**第十九套**

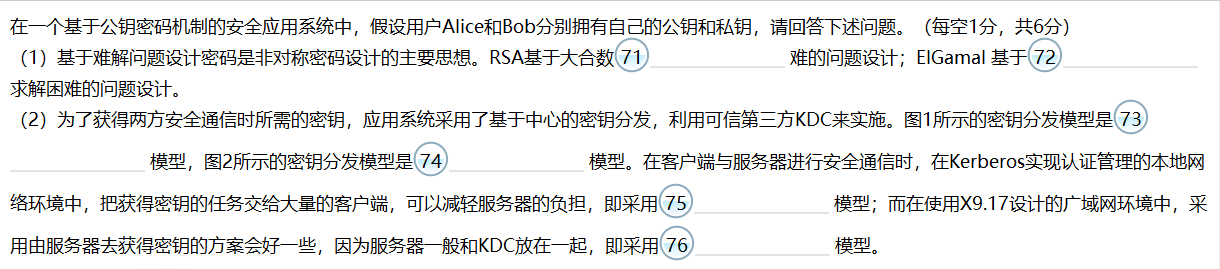
**一、选择题**

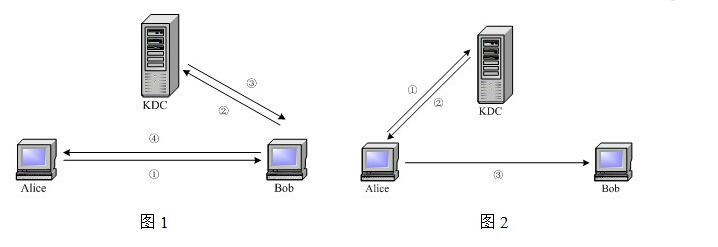
1. 属于信息安全问题产生的内在根源的是：互联网的开放性
2. 当代信息安全学起源与20世纪40年代的通讯保密，确保通信安全的核心技术是：密码技术
3. 信息系统所面临的安全风险包括：拒绝服务、假冒和欺诈、信息系统是复杂性
4. 美国第一个用于军事目的的计算机网络ARPnet出现在：20世纪60年代末
5. 下列有关对称密码的说法中，错误的是：IDEA属于序列密码
6. AES的整体结构采用的是：SP网络
7. 系统产生一个随机数r，并对其加密提供给用户；用户解密后计算r+1的加密密文，并回送给系统；最后，系统计算r+1的加密密文，并与用户返回的值进行比较，若两者相等，则系统认为用户的身份为真。该身份认证过程是：一次性口令认证
8. 下列有关智能卡存储用户私钥的说法中，错误的是：易于全面推广
9. 下列强制访问控制模型中，属于混合策略模型的是：Chinese Wall
10. 下列AAA协议中，最适合未来移动通信系统的是：Diameter
11. 不属于单点登录的优点的是：细致的分配用户权限，实现细粒度的访问控制
12. Alice为了发送保密信息给Bob，对消息进行加密所使用的密钥是：Bob公钥
13. MAC是指：强制访问控制
14. 下列关于保护环机制的说法中，错误的是：环号越低，赋予运行在该环内的进程权限就越小
15. UNIX最重要的网络服务进程是：inetd
16. 在Linux/UNIX系统中，显示上次登录过的用户的命令是：last
17. 在Windows系统中，第一个被启动的用户态进程是：smss
18. TPM是指：可信平台模块
19. CREATE USER命令中如果没有指定创建的新用户权限，默认该用户拥有的权限是：CONNECT权限
20. 如果所有外键参考现有的主键，则说明一个数据库具有：参照完整性
21. 能面向用户提供管理和网络服务的高层服务协议的TCP/IP层次是：应用层
22. TCP头部字段中有6个标志位，用于说明建立一个同步连接的标志位是：SYN
23. 将电子邮件发送到邮件服务器的简单邮件传输协议是：SMTP
24. 能对扫描行为进行有效拦截的技术是：防火墙
25. 防范应用软件漏洞攻击的措施，不包括：部署防火墙，防护应用软件漏洞攻击
26. 在SYN-Flood和ACK-Flood攻击中，数据包使用的都是：伪造的源IP
27. 最早突破软件防火墙的木马是：第四代木马
28. 在TCP三次握手中，第二次握手的数据包和SYN和ACK标志位分别为：1,1
29. 为了有效防范网站挂马，Web服务器的防护措施中不包括：Web服务器中使用最新的浏览器版本
30. 内存地址对象破坏性调用漏洞属于：UAF漏洞
31. 缓冲区溢出漏洞不包括：整数溢出漏洞
32. 为了劫持进程的控制权，漏洞利用的核心是利用程序漏洞去执行：shellcode
33. 将内存中敏感区域设置为不可执行(non-executable)状态，从而在溢出后即使跳转到恶意代码的地址，恶意代码也将无法运行，这种技术是：DEP
34. 常用的软件测试方法不包括：蓝盒测试
35. 软件的动态安全检测技术不包括：词法分析
36. Windows中的sigverif软件工具，可以检测：操作系统的文件是否被篡改
37. 缓解是一种控制方法，这种方法包括三类计划，其中不包括：事件生成计划（IGP）
38. 即使机构尽可能地控制各种漏洞，仍然存在一些风险未能够完全排除、缓解或规划，这成为：残留风险
39. 在我国计算机安全管理组织中，直接负责计算机应用和系统运行业务的单位是：系统经营单位
40. 应急计划过程开发的第一阶段是：业务影响分析
41. 访问控制通常分为三类，其中不包括：询问性访问控制
42. 事故响应的组成阶段中有：计划、检测、反应和：恢复
43. 信息安全管理中的风险计算公式为：风险=信息资产的价值（或影响）\*（ ）—已控制风险的比例 + 不确定因素：出现漏洞的可能性
44. 机关、单位应当根据工作需要，确定国家秘密的具体的保密期限、解密条件或者：解密时间
45. 符合计算机使用道德规范的是：不窃取别人的软件资源
46. 属于《计算机信息系统安全保护等级划分准则》中安全考核指标的是：数据完整性
47. 信息安全管理基本管理要求是从以下五个方面提出的：物理安全、网络安全、主机安全、应用安全、数据安全
48. 电子签名认证证书应当载明的内容是：电子认证服务提供者名称、证书持有人名称、证书序列号、证书有效期、证书持有人电子签名验证数据
49. 应当根据情况变化及时变更国家秘密的密级、知悉范围和：保密期限
50. ISO13335标准首次给出了关于IT安全的6方面含义：机密性、完整性、可用性、审计性、认证性和可靠性

