机关及其授权的机关、单位可以确定绝密级和秘密级国家秘密。（ ）

11、保守国家秘密、维护国家安全和利益是每个公民应尽的宪法义务。（ ）

12、机关、单位确因工作需要，自行销毁少量国家秘密载体的，应当使用符合国家保密标准的销毁设备和方法。（ ）

13、按照“谁定密、谁审批、谁负责”的原则，机关、单位负责人对本机关、本单位的定密工作负责。（ ）

14、机关、单位执行中央下发的机密级文件，在执行过程中产生的文件资料，应当

确定为秘密级国家秘密。()

15、没有定密权的机关、单位，可以向有相应定密权限的上一级机关或有关行政主管部门提出定密授权的申请。()

16、机关、单位对是否属于国家秘密或者属于何种密级不明确或者有争议的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门确定。()

17、机关、单位工作人员可以在涉密计算机和非涉密计算机之间交叉使用优盘等移动存储介质。()

18、军事方面的国家秘密及其密级的具体范围，由国家保密局规定。()

19、涉密人员的合法权益受法律保护。()

20、签订保密承诺书之前，应当组织对承诺人进行保密教育和培训。承诺人要了解有关保密要求，熟悉保密承诺内容，掌握相关保密知识和技能。()

21、机关、单位发现秘密已经泄露或者可能泄露的，应当立即采取补救措施，并在 12 小时内向同级保密行政管理部门和上级保密行政管理部门报告。()

22、在保密审查过程中，机关、单位认为被审查信息涉及商业秘密、个人隐私，公开后可能损害第三方合法权益的，应当口头征求第三方的意见。()

23、上网信息的保密管理坚持“谁上网谁负责”的原则。()

24、保密管理的目的是通知采取积极防范、突出重点、依法管理的方针，达到既确保国家保密安全、又便利信息资源合理利用。()

25、制定保密事项范围，既要国家安全和利益出发，把确属国家秘密的事项纳入保密范围；又要避免“宽一些保险”、“高一些有利”的片面认识，严格控制保密范围，实事求是地确定密级。()

26、保密违法行为与侵犯国家秘密犯罪行为之间的区别查处对象不同、法律后果不同、查处主体不同。()

27、要充分发挥党校、行政学院、干部学院在领导干部保密教育中的主阵地、主渠道作用，利用党委（党组）理论中心组学习、保密法制讲座和培训、保密知识考试考核等形式开展保密教育。()

28、发生泄密事件的机关、单位，只要及时采取补救措施，没有造成严重后果，可以自行处理，不向有关保密工作部门和上级机关报告。()

29、工作人员可以通过普通邮政、快递等渠道传递国家秘密载体。()

30、不得将退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途。()

31、国家秘密的密级分为绝密、机密、秘密三级。()

32、对严重违反保密承诺，泄露国家秘密的，应当依法依规给予处分；构成犯罪的，依法追究刑事责任。()

33、禁止在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传

递国家秘密。()

34、不得在未采取防护措施的情况下将互联网及其他公共信息网络上的数据复制到涉密计算机及网络。()

35、手机只要在不通话的情况下，可以带入重要涉密场所。()

36、公安、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。()

37、依照有关规定，标有“内部资料”的信息，不得公开或暂缓公开。()

38、国家对在保守、保护国家秘密以及改进保密技术、措施等方面成绩显著的单位或者个人给予奖励。()

39、根据《国家秘密载体销毁管理规定》，国家秘密载体除正在使用或者按照有关规定留存、存档外，应当及时予以销毁。()

40、各单位要坚持上网信息保密审查审批制度，按照“谁主管谁负责，谁使用谁负责”的原则，严格把好上网信息保密关。()

41、在中华人民共和国境内依法成立 2 年以上的法人，无违法犯罪记录的企业事业单位可以从事涉密业务。()

42、脆弱性分析技术，也被通俗地称为漏洞扫描技术。该技术是检测远程或本地系统安全脆弱性的一种安全技术。()

43、主机和系统是信息系统威胁的主要目标之一。()

44、网络和信息系统的关节岗位人选不得出现在其他关键岗位兼职的情况。()

45、安全是相对的，永远没有一劳永逸的安全防护措施。()

46、蹭网指攻击者使用自己计算机中的无线网卡连接他人的无线路由器上网，而不是通过正规的 ISP 提供的线路上网。()

47、计算机网络所面临的威胁主要有对网络中信息的威胁和对网络设备的威胁两种。()

48、用户在处理废弃硬盘时，只要将电脑硬盘内的数据格式化就可以了，数据就不可能被恢复了。()

49、网络操作系统是为计算机网络配置的操作系统，它使网络中每台计算机能互相通信和共享资源。()

50、按照云计算的定义可分为广义云计算和狭义云计算。()

51、在任何情况下，涉密计算机及涉密网络都不能与任何公共信息网络连接。()

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。()

