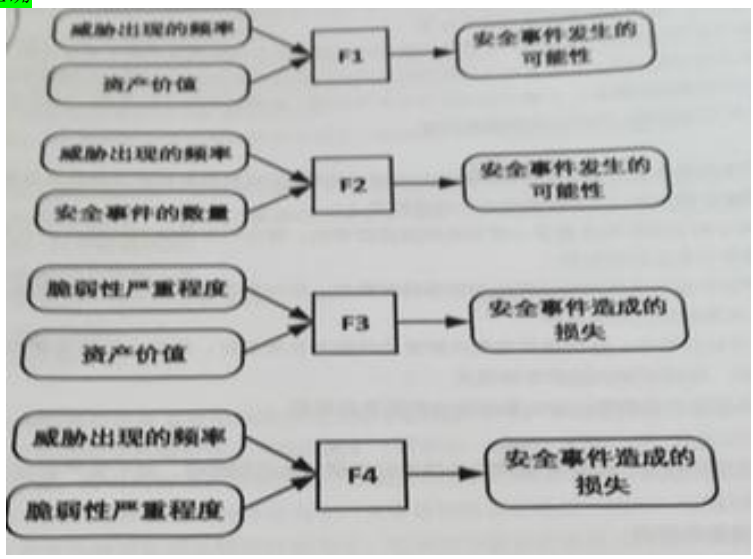
信息安全专业人员知识测试试题（四）

1. 小陈学习了有关信息安全管理体系的内容后，认为组织建立信息安全管理体系并持续运行，比起简单地实施信息安全管理，有更大的作用，他总结了四个方面的作用，其中总结错误的是（ ）
A．可以建立起文档化的信息安全管理规范，实现有“法”可依，有章可循，有据可查
B．可以强化员工的信息安全意识，建立良好的安全作业习惯，培育组织的信息安全企业文化
C．可以增强客户、业务伙伴、投资人对该组织保障其业务平台和数据信息的安全信心
D．可以深化信息安全管理，提高安全防护效果，使组织通过国际标准化组织的 ISO9001 认证
答案：

2. 随着“互联网”概念的普及，越来越多的新兴住宅小区引入了“智能楼宇”的理念，某物业为提供高档次的服务，防止网络主线路出现故障，保证小区内网络服务的可用，稳定、高效，计划通过网络冗余配置的是（）。
A、接入互联网时，同时采用不同电信运营商线路，相互备份且互不影响。
B、核心层、汇聚层的设备和重要的接入层设备均应双机设备。
C、规划网络 IP 地址，制定网络 IP 地址分配策略
D、保证网络带宽和网络设备的业务处理能力具务冗余空间，满足业务高峰期和业务发展需求
答案：

3. 小陈自学了风评的相关国家准则后，将风险的公式用图形来表示，下面 F1，F2，F3，F4 分别代表某种计算函数，四张图中，那个计算*关系正确*

A



B

C.

D

答案：

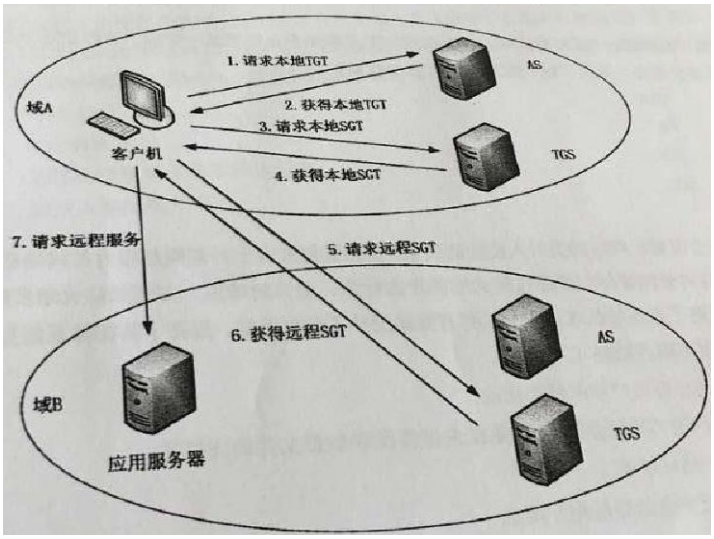
4. 在网络信息系统建设中部署防火墙，往往用于提高内部网络的安全防护能力。某公司准备部署一台防火墙来保护内网主机，下列选项中部署位置正确的是（）
A. 内网主机——交换机——防火墙——外网
B. 防火墙——内网主机——交换机——外网
C. 内网主机——防火墙——交换机——外网
D. 防火墙——交换机——内网主机——外网
答案：