二、填空题

1. 信息系统安全保障涵盖三个方面：生命周期、保障要素和 安全特征
2. P2DR安全模型的核心是：策略
3. 在20世纪90年代初提出了两种有效的对称密码的选择明文分析方法： 差分分析 和对称分析
4. DES算法的密钥长度是64位，但其中有 8或八 位被用做奇偶校验
5. 在密钥未过期之前，如果密钥丢失或其它原因，需要将它从运行使用的集合中除去，称为密钥的 撤销
6. AAA是指 认证 、授权和审计。
7. 如果采用ECC算法，选取的参数p的规模应大于 160 位
8. 进程就是为了实现 多任务 而提出的概念，其实它还有更细的管理单位——线程
9. 在Linux/UNIX中，最后一次登录信息可以用 lastlog 命令查看，它根据UID排序显示登录名、端口号和上次登录时间
10. 在Windows NT里，口令字密文保存在 SAM 文件里
11. 信任链把信任关系从 信任根 传递扩展到整个计算机系统
12. 代理服务器和包过滤技术、NAT技术不同之处在于，代理服务器在 应用 层对这些数据进行安全规则过滤
13. IPSec协议中，既支持加密功能也支持数据完整性鉴别功能的是 ESP或安全载荷封装 协议
14. 当一个函数被调用时，这个被调用函数的相关信息会保存在内存中的栈区，这块内存中连续的栈区域被称为 栈帧
15. 编制或者在计算机程序中插入的破坏计算机功能或毁坏数据，影响计算机使用并能够自我复制的一组计算机指令或者程序代码，被称为计算机 病毒
16. 微软的 软件安全开发生命周期 模型是微软公司总结的一套完整的软件安全开发流程，将安全融入到了软件开发的每个阶段
17. 国家信息安全漏洞共享平台是CNCERT联合国内重要信息系统单位建立的信息安全漏洞信息共享知识库，它的英文缩写是 CNVD
18. 0day漏洞是指还处于 未公开 状态的漏洞
19. 技术层面和管理层面的良好配合，是组织机构实现网络与信息安全系统的有效途径。在管理层面，通过构架 安全管理 体系来实现
20. 电子签名需要第 三 方认证，是由依法设立的电子认证服务提供方提供认证服务的
21. **综合题**