53、浏览器缓存和上网历史记录能完整还原用户访问互联网的详细信息，并反映用户的使用习惯、隐私等。因此应当定期清理这些信息以避免他人获得并造成隐私泄密。()

- 54、机密性、完整性和可用性是评价信息资产的三个安全属性。()
- 55、信息安全应急响应通常是指一个组织机构为了应对各种信息安全意外事件的发生所采取的措施,其目的是避免、降低危害和损失,以及从危害中恢复。()
- 56、互联网上网服务营业场所经营单位对上网消费者的登记内容和上网记录备份。在保存期内对不需要的内容可以由经营单位修改或者删除。()
- 57、对网络的绝对信任和完全坦诚是最大的错误。()
- 58、在网络系统安全中,人的作用相对于软件、硬件和网络而言,不是很重要的。()
- 59、黑客的主要攻击手段包括社会工程攻击、蛮力攻击和技术攻击。()
- 60、APT 攻击是一种“恶意商业间谍威胁”的攻击。()

7.2 单项选择题

将正确选项的编号填写在括号中。

- 1、在以下人为的恶意攻击行为中,属于主动攻击的是()
- A. 数据篡改及破坏 B. 数据窃听 C. 数据流分析 D. 非法访问
- 2、数据完整性指的是()
- A. 保护网络中各系统之间交换的数据,防止因数据被截获而造成泄密
- B. 提供连接实体身份的鉴别
- C. 防止非法实体对用户的主动攻击,保证数据接受方收到的信息与发送方发送的信息完全一致
- D. 确保数据数据是由合法实体发出的
- 3、网络攻击的发展趋势是()
- A、黑客技术与网络病毒日益融合 B、攻击工具日益先进
- C、病毒攻击 D、黑客攻击
- 4、拒绝服务攻击是()
- A、用超出被攻击目标处理能力的海量数据包消耗可用系统、带宽资源等方法的攻击
- B、全称是 Distributed Denial Of Service
- C、拒绝来自一个服务器所发送回应请求的指令
- D、入侵控制一个服务器后远程关机
- 5、HTTP 默认端口号为()
- A、21 B、80 C、8080 D、23
- 6、网络监听是()
- A、远程观察一个用户的计算机 B、监视网络的状态、传输的数据流

- C、监视 PC 系统的运行情况 D、监视一个网站的发展方向
- 7、在公开密钥体制中，加密密钥即（ ）
- A、解密密钥 B、私密密钥 C、私有密钥 D、公开密钥
- 8、计算机网络的安全是指（ ）
- A、网络中设备设置环境的安全 B、网络中信息的安全
- C、网络中使用者的安全 D、网络中财产的安全
- 9、打电话请求密码属于_____攻击方式（ ）
- A、木马 B、社会工程学 C、电话系统漏洞 D、拒绝服务
- 10、_____是网络通信中标志通信各方身份信息的一系列数据，提供一种在 Internet 上验证身份的方式（ ）
- A、数字认证 B、数字证书 C、电子证书 D、电子认证
- 11、数字签名功能不包括（ ）
- A、防止发送方的抵赖行为 B、接收方身份确认
- C、发送方身份确认 D、保证数据的完整性
- 12、目前无线局域网主要以_____作传输媒介（ ）
- A、短波 B、微波 C、激光 D、红外线
- 13、防火墙能够（ ）
- A、防范通过它的恶意连接 B、防范恶意的知情者
- C、防备新的网络安全问题 D、完全防止传送已被病毒感染的软件和文件
- 14、计算机病毒的传播方式有（ ）
- A、通过共享资源传播 B、通过网页恶意脚本传播
- C、通过网络文件传输传播 D、通过电子邮件传播
- E、以上都是
- 15、以下属于木马入侵的常见方法的是（ ）
- A、捆绑欺骗 B、邮件冒名欺骗 C、危险下载
- D、打开邮件的附件 E、以上都是
- 16、关于网络防火墙的作用，不正确的是（ ）
- A、防止内部信息外泄 B、防止系统感染病毒与非法访问
- C、防止黑客访问 D、建立内部信息和功能与外部信息和功能之间的屏障
- 17、任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息（ ）
- A、煽动抗拒、破坏宪法和法律、行政法规实施的；煽动颠覆国家政权，推翻社会主义制度的
- B、煽动分裂国家、破坏国家统一的；煽动民族仇恨、民族歧视，破坏民族团结的
- C、捏造或者歪曲事实、散布谣言，扰乱社会秩序的；公然侮辱他人或者捏造事