5. 下列关于软件安全开发中的 BSI（Build Security In)系列模型说法错误的是（）
A、BIS 含义是指将安全内建到软件开发过程中，而不是可有可无，更不是游离于软件开发生命周期之外
B、软件安全的三根支柱是风险管理、软件安全触点和安全测试
C、软件安全触点是软件开发生命周期中一套轻量级最优工程化方法，它提供了从不同角度保障安全的行为方式
D、BSI 系列模型强调应该使用工程化的方法来保证软件安全，即在整个软件开发生命周期中都要确保将安全作为软件的一个有机组成部分
答案：
解释：安全测试修改为安全知识。

6. 访问控制是对用户或用户访问本地或网络上的域资源进行法令一种机制。在 Windows2000 以后的操作系统版本中，访问控制是一种双重机制，它对用户的授权基于用户权限和对象许可，通常使用 ACL、访问令牌和授权管理器来实现访问控制功能。以下选项中，对 windows 操作系统访问控制实现方法的理解错误的是（）
A、ACL 只能由管理员进行管理

B、ACL 是对象安全描述的基本组成部分，它包括有权访问对象的用户和级的 SID
C、访问令牌存储着用户的 SID，组信息和分配给用户的权限
D、通过授权管理器，可以实现基于角色的访问控制
答案：

7. 在现实的异构网络环境中，越来越多的信息需要实现安全的互操作。即进行跨域信息交换和处理。Kerberos 协议不仅能在域内进行认证，也支持跨域认证，下图显示的是 Kerberos 协议实现跨域认证的 7 个步骤，其中有几个步骤出现错误，图中错误的描述正确的是：



A. 步骤 1 和步骤 2 发生错误
B. 步骤 3 和步骤 4 发生错误
C. 步骤 5 和步骤 6 发生错误
D. 步骤 5 和步骤 6 发生错误
答案：3 和 4 是错误的，应该是 3 访问域 B 的 AS（请求远程 TGT），4 是域 B 的 AS 返回客户机(返回 TGT)。

8. 某黑客通过分析和整理某报社记者小张的博客，找到一些有用的信息，通过伪装的新闻线索，诱使其执行木马程序，从而控制了小张的电脑，并以她的电脑为攻击的端口，使报社的局域网全部感染木马病毒，为防范此类社会工程学攻击，报社不需要做的是（）
A、加强信息安全意识培训，提高安全防范能力，了解各种社会工程学攻击方法，防止受到此类攻击
B、建立相应的安全相应应对措施，当员工受到社会工程学的攻击，应当及时报告
C、教育员工注重个人隐私保护
D、减少系统对外服务的端口数量，修改服务旗标
答案：

9. 2016 年 9 月，一位安全研究人员在 Google Cloud IP 上通过扫描，发现了完整的美国路易斯安邦州 290 万选民数据库。这套数据库中囊括了诸如完整姓名、电子邮箱地址、性别与种族、选民状态、注册日期与编号、政党代名和密码，以防止攻击者利用以上信息进行（）攻击。
A、默认口令 B、字典 C、暴力 D、XSS
答案：

10. 下图中描述网络动态安全的 P2DR 模型，这个模型经常使用图形的形式来表达的下图空白处应填（）

A. 策略 B. 方针 C. 人员 D. 项目
答案：

11. 如图所示，主机 A 向主机 B 发出的数据采用 AH 或者 ESP 的**传输模式**对流量进行保护时，主机 A 和主机 B 的 IP 地址在应该在下列哪个范围？