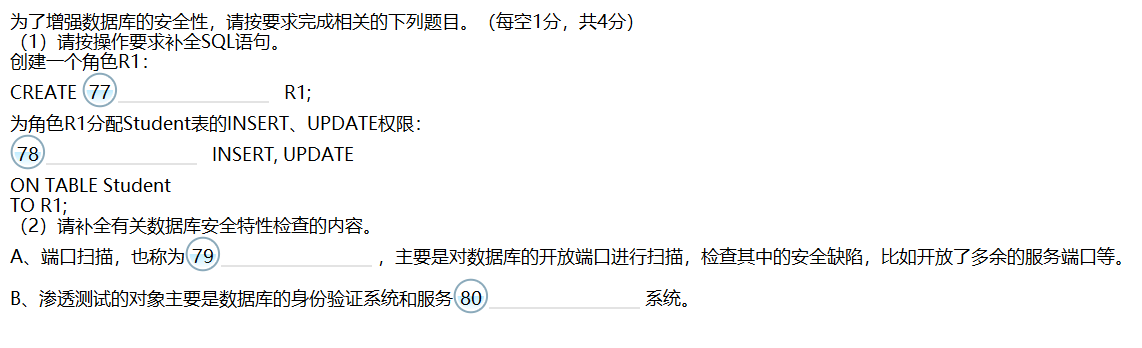
**71~76（每空1分，共6分）**





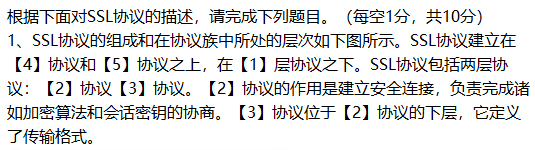
1. 因式分解
2. 离散对数
3. 推
4. 拉
5. 拉
6. 推

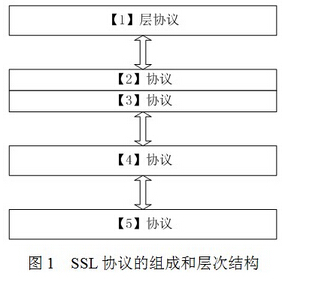
**77~80（每空1分，共4分）**



1. ROLE
2. GRANT
3. 服务发现
4. 监听

**81~90（每空1分，共10分）**





1. 【1】应用
2. 【2】SSL握手
3. 【3】SSL记录
4. 【4】TCP
5. 【5】IP



1. 数字证书
2. 数字证书
3. 数字证书
4. 公钥
5. 会话

**第二十套**

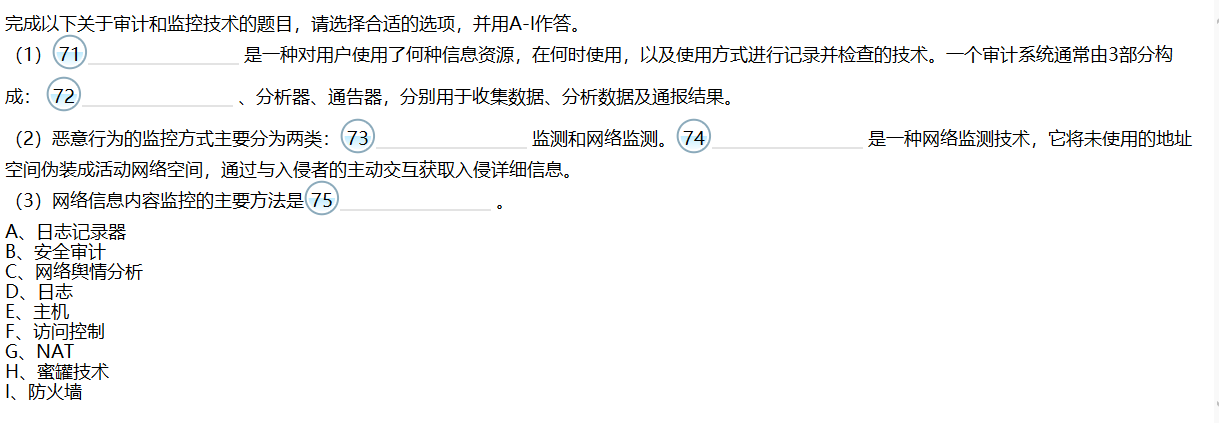
1. **选择题**
2. 不属于信息安全发展阶段的是：文件保密阶段
3. 1945年。提出“存储程序通用电子计算机方案”—EDVAC的是：冯诺依曼
4. 信息安全问题产生的根源中，内因是：信息系统的复杂性
5. P2DR安全模型的核心是：策略
6. 不属于分组密码算法的是：RSA
7. 密码设计应该遵循公开原则，即密码体制的安全应仅依赖于保护：密钥
8. 最容易防范的密码攻击方式是：唯密文攻击
9. 已知RSA算法的公钥为（n=55，e=7），则其私钥d为：23
10. 关于数字签名，说法正确的是：发信人用自己的私钥生成签名，收信人用发信人的公钥验证签名
11. 两个通信终端用户在一次交换数据会话时所采用的密钥称为：会话密钥
12. Biba模型是一种：强制访问控制模型
13. 在Needham-Schroeder认证协议中，KDC的含义是：密钥分发中心
14. 不是集中式AAA管理协议的是：SESAME
15. 数据库提供了多种强制数据完整性的约束机制，通过限制用户输入的值来加强域完整性的约束是：CHECK
16. 数据库事务处理的特性，不包括：机密性
17. 在Windows系统中，用来保存用户账号和口令的数据库为：SAM
18. TPM的含义是：可信平台模块
19. 在Windows的口令策略中，默认口令最长的存留期为：42天
20. 用于设置数据库审计功能的SQL命令为：AUDIT
21. 在Linux系统中，运行chrmod 666 myfile后，文件mufile的权限位变为：rw-rw-rw-
22. 利用TCP全连接发起的DDoS攻击是：Port Connection Flood