实诽谤他人的

D. 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；其他违反宪法和法律、行政法规的

E. 以上都是

18、下列行为中，是《计算机信息网络国际联网安全保护管理办法》所不允许利用国际联网进行的活动（ ）

A. 危害国家安全的行为

B. 泄露国家秘密的行为

C. 侵犯国家的、社会的、集体的利益的行为

D. 侵犯公民的合法权益的行为

E. 以上都是

19、互联网上网服务营业场所经营单位的禁止行为包括（ ）

A. 禁止利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播国家法律、法规所禁止的有害信息的行为；禁止利用互联网上网服务营业场所侵犯用户的通信自由、通信秘密等涉及个人隐私的行为

B. 禁止擅自停止实施安全技术措施的行为；禁止在互联网上网服务营业场所从事破坏网络安全的行为

C. 禁止在互联网上网服务营业场所内使用盗版产品等侵犯知识产权的行为；禁止利用互联网上网服务营业场所进行赌博和变相赌博行为

D. 禁止接纳未成年人进入互联网上网服务营业场所的行为

E. 以上都是

20、《互联网上网服务营业场所管理条例》规定，互联网上网服务营业场所经营单位应当依法履行消防安全职责，并遵守_____规定（ ）

A. 禁止明火照明和吸烟并悬挂禁止吸烟标志

B. 禁止带入和存放易燃、易爆物品

C. 不得安装固定的封闭门窗栅栏

D. 营业期间禁止封堵或者锁闭门窗、安全疏散通道和安全出口

E. 以上都是

21、机关、团体、企业、事业单位应当履行下列_____消防安全职责（ ）

A. 制定消防安全制度、消防安全操作规程

B. 实行防火安全责任制，确定本单位和所属各部门、岗位的消防安全责任人

C. 按照国家有关规定配置消防设施和器材、设置消防安全标志，并定期组织检验、维修，确保消防设施和器材完好、有效

D. 保障疏散通道、安全出口畅通，并设置符合国家规定的消防安全疏散标志

E. 以上都是

22、互联网上网服务营业场所经营单位和上网消费者不得进行下列危害信息网络安全的活动（ ）

- A. 非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序
- B. 故意制作或者传播计算机病毒以及其他破坏性程序
- C. 行政法规禁止的其他行为
- D. 法律禁止的其他行为
- E. 以上都是

23、互联网上网服务营业场所经营单位和上网消费者不得利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用含有下列内容的信息()

- A. 反对宪法确定的基本原则的；危害国家统一、主权和领土完整的；泄露国家秘密，危害国家安全或者损害国家荣誉和利益的
- B. 煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的
- C. 破坏国家宗教政策，宣扬邪教、迷信的；散布谣言，扰乱社会秩序，破坏社会稳定的；宣传淫秽、赌博、暴力或者教唆犯罪的
- D. 侮辱或者诽谤他人，侵害他人合法权益的；含有法律、行政法规禁止的其他内容的
- E. 以上都是

24、互联网上网服务营业场所的安全管理制度，应该包括哪些基本制度()

- A. 审核登记制度
- B. 场内巡查与情况报告制度
- C. 上网登记制度
- D. 信息安全培训制度
- E. 以上都是

25、互联网上网服务营业场所经营单位承担的责任应该包括()

- A. 维护场所安全
- B. 维护国家安全
- C. 维护社会秩序
- D. 提高自身素质、加强行业自律、宣讲文明上网
- E. 以上都是

26、信息安全的基本属性是()

- A. 机密性
- B. 可用性
- C. 完整性
- D. 以上都是

27、“会话侦听和劫持技术”是属于_____的技术()

- 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

28、对攻击可能性的分析在很大程度上带有()

- A. 客观性
- B. 主观性
- C. 盲目性
- D. 以上都是

29、从安全属性对各种网络攻击进行分类，阻断攻击是针对_____的攻击()

- A. 机密性
- B. 可用性
- C. 完整性
- D. 真实性

30、从安全属性对各种网络攻击进行分类，截获攻击是针对_____的攻击()

- A. 机密性
- B. 可用性
- C. 完整性
- D. 真实性

31、拒绝服务攻击的后果是()