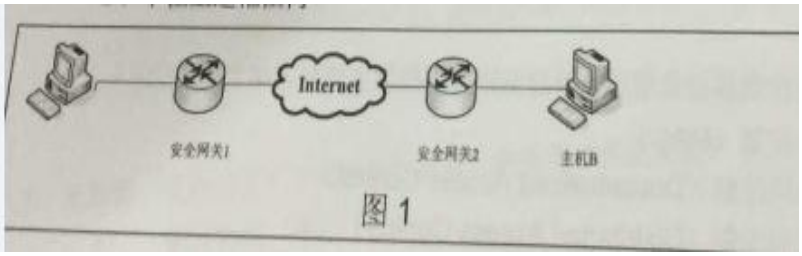
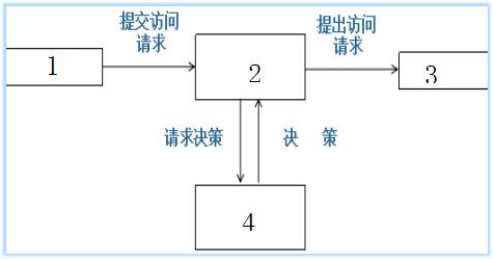


图 1

A. 10.0.0.0~10.255.255.255
B. 172.16.0.0~172.31.255.255
C. 192.168.0.0~192.168.255.255
D. 不在上述范围内
答案：

12. 小王是某大学计算机科学与技术专业的学生，最近因为生病缺席了几堂信息安全课程，这几次课的内容是自主访问控制与强制访问控制，为了赶上课程进度，他向同班的小李借来课堂笔记，进行自学。而小李在听课时由于经常走神，所以笔记中会出现一些错误。下列选项是小李笔记中关于强制访问控制模型的内容，其中出现错误的选项是（）
A、强制访问控制是指主体和客体都有一个固定的安全属性，系统用该安全属性来决定一个主体是否可以访问某个客体
B、安全属性是强制性的规定，它由安全管理员或操作系统根据限定的规则确定，不能随意修改
C、系统通过比较客体和主体的安全属性来决定主体是否可以访问客体
D、它是一种对单个用户执行访问控制的过程控制措施
答案：

13. 下图排序你认为那个是正确的：



A. 1 是主体，2 是客体,3 是实施，4 是决策
B. 1 是客体，2 是主体 3 是决策，4 是实施
C. 1 实施，2 是客体 3 是主题，4 是决策
D. 1 是主体，2 是实施 3 是客体，4 是决策
答案：

14. 某社交网站的用户点击了该网站上的一个广告。该广告含有一个跨站脚本，会将他的浏览器定向到旅游网站，旅游网站则获得了他的社交网络信息。虽然该用户没有主动访问该旅游网站，但旅游网站已经截获了他的社交网络信息（还有他的好友们的信息），于是犯罪分子便可以躲藏在社交网站的广告后面，截获用户的个人信息了，这种向 Web 页面插入恶意 html 代码的攻击方式称为（）
A. 分布式拒绝服务攻击 B、跨站脚本攻击 C、SQL 注入攻击 D、缓冲区溢出攻击
答案：

15. 模糊测试也称 Fuzz 测试，是一种通过提供非预期的输入并监视异常结果来发现软件故障的方法。下面描述正确的是（）
A、模糊测试本质上属于黑盒测试
B、模糊测试本质上属于白盒测试
C、模糊测试有时属于黑盒测试，有时属于白盒测试，取决于其使用的测试方法
D、模糊测试既不属于黑盒测试，也不属于白盒测试
答案：
解释：拿分选 A，知识点是 C。

16. 若一个组织声称自己的 ISMS 符合 ISO/IEC 27001 或 GB/T22080 标准要求，其信息安全控制措施通常需要在人力资源安全方面实施常规控制，人力资源安全划分为 3 个控制阶段，不包括哪一项（）
A、任用之前 B、任用中 C、任用终止或变化 D、任用后
答案：

17. 下图是安全测试人员连接某远程主机时的操作界面，请您仔细分析该图，下面分析推理正确的是（）

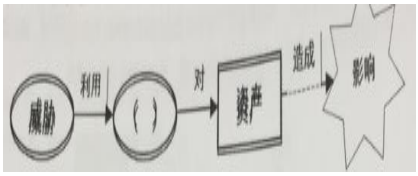
```
C:\WINDOWS\system32\cmd.exe
220 Serv-U FTP Server V6.0 for WinSock ready…
Quit
221 Goodbye!

失去了跟主机的连接
C:\Documents and Settings\lyxiaowei>
```