23. 网站挂马技术，不包括：诱骗下载
24. 和包过滤防火墙相比，状态检测防火墙的优点不包括：支持采用包过滤技术进行攻击的拦截
25. 支持多种不同类型的CA系统相互传递信任关系的信任模型是：桥CA信任模型
26. 证书的验证，不需要验证证书的：保密性
27. 对外公开发布用户证书的服务器是：CDS服务器
28. 提供票据许可服务的Kerberos服务器是：TGS
29. AH协议不提供：数据加密保护功能
30. IPSc协议是一组开放协议的总称，不包括：SSL
31. 软件源代码的静态安全检测技术，不包括：模糊测试
32. 代码混淆技术，不包括：同源性比对
33. 可实现对软件逆向分析的逆向分析辅助工具，不包括：Fortify
34. 对恶意程序的安全防护技术，不包括：防止因上传造成的恶意程序入侵
35. 恶意程序的破坏功能，不包括：操作系统补丁升级
36. 攻击者窃听了用户访问HTTP时的用户名和密码，或者是用户的会话，从而得到sessionID，进而冒充用户进行HTTP访问攻击是：遭破坏的认证和会话管理
37. 对Web服务器端的安全防护技术，不包括：及时针对Web浏览器进行版本更新，并及时打补丁
38. ISMS建立的基础是：安全风险评估
39. ISMS风险管理的方针手册，内容包括：以上全包括（信息安全方针的阐述、控制目标与控制方式描述、程序或其引用）
40. 信息安全管理审核准备工作，不包括：进行现场审核
41. 信息安全管理体系认证，基于：自愿的原则
42. 信息安全评估原则，不包括：强制
43. 信息安全风险控制中，缓解方法包括：以上全包括（事件响应计划、灾难恢复计划、业务持续性计划）
44. 系统安全维护活动，不包括：方便性维护
45. 与信息安全标准化有关的主要组织，不包括：WTO
46. 第一个信息安全评估的国标标准是1985年公布的TCSEC
47. 关于CC标准描述，属于其缺点的是：更适合于产品在市场推广前的认证，产品经过安全性评价和可用性鉴定之后投入实际使用，所以适合于指导开发的过程，而对已经使用的信息系统不太适用
48. 能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后能够恢复部分功能，属于信息系统安全保护等级对应的：第一级安全保护能力
49. 我国关于网络安全工作的基本大法是：《网络安全法》
50. 《电子签名法》第九条规定，信息被视为发件人发送的是：以上全包括（经发件人授权发送的、发件人的信息系统自动发送的、收件人按照发件人认可的方法对数据电文进行验证后结果相符的）
51. 我国信息安全测评中心的简称是：CNITSEC