- A. 信息不可用
- B. 应用程序不可用
- C. 系统宕机

- D. 阻止通信 E. 以上都是
- 32、机密性服务提供信息的保密，机密性服务包括（ ）
- A. 文件机密性 B. 信息传输机密性
- C. 通信流的机密性 D. 以上都是
- 33、最新的研究和统计表明，安全攻击主要来自（ ）
- A. 接入网 B. 企业内部网 C. 公用 IP 网 D. 个人网
- 34、攻击者用传输数据来冲击网络接口，使服务器过于繁忙以至于不能应答请求的攻击方式是（ ）
- A. 拒绝服务攻击 B. 地址欺骗攻击
- C. 会话劫持 D. 信号包探测程序攻击
- 35、攻击者截获并记录了从甲到乙的数据，然后又从早些时候所截获的数据中提取出信息重新发往乙称为（ ）
- A. 中间人攻击 B. 口令猜测器和字典攻击
- C. 强力攻击 D. 回放攻击
- 36、以下不属于代理服务技术优点的是（ ）
- A. 可以实现身份认证 B. 内部地址的屏蔽和转换功能
- C. 可以实现访问控制 D. 可以防范数据驱动侵袭
- 37、黑客利用 IP 地址进行攻击的方法有（ ）
- A. IP 欺骗 B. 解密 C. 窃取口令 D. 发送病毒
- 38、防止用户被冒名所欺骗的方法是（ ）
- A. 对信息源发方进行身份验证 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
- 39、屏蔽路由器型防火墙采用的技术是基于（ ）
- A. 数据包过滤技术 B. 应用网关技术
- C. 代理服务技术 D. 三种技术的结合
- 40、以下关于防火墙的设计原则说法正确的是（ ）
- A. 保持设计的简单性
- B. 不单单要提供防火墙的功能，还要尽量使用较大的组件
- C. 保留尽可能多的服务和守护进程，从而能提供更多的网络服务
- D. 一套防火墙就可以保护全部的网络
- 41、SSL 指的是（ ）
- A. 加密认证协议 B. 安全套接层协议
- C. 授权认证协议 D. 安全通道协议
- 42、CA 指的是（ ）
- A. 证书授权 B. 加密认证 C. 虚拟专用网 D. 安全套接层

- 43、在安全审计的风险评估阶段，通常是按什么顺序来进行的（ ）
- A. 侦查阶段、渗透阶段、控制阶段 B. 渗透阶段、侦查阶段、控制阶段
C. 控制阶段、侦查阶段、渗透阶段 D. 侦查阶段、控制阶段、渗透阶段
- 44、以下哪一项不属于入侵检测系统的功能（ ）
- A. 监视网络上的通信数据流 B. 捕捉可疑的网络活动
C. 提供安全审计报告 D. 过滤非法的数据包
- 45、入侵检测系统的第一步是（ ）
- A. 信号分析 B. 信息收集 C. 数据包过滤 D. 数据包检查
- 46、以下哪一项不是入侵检测系统利用的信息（ ）
- A. 系统和网络日志文件 B. 目录和文件中的不期望的改变
C. 数据包头信息 D. 程序执行中的不期望行为
- 47、入侵检测系统在进行信号分析时，一般通过三种常用的技术手段，以下哪一种不属于通常的三种技术手段（ ）
- A. 模式匹配 B. 统计分析 C. 完整性分析 D. 密文分析
- 48、以下哪一种方式是入侵检测系统所通常采用的（ ）
- A. 基于网络的入侵检测 B. 基于 IP 的入侵检测
C. 基于服务的入侵检测 D. 基于域名的入侵检测
- 49、以下哪一项属于基于主机的入侵检测方式的优势（ ）
- A. 监视整个网段的通信 B. 不要求在大量的主机上安装和管理软件
C. 适应交换和加密 D. 具有更好的实时性
- 50、以下关于计算机病毒的特征说法正确的是（ ）
- A. 计算机病毒只具有破坏性，没有其他特征
B. 计算机病毒具有破坏性，不具有传染性
C. 破坏性和传染性是计算机病毒的两大主要特征
D. 计算机病毒只具有传染性，不具有破坏性
- 51、以下关于宏病毒说法正确的是（ ）
- 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. 宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区
D. CIH 病毒属于宏病毒
- 52、以下哪一项不属于计算机病毒的防治策略（ ）
- A. 防毒能力 B. 查毒能力 C. 解毒能力 D. 禁毒能力
- 53、网络层安全性的优点是（ ）
- A. 保密性 B. 按照同样的加密密钥和访问控制策略来处理数据包
C. 提供基于进程对进程的安全服务 D. 透明性

- 54、加密技术不能实现（ ）
- A. 数据信息的完整性
 - B. 基于密码技术的身份认证
 - C. 机密文件加密
 - D. 基于 IP 头信息的包过滤
- 55、所谓加密是指将一个信息经过_____及加密函数转换，变成无意义的密文，而接受方则将此密文经过解密函数、_____还原成明文（ ）
- A. 加密密钥、解密密钥
 - B. 解密密钥、解密密钥
 - C. 加密密钥、加密密钥
 - D. 解密密钥、加密密钥
- 56、以下关于对称密钥加密说法正确的是（ ）
- 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
- 57、以下关于非对称密钥加密说法正确的是（ ）
- 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是相同的
 - D. 加密密钥和解密密钥没有任何关系
- 58、以下关于混合加密方式说法正确的是（ ）
- A. 采用公开密钥体制进行通信过程中的加解密处理
 - B. 采用公开密钥体制对对称密钥体制的密钥进行加密后的通信
 - C. 采用对称密钥体制对对称密钥体制的密钥进行加密后的通信
 - D. 采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密处理速度快的双重优点
- 59、以下关于数字签名说法正确的是（ ）
- A. 数字签名是在所传输的数据后附加上一段和传输数据毫无关系的数字信息
 - B. 数字签名能够解决数据的加密传输，即安全传输问题
 - C. 数字签名一般采用对称加密机制
 - D. 数字签名能够解决篡改、伪造等安全性问题
- 60、以下关于 CA 认证中心说法正确的是（ ）
- A. CA 认证是使用对称密钥机制的认证方法
 - B. CA 认证中心只负责签名，不负责证书的产生
 - C. CA 认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份
 - D. CA 认证中心不用保持中立，可以随便找一个用户来做为 CA 认证中心
- 61、在 OSI 七个层次的基础上，将安全体系划分为四个级别，以下那一个不属于四个级别（ ）