A.安全测试人员链接了远程服务器的 220 端口
B.安全测试人员的本地操作系统是 Linux
C.远程服务器开启了 FTP 服务，使用的服务器软件名 FTP Server
D.远程服务器的操作系统是 windows 系统
答案：

18. 某信息安全公司的团队对某款名为“红包快抢”的外挂进行分析发现此外挂是一个典型的木马后门，使黑客能够获得受害者电脑的访问权，该后门程序为了达到长期驻留在受害者的计算机中，通过修改注册表启动项来达到后门程序随受害者计算机系统启动而启动为防范此类木马的攻击，以下做法无用的是（）
A、不下载、不执行、不接收来历不明的软件和文件
B、不随意打开来历不明的邮件，不浏览不健康不正规的网站
C、使用共享文件夹
D、安装反病毒软件和防火墙，安装专门的木马防范软件
答案：

19. 小华在某电子商务公司工作，某天他在查看信息系统设计文档时，发现其中标注该信息系统的 RPO（恢复点目标）指标为 3 小时。请问这意味着（）
A、该信息系统发生重大安全事件后，工作人员应在 3 小时内到位，完成问题定位和应急处理工作
B、该信息系统发生重大安全事件后，工作人员应在 3 小时内完整应急处理工作并恢复对外运行
C、该信息系统发生重大安全事件后，工作人员在完成处置和灾难恢复工作后，系统至少能提供 3 小时的紧急业务服务能力
D、该信息系统发生重大安全事件后，工作人员在完成处置和灾难恢复工作后，系统至多能丢失 3 小时的业务数据
答案：

20. 陈工学习了信息安全风险的有关知识，了解到信息安全风险的构成过程，有五个方面：起源、方式、途径、受体和后果，他画了下面这张图来描述信息安全风险的构成过程，图中空白处应填写？



A.信息载体 B.措施 C.脆弱性 D.风险评估
答案：

21. Kerberos 协议是一种集中访问控制协议，他能在复杂的网络环境中，为用户提供安全的单点登录服务。单点登录是指用户在网络中进行一次身份认证，便可以访问其授权的所有网络资源，而不在需要其他的认证过程，实质是消息 M 在多个应用系统之间的传递或共享。其中消息 M 是指以下选项中的()
A、安全凭证 B、用户名 C、加密密钥 D、会话密钥
答案：
解释：安全凭证指的是服务许可票据。

22. 若一个组织声称自己的 ISMS 符合 ISO/IEC 27001 或 GB/T22080 标准要求。其信息安全控制措施通常需要在物理和环境安全方面实施常规控制。物理和环境安全领域包括安全区域和设备安全两个控制目标。安全区域的控制目标是防止对组织场所和信息的未授权物理访问、损坏和干扰。关键或敏感的信息及信息处理设施应放在安全区域内并受到相应保护。该目标可以通过以下控制措施来实现，不包括哪一项
A. 物理安全边界、物理入口控制 B. 办公室、房间和设施的安全保护。外部和环境威胁的安全防护
C. 在安全区域工作。公共访问、交接区安全 D. 人力资源安全
答案：

23. 风险分析师风险评估工作的一个重要内容，GB/T 20984-2007 在资料性附录中给出了一种矩阵法来计算信息安全风险大小，如下图所示，图中括号应填那个？

（ ）	安全事件发生可能性				
	1	2	3	4	5
1	3	6	9	12	16
2	5	8	11	15	18
3	6	9	13	17	21
4	7	11	16	20	23
5	9	14	20	23	25

A. 安全资产价值大小等级　　C. 安全风险隐患严重等级
B. 脆弱性严重程度等级　　D. 安全事件造成损失大小
答案：

24. 关于信息安全管理体系的作用，下面理解错误的是
A. 对内而言，有助于建立起文档化的信息安全管理规范，实现有“法”可依，有据可查
B. 对内而言，是一个光花钱不挣钱的事情，需要组织通过其他方法收入来弥补投入
C. 对外而言，有助于使各科室相关方对组织充满信心
D. 对外而言，规范工作流程要求，帮助界定双方各自信息安全责任
答案：