**二、填空题**

1. 信息系统安全保障涵盖三个方面：生命周期、保障要素和 安全特征
2. P2DR安全模型的核心是： 策略
3. 1949年， 香农 在发表的《保密系统的通信理论》中，首先用信息理论的观点对信息保密问题作了全面的论述
4. IATF提出了3个主要核心要素：人员、 技术 和操作
5. 对称密码的主要设计思想是扩散和 混淆
6. 在访问控制技术中，AAA服务是指认证、授权和 审计 三种服务
7. AES算法的分组长度为 128 比特
8. ELGamal算法是基于 离散对数 问题的求解困难性设计的
9. DH 密钥交换协议是第一个实用的在非保护信道中创建共享密钥的密钥交换协议。
10. 现代CPU通常运行在两种模式下：用户模式和 内核 模式
11. 操作系统采用 保护环 机制来确保进程不会咋彼此之间或对系统的重要组件造成负面影响
12. 数据库执行3种类型的完整性服务：语义完整性、 参照 完整性和实体完整性
13. 在Linux中，用于设置用户创建文件的默认权限的命令为 umask
14. PKI系统的核心是 证书认证机构
15. SSL协议包括两层协议：记录协议和 握手 协议
16. 微软公司安全公告中软件漏洞危险等级最高的第一定义为 严重 级
17. 还处于未公开状态的漏洞被称为 0 day漏洞
18. 将可执行文件进行解压或者解密，从而使可执行文件还原为可执行的正常状态，这被称为软件 脱壳
19. 依据恶意程序的 特征码 进行查杀是最基本的一种杀毒技术
20. 信息安全风险评估的复杂程度取决于受保护的资产对安全的 敏感程度 和所面临风险的复杂程度