- A. 网络级安全 B. 系统级安全 C. 应用级安全 D. 链路级安全
- 62、关于 CA 和数字证书的关系，以下说法不正确的是（ ）
- A. 数字证书是保证双方之间的通讯安全的电子信任关系，他由 CA 签发
- B. 数字证书一般依靠 CA 中心的对称密钥机制来实现
- C. 在电子交易中，数字证书可以用于表明参与方的身份
- D. 数字证书能以一种不能被假冒的方式证明证书持有人身份
- 63、以下关于 VPN 说法正确的是（ ）
- A. VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路
- B. VPN 指的是用户通过公用网络建立的临时的、安全的连接
- C. VPN 不能做到信息认证和身份认证
- D. VPN 只能提供身份认证、不能提供加密数据的功能
- 64、计算机网络按威胁对象大体可分为两种：一是对网络中信息的威胁，二是（ ）
- A. 人为破坏 B. 对网络中设备的威胁
- C. 病毒威胁 D. 对网络人员的威胁
- 65、CA 认证中心的主要作用是（ ）
- A. 加密数据 B. 发放数字证书 C. 安全管理 D. 解密数据
- 66、数字证书上除了有签证机关、序列号、加密算法、生效日期等等外，还有（ ）
- A. 公钥 B. 私钥 C. 用户帐户
- 67、Telnet 服务自身的主要缺陷是（ ）
- A. 不用用户名和密码 B. 服务端口 23 不能被关闭
- C. 明文传输用户名和密码 D. 支持远程登录
- 68、防火墙中地址翻译的主要作用是（ ）
- A. 提供代理服务 B. 隐藏内部网络地址
- C. 进行入侵检测 D. 防止病毒入侵
- 69、防治要从防毒、查毒、_____三方面来进行（ ）
- A. 解毒 B. 隔离 C. 反击 D. 重起
- 70、木马病毒是（ ）
- A. 宏病毒 B. 引导型病毒 C. 蠕虫病毒 D. 基于服务/客户端病毒
- 71、IDS 规则包括网络误用和（ ）
- A. 网络异常 B. 系统误用 C. 系统异常 D. 操作异常
- 72、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（ ）
- A. 对称密钥加密 B. 非对称密钥加密
- 73、以下那些属于系统的物理故障（ ）
- A. 硬件故障与软件故障 B. 计算机病毒
- C. 人为的失误 D. 网络故障和设备环境故障

- 74、对称密钥密码体制的主要缺点是（ ）
- A. 加、解密速度慢 B. 密钥的分配和管理问题
- C. 应用局限性 D. 加密密钥与解密密钥不同
- 75、数字签名是用来作为（ ）
- A. 身份鉴别的方法 B. 加密数据的方法
- C. 传送数据的方法 D. 访问控制的方法
- 76、加密密钥的强度是（ ）
- A. 2^N B. 2^{N-1} C. $2N$ D. $2^N - 1$
- 77、在互联网上的计算机病毒呈现出的特点是（ ）
- A. 与因特网更加紧密地结合，利用一切可以利用的方式进行传播
- B. 所有的病毒都具有混合型特征，破坏性大大增强
- C. 因为其扩散极快，不再追求隐蔽性，而更加注重欺骗性
- D. 利用系统漏洞传播病毒 E:利用软件复制传播病毒
- E. 以上都是
- 78、信息安全中的木桶原理，是指（ ）
- A. 整体安全水平由安全级别最低的部分所决定
- B. 整体安全水平由安全级别最高的部分所决定
- C. 整体安全水平由各组成部分的安全级别平均值所决定
- D. 以上都不对
- 79、相对于现有杀毒软件在终端系统中提供保护不同，_____在内外网络边界处提供更加主动和积极的病毒保护（ ）
- A. 防火墙 B. 病毒网关 C. IPS D. IDS
- 80、国家秘密是_____，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项（ ）
- A. 关系企业安全和利益 B. 关系国家安全和利益
- C. 关系单位安全和利益 D. 关系公民个人安全和利益
- 81、机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益（ ）
- A. 遭受损害 B. 遭受一般损害
- C. 遭受严重的损害 D. 遭受特别严重的损害
- 82、涉密人员不得在手机中存储涉及国家秘密的信息，不得在手机通话中涉及国家秘密事项，不得（ ）
- A. 用手机发送涉及工作秘密的信息 B. 用手机发送涉及商业秘密的信息
- C. 用手机发送涉及国家秘密的信息 D. 用手机发送涉及个人隐私的信息
- 83、《中华人民共和国保守国家秘密法实施条例》，自_____起施行（ ）
- A. 2011 年 3 月 1 日 B. 2012 年 3 月 1 日