25. 关于补丁安装时应注意的问题，以下说法正确的是
A. 在补丁安装部署之前不需要进行测试，因为补丁发布之前厂商已经经过了测试
B. 补丁的获取有严格的标准,必须在厂商的官网上获取
C. 信息系统打补丁时需要做好备份和相应的应急措施
D. 补丁安装部署时关闭和重启系统不会产生影响
答案：

26. 某电子商务网站架构设计时，为了避免数据误操作，在管理员进行订单删除时，需要由审核员进行审核后该删除操作才能生效，这种设计是遵循了发下哪个原则
A. 权限分离原则　　B. 最小的特权原则　　C. 保护最薄弱环节的原则　　D. 纵深防御的原则
答案：

27. 实体身份鉴别的方法多种多样，且随着技术的进步，鉴别方法的强度不断提高，常见的方法有指令鉴别、令牌鉴别、指纹鉴别等。如图，小王作为合法用户使用自己的账户进行支付、转账等操作。这说法属于下列选项中的（）

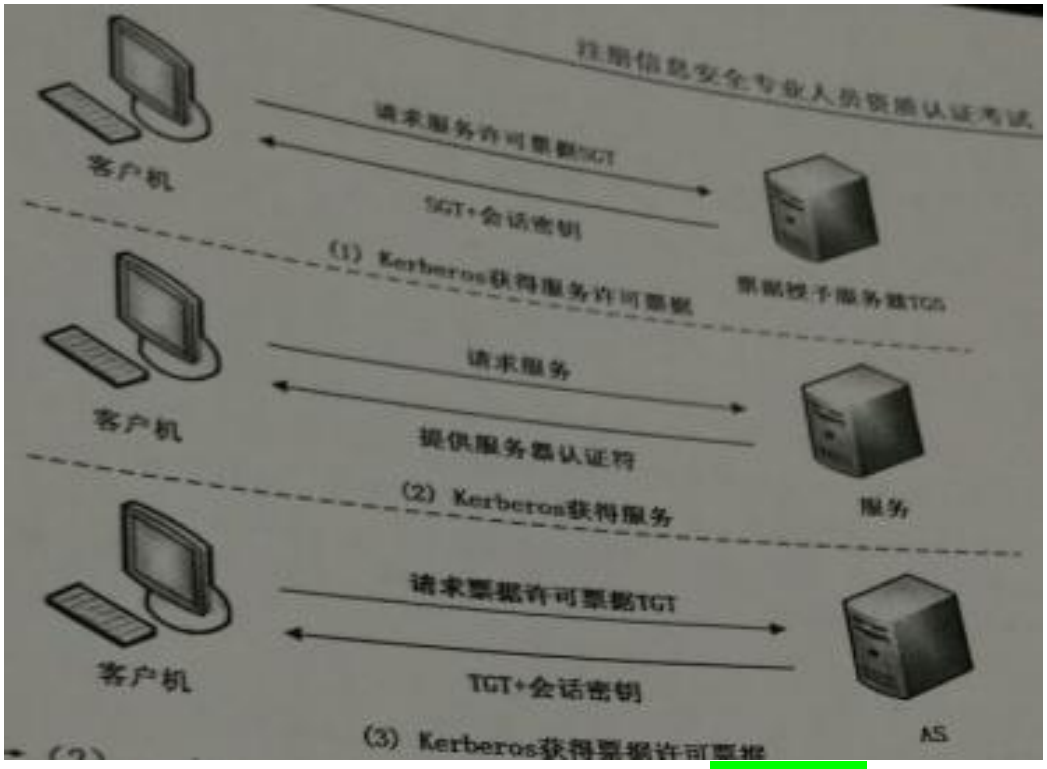
A. 实体所知的鉴别方法　B. 实体所有的鉴别方法　C. 实体特征的鉴别方法　D. 实体所见的鉴别方法
答案：