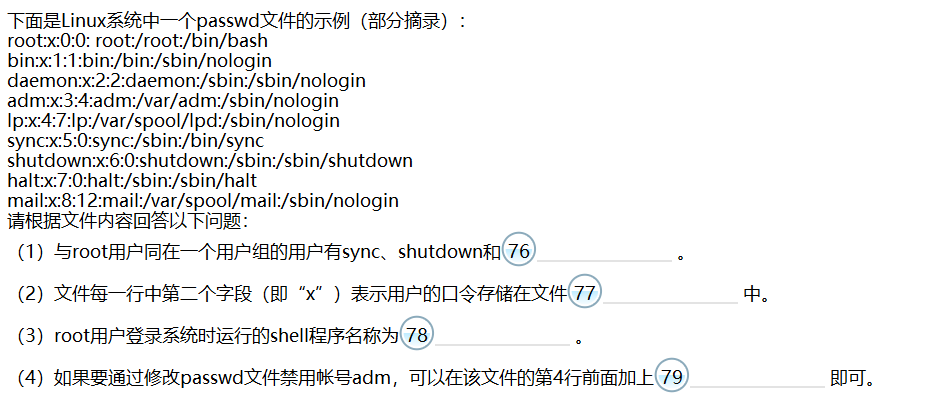
**三、综合题**

**71~75（每空1分，共5分）**



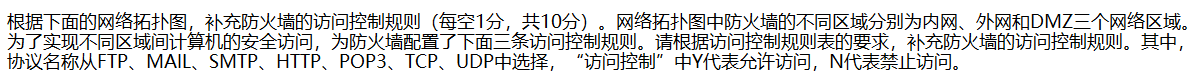
1. B
2. A
3. E
4. H
5. C

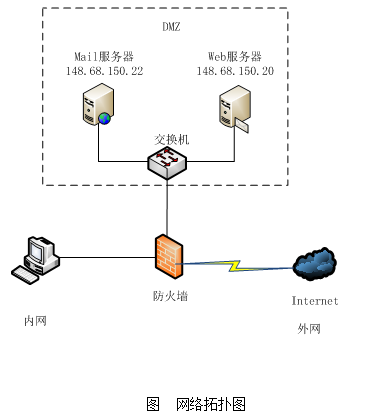
**76~79（每空1分，共5分）**



1. halt
2. shadow
3. bash
4. #

**80~89（每空1分，共10分）**





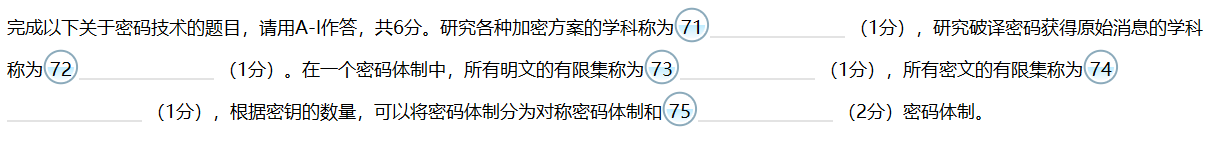


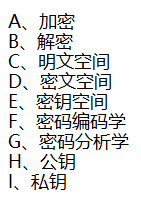
1. 内网
2. DMZ
3. 148.68.150.22
4. SMTP
5. POP3
6. 外网
7. DMZ
8. 148.68.150.20
9. HTTP
10. N