- C. 2013 年 3 月 1 日 D. 2014 年 3 月 1 日
- 84、涉密网络中介质交叉使用的风险是指（ ）
- A. 硬盘等磁介质存在数据丢失的可能
B. 移动存储介质易发生丢失，导致泄密
C. 在涉密计算机上使用非涉密移动存储介质或在非涉密计算机上使用涉密移动存储介质，导致涉密信息极易被窃取
D. 利用移动存储介质在不同涉密机上拷贝信息，易导致病毒木马传播
- 85、涉密人员分为____、重要涉密人员、一般涉密人员（ ）
- A. 非常重要 B. 十分重要 C. 特别重要 D. 核心
- 86、涉密载体是指经文字、数据符号、图形、声音为方式记载国家秘密信息的纸介质、光介质、____等各类物品（ ）
- A. U 盘 B. 移动硬盘 C. 电磁介质 D. 磁盘
- 87、国家秘密的本质属性是（ ）
- A. 依照法律程序确定 B. 关系国家安全和利益
C. 在一定时间内保密 D. 只限一定范围的人员知悉
- 88、秘密可分为（ ）
- A. 个人隐私 B. 国家秘密 C. 工作秘密 D. 商业秘密 E. 以上都是
- 89、恶意代码传播速度最快、最广的途径是（ ）
- A. 通过光盘复制来传播文件时 B. 安装系统软件时
C. 通过 U 盘复制来传播文件时 D. 通过网络来传播文件时
- 90、以下关于无线网络相对于有线网络的优势不正确的是（ ）
- A. 可扩展性好 B. 灵活度高 C. 维护费用低 D. 安全性更高
- 91、《保密法》的立法依据是（ ）
- A. 宪法 B. 刑法 C. 政府 D. 党和国家领导人的指示
- 92、为境外的机构，组织、人员窃取、刺探、收买、非法提供国家秘密或情报，对国家和人民危害特别严重，情节特别恶劣的，可以判处（ ）
- A. 死刑 B. 三年以上五年以下有期徒刑
C. 五年以上十年以下有期徒刑 D. 十年以上有期徒刑或者无期徒刑
- 93、《保密法》规定，一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守_____的义务（ ）
- A. 国家秘密 B. 党和国家工作秘密 C. 企业商业秘密 D. 政府信息
- 94、国家机关工作人员，未经批准，私自留存国家秘密文件，属于_____行为（ ）
- A. 违反保密规定 B. 非法持有国家秘密
C. 违反国家机关工作人员职业道德 D. 内部

- 95、销毁国家秘密文件，应当到（ ）
- A. 国有造纸厂 B. 保密工作部门指定的地点
- C. 废品收购站 D. 任意地
- 96、根据《印刷、复印等行业复制国家秘密载体暂行管理办法》的规定，私营企业、个体工商户、外商投资企业_____承担复制国家秘密载体的业务（ ）
- A. 可以 B. 不得 C. 经批准可以 D. 视情况
- 97、技术信息中的商业秘密包括（ ）
- A. 技术水平 B. 技术潜力 C. 新技术前景预测
- D. 替代技术的预测 E. 以上都是
- 98、国家秘密的保密期限，除另有规定外（ ）
- A. 绝密级不超过三十年 B. 机密级不超过二十年
- C. 秘密级不超过十年 D. 以上都是
- 99、我国信息安全等级保护的内容不包括包括（ ）
- A. 对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输和处理这些信息的信息系统分等级实行安全保护
- B. 对信息系统中使用的信息安全产品实行按等级管理
- C. 对信息安全从业人员实行按等级管理
- D. 对信息系统中发生的信息安全事件按照等级进行响应和处置
- E. 对信息安全违反行为实行按等级惩处
- 100、全国人民代表大会常务委员会《关于维护互联网安全的决定》规定，为了维护社会主义市场经济秩序和社会管理秩序，____行为，构成犯罪的，依照刑法有关规定追究刑事责任（ ）
- A. 利用互联网销售伪劣产品或者对商品、服务作虚假宣传
- B. 利用互联网侵犯他人知识产权
- C. 利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息
- D. 利用互联网损害他人商业信誉和商品声誉
- E. 在互联网上建立淫秽网站、网页，提供淫秽站点链接服务，或者传播淫秽书刊、影片、音像、图片
- F. 以上都是
- 101、在安全评估过程中，安全威胁的来源包括（ ）
- A. 外部黑客 B. 内部人员 C. 信息技术本身
- D. 物理环境 E. 自然界 F. 以上都是
- 102、涉密安全管理不包括（ ）
- A. 涉密设备管理 B. 涉密信息管理 C. 涉密人员管理