28. 定量风险分析是从财务数字上对安全风险进行评估，得出可以量化的风险分析结果，准确度量风险的可以性和损失量。小王采用该方法来为单位机房计算火灾风险大小，假设单位机房的总价值为 200 万元人民币，暴露系数（ExposureFactor,EF）是 x,年度发生率（Annual izod Eato of Occurrence,ARO）为 0.1，而小王计算的年度预期损失（Annual izod Loss Erpectancy,ALE）值为 5 万元人民币，由此，x 值应该是
A. 2.5%　　B. 25%　　C. 5%　　D. 50%
答案：
解析：200X*0.1=5 万

29. 关于 Kerberos 认证协议，以下说法错误的是：
A. 只要用户拿到了认证服务器（AS）发送的票据许可票据（TGT）并且该 TGT 没有过期，就可以使用该 TGT 通过票据授权服务器（TGS）完成到任一个服务器的认证而不必重新输入密码

B.认证服务器（AS）和票据授权服务器（TGS）是集中式管理，容易形成瓶颈，系统的性能和安全也严重依赖于 AS 和 TGS 的性能和安全
C.该协议通过用户获得票据许可票据、用户获得服务许可票据、用户获得服务三个阶段，仅支持服务器对用户单向认证
D.该协议是一种基于对称密码算法的网络认证协议，随用户数量增加，密钥管理较复杂
答案：

30. kerberos 协议是常用的集中访问控制协议,通过可信第三的认证服务,减轻应用 Kerberos 的运行环境由秘钥分发中心（KDC）、应用服务器和客户端三个部分组成，认证服务器 AS 和票据授权服务器



A.1——2——3 B.3——2——1 C.2——1——3 D.3——1——2
答案：

31. 某单位系统管理员对组织内核心资源的访问制定访问策略，针对每个用户指明能够访问的资源，对于不在指定资源列表中的对象不允许访问。该访问控制策略属于以下哪一种：
A.强制访问控制 B.基于角色的访问控制 C.自主访问控制 D.基于任务的访问控制
答案：

32. 由于 Internet 的安全问题日益突出，基于 TCP/IP 协议，相关组织和专家在协议的不同层次设计了相应的安全通信协议，用来保障网络各层次的安全。其中，属于或依附于传输层的安全协议是（）
A. PP2P B. L2TP C. SSL D. IPSec
答案：

33. 根据 Bell-LaPedula 模型安全策略，下图中写和读操作正确的是（ ）

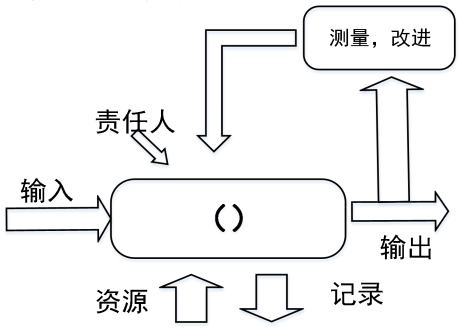
A.可读可写 B.可读不可写 C.可写不可读 D.不可读不可写
答案：

34. 防火墙是网络信息系统建设中常采用的一类产品，它在内外网隔离方面的作用是（）。
A.既能物理隔离，又能逻辑隔离 B.能物理隔离，但不能逻辑隔离
C.不能物理隔离，但是能逻辑隔离 D.不能物理隔离，也不能逻辑隔离
答案：

35. 张主任的计算机使用 Windows7 操作系统，他常登陆的用户名为 zhang，张主任给他个人文件夹设置了权限为只有 zhang 这个用户有权访问这个目录，管理员在某次维护中无意将 zhang 这个用户删除了，随后又重新建了一个用户名为 zhang，张主任使用 zhang 这个用户登录系统后，发现无法访问他原来的个人文件夹，原因是：
A. 任何一个新建用户都需要经过授权才能访问系统中的文件
B. Windows7 不认为新建立的用户 zhang 与原来用户 zhang 是同一个用户，因此无权访问
C. 用户被删除后，该用户创建的文件夹也会自动删除，新建用户找不到原来用户的文件夹，因此无法访问
D. 新建的用户 zhang 会继承原来用户的权限，之所以无权访问是因为文件夹经过了加密
答案：