**第21套**

1. **选择题**
2. 有关信息和消息的关系，表述正确的是：消息是信息的外壳，信息则是消息的内核
3. 信息技术的消极影响，不包括：信息损失
4. 信息安全发展经历的三个阶段，不包括：密码应用阶段
5. 《中华人民共和国电子签名法》正式颁布于：2004年
6. 不属于分组密码算法的是：RSA
7. 密码设计应该遵循公开原则，即密码体制的安全依赖于：密钥的保密
8. 相对于公钥密码，对称密码的优点是：加解密速度快
9. 已知RSA算法的公钥为（n=33，e=7），则其私钥d为：3。
10. 密钥长度为128位时，AES算法的加密轮数（圈数）为：10
11. 在密码分析学中，攻击者仅仅知道加解密算法和要解密的密文，此时的攻击称为：唯密文攻击
12. BibA模型是一种：强制访问控制模型
13. Needham-Schroeder认证协议是一种：基于对称密码的认证协议
14. 在访问控制技术中，安全标签用于：强制访问控制模型
15. 数据库提供了多种强制数据完整性的约束机制，通过限制用户输入的值来加强域完整性的是：CHECK
16. 不属于数据库事务处理特性的是：机密性
17. 在Windows系统中用于保存用户账号和口令的数据库是：SAM
18. 可信计算中的术语TGG的含义是：可信计算组织
19. 在Windows的口令（密码）策略中，口令的默认最长存留期为：6周
20. 用于设置数据库审计功能的SQL语句是：AUDIT语句
21. Linux命令chrmod 666 myfil运行e后，文件mufile的权限位变为：rw-rw-rw-
22. 不属于应用层协议的是：OSPF
23. TCP中RST标志位的作用是：表示出现差错，必须释放TCP连接重新建立新连接
24. 下面有关UDP描述错误的是：在发送端和接收端之间的交互信息比TCP多
25. 端口扫描软件扫描出的网络端口为23，对应的网络服务是：TELNET
26. 不属于网络嗅探软件的是：Nessus
27. 伪装欺骗挂马不包括：虚拟机伪装
28. 不利用TCP协议的拒绝服务攻击是：DNS洪水攻击
29. CA系统的主要功能不包括：下载证书
30. MPLS VPN属于：介于二、三层之间的隧道协议
31. 软件漏洞产生的原因不包括：软件漏洞的隐蔽性使其不易被发现
32. 属于软件漏洞特点的是：软件漏洞影响广泛
33. 公开的漏洞库不包括：VuldA
34. C语言标准库中，与字符串操作有关，如果数组和指针没有进行正确的边界检查就可能造成缓冲区溢出危险的函数，不包括：for
35. 内存地址对象破坏性调用漏洞属于：UAF漏洞
36. 软件安全开发技术不包括：安全漏洞利用
37. 针对恶意程序检测或查杀的主要技术不包括：被动防御查杀
38. 不属于ISMS架构的具体实施是：体系审核
39. 在信息安全管理体系审核实施的过程中，审核报告的内容不包括：纠正措施
40. 风险管理的第一阶段是：风险识别
41. 风险评估过程包括：以上都对（信息资产评估、风险的确定、识别可能的控制，记录风险评估的结果）
42. 残留风险可以是：以上都对（降低了通过安全措施减小威胁的效果的一种威胁、降低了通过安全措施减少漏洞的效果的一种漏洞、降低了通过安全措施保护资产价值的效果的一种资产）
43. 信息安全管理系统的特征，不包括：智能化
44. 访问控制的实现可以按照行政、逻辑/技术、物理分为三类，其中行政性控制不包括：防护装置、移动探测器
45. 不属于国际信息安全标准化组织的是：CITS
46. 保证没有经过授权的用户不能改变或删除信息，符合信息技术安全评估标准有关信息安全的：完整性
47. 受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或对社会秩序和公共利益造成损害，但不损害国家安全的信息系统，属于信息系统安全保护等级的：第二级
48. 不属于我国网络空间安全战略任务的是：彻底消除网络犯罪活动的威胁
49. 我国网络空间安全战略的基本原则，不包括：加大惩处力度
50. 确定国家秘密的等级，应当遵守定密权限，其中，省级机关可以确定的密级是：所有密级（秘密级、机密级、绝密级）
51. 根据我国《电子签名法》，可以使用电子签名的文书不包括：涉及金融、保险等商业合同的
52. 填空题
53. 美国于 1977 年制定的数据加密标准DES，为加密算法的标准化奠定了基础
54. P2DR模型的4个主要部分包括： 策略 、防护、检测和响应
55. 如果密钥的二进制位数为8位，则密钥空间大小为 256
56. 在访问控制技术中，AAA服务是指认证、授权和 审计 三种服务
57. RSA 算法的安全性是建立在大整数分解的困难问题之上的
58. ELGAmAI算法是基于 离散对数 求解困难的问题设计的
59. 国密算法中的公钥密码算法有SM2和 SM9
60. 现代CPU通常运行在两种模式下： 用户 模式和内核模式
61. 操作系统采用 保护环 机制来确保进程不会在彼此之间或对系统的重要组件造成负面影响
62. 数据库软件提供三种类型的完整性服务： 域 完整性、参照完整性和实体完整性
63. 在Linux中，有关当前登录用户信息保存在 utmp 文件中
64. TCP全连接扫描技术在扫描时，源主机和目标主机的TCP连接状态出于 三次握手 状态
65. PKI是用公钥密码技术来实施和提供安全服务的安全基础设施，它是创建、管理、存储、分发和作废 数字证书 的一系列软件、硬件、人员、策略和过程的集合
66. 用于存放一个始终指向返回地址的指针的寄存器是 指令 寄存器
67. 栈帧包括两个指针，一个为帧指针，固定指向栈的基址；另一个为 栈顶 指针，随着分配的局部变量空间大小而变动
68. 限制内存堆栈区的代码为不可执行的状态，从而防范溢出后代码的执行，该安全防护技术称为数据执行保护技术，其英文缩写为 DEP
69. 模糊 测试是一种自动化或半自动化的安全漏洞检测技术，通过向目标软件输入大量的畸形数据并监测目标系统的异常来发现潜在的软件漏洞
70. 代码混淆 技术是在保持原有代码功能的基础上，通过代码变换等混淆手段实现降低代码的人工可读性，隐藏代码原始逻辑的一种技术
71. 事故响应的四个阶段为计划、检测、反应和 恢复
72. 计算机系统信息安全评估的第一个正式标准是“可信计算机系统安全评估标准”，其英文缩写为 TCSEC ，也称橘皮书
73. **综合题**