- D. 涉密场所管理 E. 涉密媒体管理
- 103、____是建立有效的计算机病毒防御体系所需要的技术措施（ ）
- A. 杀毒软件 B. 补丁管理系统 C. 防火墙
- D. 网络入侵检测 E. 漏洞扫描 F. 以上都是
- 104、信息安全策略必须具备____属性（ ）
- A. 确定性 B. 全面性 C. 有效性 D. 以上都是
- 105、治安管理处罚法规定，____行为，处 5 日以下拘留；情节较重的，处 5 日以上 10 日以下拘留（ ）
- A. 违反国家规定，侵入计算机信息系统，造成危害的
- B. 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的
- C. 违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的
- D. 故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的
- E. 以上都是
- 106、____可能给网络和信息系带来风险，导致安全事件（ ）
- A. 计算机病毒 B. 网络入侵 C. 软硬件故障
- D. 人员误操作 E. 不可抗灾难事件 F. 以上都是
- 107、安全威胁是产生安全事件的（ ）
- A. 内因 B. 外因 C. 根本原因 D. 不相关因素
- 108、安全脆弱性是产生安全事件的（ ）
- A. 内因 B. 外因 C. 根本原因 D. 不相关因素
- 109、关于信息安全，下列说法中正确的是（ ）
- A. 信息安全等同于网络安全 B. 信息安全由技术措施实现
- C. 信息安全应当技术与管理并重 D. 管理措施在信息安全中不重要
- 110、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行（ ）
- A. 逻辑隔离 B. 物理隔离 C. 安装防火墙 D. VLAN 划分
- 111、目前，针对计算机信息系统及网络的恶意程序正逐年成倍增长，其中最为严重的是（ ）
- A. 木马病毒 B. 僵尸网络 C. 系统漏洞 D. 蠕虫病毒
- 112、以下____是开展信息系统安全等级保护的环节（ ）
- A. 自主定级 B. 备案 C. 监督检查 D. 等级测评 E. 以上都是

- 113、涉密信息工程监理工作应由_____的单位或组织自身力量承担（ ）
- A. 具有信息工程监理资质的单位 B. 具有涉密工程监理资质的单位
C. 涉密信息工程建设不需要监理 D. 保密行政管理部门
- 114、我国卫星导航系统的名字叫（ ）
- A. 天宫 B. 玉兔 C. 神州 D. 北斗
- 115、计算机病毒是（ ）
- A. 一种芯片 B. 具有远程控制计算机功能的一段程序
C. 一种生物病毒 D. 具有破坏计算机功能或毁坏数据的一组程序代码
- 116、Windows 操作系统中受限用户在默认的情况下可以访问和操作自己的文件，使用部分被允许的程序，一般不能对系统配置进行设置和安装程序，这种限制策略被称为（ ）
- A. 特权受限原则 B. 最大特权原则
C. 最小特权原则 D. 最高特权原则
- 117、计算机感染恶意代码的现象有（ ）
- A. 计算机运行速度明显变慢 B. 无法正常启动操作系统
C. 磁盘空间迅速减少 D. 正常的计算机经常无故突然死机
E. 以上都是
- 118、信息隐藏是（ ）
- A. 加密存储 B. 把秘密信息隐藏在大量信息中不让对手发觉的一种技术
C. 对信息加密 D. 以上答案都对
- 119、IP 地址是（ ）
- A. 计算机设备在网络上的地址 B. 计算机设备在网络上的物理地址
C. 计算机设备在网络上的共享地址 D. 以上答案都对
- 120、以下关于无线网络相对于有线网络的优势不正确的是（ ）
- A. 维护费用低 B. 可扩展性好 C. 灵活度高 D. 安全性更高
- 121、信息安全主要包括_____内容（ ）
- A. 运行安全和系统安全 B. 物理（实体）安全和通信保密
C. 计算机安全和数据（信息）安全 D. 系统可靠性和信息保障
E. 以上都是
- 122、安全收发电子邮件可以遵循的原则有（ ）
- A. 对于隐私或重要的文件可以加密之后再发送
B. 不要查看来源不明和内容不明的邮件，应直接删除
C. 区分工作邮箱和生活邮箱
D. 为邮箱的用户账号设置高强度的口令
E. 以上都是