36. 以下关于 Windows 系统的账号存储管理机制（Security Accounts Manager）的说法哪个是正确的：
A. 存储在注册表中的账号数据是管理员组用户都可以访问，具有较高的安全性
B. 存储在注册表中的账号数据只有 administrator 账户才有权访问，具有较高的安全性
C. 存储在注册表中的账号数据任何用户都可以直接访问，灵活方便
D. 存储在注册表中的账号数据有只有 System 账户才能访问，具有较高的安全性
答案：

37. ISO9001-2000 标准在制定、实施质量管理体系以及改进其有效性时采用过程方法，通过满足顾客要求增进顾客满意。下图是关于过程方法的示意图，图中括号空白处应填写（）

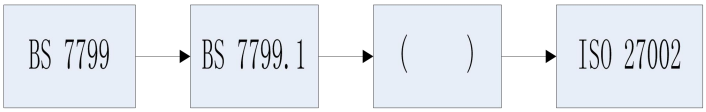


A. 策略 B. 管理者 C. 组织 D. 活动
答案：

38. 设计信息系统安全保障方案时，以下哪个做法是错误的：
A. 要充分切合信息安全需求并且实际可行
B. 要充分考虑成本效益，在满足合规性要求和风险处置要求的前提下，尽量控制成本
C. 要充分采取新技术，在使用过程中不断完善成熟，精益求精，实现技术投入保值要求
D. 要充分考虑用户管理和文化的可接受性，减少系统方案实施障碍
答案：

39. Windows 文件系统权限管理访问控制列表（Access Control List，ACL）机制，以下哪个说法是错误的：
A. 安装 Windows 系统时要确保文件格式使用的是 NTFS，因为 Windows 的 ACL 机制需要 NTFS 文件格式的支持
B. 由于 Windows 操作系统自身有大量的文件和目录，因此很难对每个文件和目录设置严格的访问权限，为了使用上的便利，Windows 上的 ACL 存在默认设置安全性不高的问题
C. Windows 的 ACL 机制中，文件和文件夹的权限是与主体进行关联的，即文件夹和文件的访问权限信息是写在用户数据库中
D. 由于 ACL 具有很好的灵活性，在实际使用中可以为每一个文件设定独立用户的权限
答案：

40. ISO27002（Information technology-Security techniques0Codeofpratice for inforeation security managcacnt）是重要的信息安全管理标准之一，下图是关于其演进变化示意图，图中括号空白处应填写（）

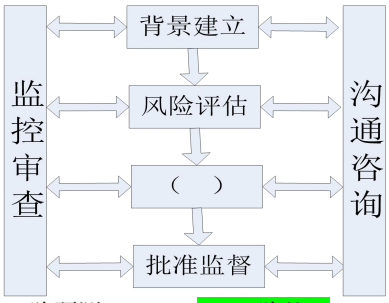


A. BS 7799.1.3 B. ISO 17799 C. AS/NZS 4630 D. NIST SP 800-37
答案：

41. 自主访问控制模型（DAC）的访问控制关系可以用访问控制（ACL）来表示，该 ACL 利用在客体上附加一个主体明细表的方法来表示访问控制矩阵，通常使用由客体指向的链表来存储相关数据。下面选项中说法正确的是（）
A. ACL 是 Bell-LaPadula 模型的一种具体实现
B. ACL 在删除用户时，去除该用户所有的访问权限比较方便
C. ACL 对于统计某个主体能访问哪些客体比较方便
D. ACL 在增加客体时，增加相关的访问控制权限较为简单
答案：

42. 数据库的安全很复杂，往往需要考虑多种安全策略，才可以更好地保护数据库的安全。以下关于数据库常用的安全策略理解不正确的是：
A.最小特权原则，是让用户可以合法的存取或修改数据库的前提下，分配最小的特权，使得这些信息恰好能够完成用户的工作
B.最大共享策略，在保证数据库的完整性、保密性和可用性的前提下，最大程度也共享数据库中的信息
C.粒度最小策略，将数据库中的数据项进行划分，粒度越小，安全级别越高，在实际中需要选择最小粒度
D.按内容存取控制策略，不同权限的用户访问数据库的不同部分
答案：