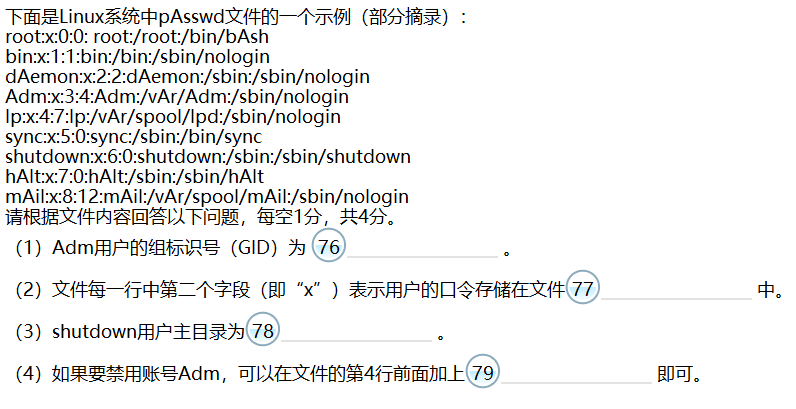
**71~75（第75空2分，其余每空1分，共6分）**





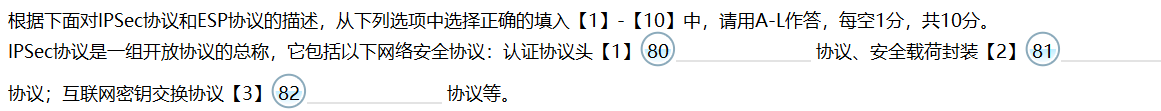
1. F
2. G
3. C
4. D
5. H

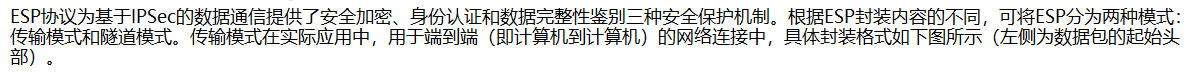
**76~79（每空1分，共4分）**

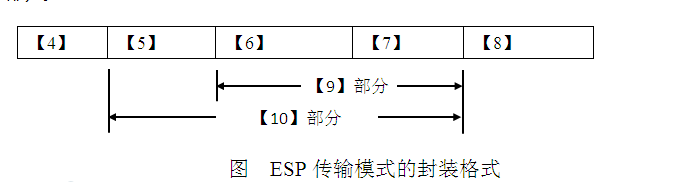


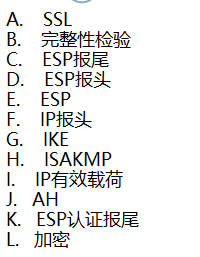
1. 4
2. shAdow
3. sbin
4. #

**80~89（每空1分，共10分）**









1. 【1】J
2. 【2】E
3. 【3】G
4. 【4】F
5. 【5】D
6. 【6】I
7. 【7】C
8. 【8】K
9. 【9】L
10. 【10】B