- 123、为了保护个人隐私，应该（ ）
- A. 删除来历不明文件
 - B. 使用“文件粉碎”功能删除文件
 - C. 废弃硬盘要进行特殊处理
 - D. 给个人电脑设置安全密码，避免让不信任的人使用你的电脑
 - E. 以上都是
- 124、万维网是（ ）
- A. 由许多互相链接的超文本组成的信息系统
 - B. 互联网
 - C. 有许多计算机组成的网络
 - D. 以上答案都对
- 125、“核高基”是指（ ）
- A. 通用电子器件、核心芯片及基础软件产品
 - B. 核心电子器件、高端软件产品及基础通用芯片
 - C. 核心软件、高端电子器件及基础通用芯片
 - D. 核心电子器件、高端通用芯片及基础软件产品
- 126、容灾备份的类型有（ ）
- A. 数据级容灾备份
 - B. 应用级容灾备份
 - C. 业务级容灾备份
 - D. 存储介质容灾备份
 - E. 以上都是
- 127、属于办公自动化设备存在泄密隐患的是（ ）
- A. 维修过程泄密
 - B. 连接网络泄密
 - C. 安装窃密装置
 - D. 存储功能泄密
 - E. 以上都是
- 128、在 Windows 系统下，管理员账户拥有的权限包括（ ）
- A. 可以对系统配置进行更改
 - B. 可以创建、修改和删除用户账户
 - C. 可以安装程序并访问操作所有文件
 - D. 对系统具有最高的操作权限
 - E. 以上都是
- 129、黑客在攻击中进行端口扫描可以完成（ ）
- 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
- 130、以下属于电子商务功能的是（ ）
- A. 意见征询、交易管理
 - B. 广告宣传、咨询洽谈
 - C. 网上订购、网上支付
 - D. 电子账户、服务传递
 - E. 以上都是

7 网络信息类安全题参考答案

7.1 判断题

- | | | | | |
|----------|----------|----------|----------|----------|
| 1、(√) | 2、(√) | 3、(×) | 4、(√) | 5、(×) |
| 6、(√) | 7、(√) | 8、(√) | 9、(×) | 10、(×) |
| 11、(√) | 12、(√) | 13、(√) | 14、(×) | 15、(√) |
| 16、(√) | 17、(×) | 18、(×) | 19、(√) | 20、(√) |
| 21、(×) | 22、(×) | 23、(√) | 24、(√) | 25、(√) |
| 26、(×) | 27、(√) | 28、(×) | 29、(×) | 30、(√) |
| 31、(√) | 32、(√) | 33、(√) | 34、(√) | 35、(×) |
| 36、(√) | 37、(√) | 38、(√) | 39、(√) | 40、(√) |
| 41、(×) | 42、(√) | 43、(√) | 44、(√) | 45、(√) |
| 46、(√) | 47、(√) | 48、(×) | 49、(√) | 50、(√) |
| 51、(√) | 52、(√) | 53、(√) | 54、(√) | 55、(√) |
| 56、(×) | 57、(√) | 58、(×) | 59、(√) | 60、(√) |

7.2 单项选择题

- | | | | | |
|----------|----------|----------|----------|----------|
| 1、(A) | 2、(C) | 3、(B) | 4、(A) | 5、(B) |
| 6、(B) | 7、(D) | 8、(B) | 9、(B) | 10、(B) |
| 11、(B) | 12、(B) | 13、(A) | 14、(E) | 15、(E) |
| 16、(B) | 17、(E) | 18、(E) | 19、(E) | 20、(E) |
| 21、(E) | 22、(E) | 23、(E) | 24、(E) | 25、(E) |
| 26、(D) | 27、(B) | 28、(B) | 29、(B) | 30、(A) |
| 31、(E) | 32、(D) | 33、(B) | 34、(A) | 35、(D) |
| 36、(D) | 37、(A) | 38、(A) | 39、(B) | 40、(A) |
| 41、(B) | 42、(A) | 43、(A) | 44、(D) | 45、(B) |
| 46、(C) | 47、(D) | 48、(A) | 49、(C) | 50、(C) |
| 51、(B) | 52、(D) | 53、(A) | 54、(D) | 55、(A) |
| 56、(C) | 57、(B) | 58、(B) | 59、(D) | 60、(C) |
| 61、(D) | 62、(B) | 63、(B) | 64、(B) | 65、(B) |
| 66、(A) | 67、(C) | 68、(B) | 69、(A) | 70、(C) |
| 71、(A) | 72、(B) | 73、(A) | 74、(B) | 75、(A) |

76、(A)	77、(E)	78、(A)	79、(B)	80、(B)
81、(C)	82、(C)	83、(D)	84、(C)	85、(D)
86、(C)	87、(B)	88、(E)	89、(D)	90、(D)
91、(A)	92、(A)	93、(A)	94、(A)	95、(B)
96、(B)	97、(E)	98、(D)	99、(C)	100、(F)
101、(F)	102、(A)	103、(F)	104、(D)	105、(E)
106、(F)	107、(B)	108、(A)	109、(C)	110、(B)
111、(A)	112、(E)	113、(A)	114、(D)	115、(D)
116、(C)	117、(E)	118、(B)	119、(A)	120、(A)
121、(E)	122、(E)	123、(E)	124、(A)	125、(D)
126、(E)	127、(E)	128、(E)	129、(C)	130、(E)