43. 我国标准《信息安全风险管理指南》（GB/Z24364）给出了信息安全风险管理的内容和过程，可以用下图来表示。图中空白处应该填写（）

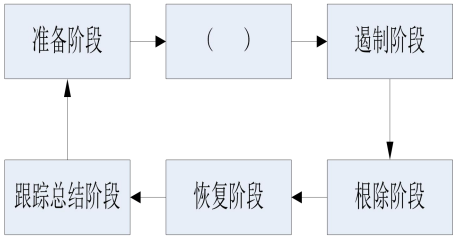


A.风险计算 B.风险评价 C.风险预测 D.风险处理
答案：

44. 以下哪一项不是信息系统集成项目的特点：
A.信息系统集成项目要以满足客户和用户的需求为根本出发点
B.系统集成就是选择最好的产品和技术，开发相应的软件和硬件，将其集成到信息系统的过程
C.信息系统集成项目的指导方法是“总体规划、分步实施”
D.信息系统集成包含技术，管理和商务等方面，是一项综合性的系统工程
答案：

45. 某单位的信息安全主管部门在学习我国有关信息安全的政策和文件后，认识到信息安全风险评估分为自评估和检查评估两种形式。该部门将有关检查评估的特点和要求整理成如下四条报告给单位领导，其中描述错误的是（）
A.检查评估可依据相关标准的要求，实施完整的风险评估过程；也可在自评估的基础上，对关键环节或重点内容实施抽样评估
B.检查评估可以由上级管理部门组织，也可以由本级单位发起，其重点是针对存在的问题进行检查和评测
C.检查评估可以由上级管理部门组织，并委托有资质的第三方技术机构实施
D.检查评估是通过行政手段加强信息安全管理的重要措施，具有强制性的特点
答案：

46. 为了能够合理、有序地处理安全事件，应事件制定出事件应急响应方法和过程，有助于一个组织在事件发生时阻止混乱的发生或是在混乱状态中迅速恢复控制，将损失和负面影响降至最低。PDCERF 方法论是一种防范使用的方法，其将应急响应分成六个阶段，如下图所示，请为图中括号空白处选择合适的内容（）



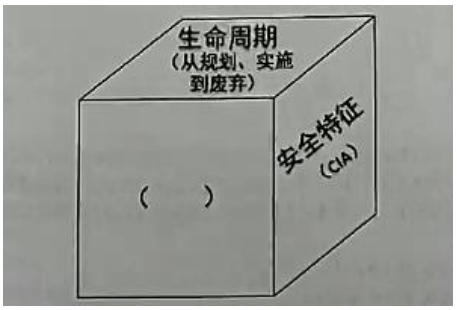
A.培训阶段 B.文档阶段 C.报告阶段 D.检测阶段

答案：

47. 关于信息安全管理，下面理解片面的是（）
A.信息安全管理是组织整体管理的重要、固有组成部分，它是组织实现其业务目标的重要保障
B.信息安全管理是一个不断演进、循环发展的动态过程，不是一成不变的
C.在信息安全建设中，技术是基础，管理是拔高，有效的管理依赖于良好的技术基础
D.坚持管理与技术并重的原则，是我国加强信息安全保障工作的主要原则之一
答案：

48. 关于风险要素识别阶段工作内容叙述错误的是：
A.资产识别是指对需要保护的资产和系统等进行识别和分类
B.威胁识别是指识别与每项资产相关的可能威胁和漏洞及其发生的可能性
C.脆弱性识别以资产为核心，针对每项需要保护的资产，识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估
D.确认已有的安全措施仅属于技术层面的工作，牵涉到具体方面包括：物理平台、系统平台、网络平台和应用平台
答案：

49. 某学员在学习国家标准《信息系统安全保障评估框架第一部分：简介和一般模型》（GB/T 20274.1-2006）后，绘制了一张简化的信息系统安全保障模型图，如下所示。请为图中括号空白处选择合适的选项（）



A.安全保障（方针和组织） B.安全防护（技术和管理）
C.深度防御（策略、防护、检测、响应） D.保障要素（管理、工程、技术、人员）
答案：

50. 为了进一步提供信息安全的保障能力和防护水平，保障和促进信息化建设的健康发展，公安部等四部门联合发布《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号），对等级保护工作的开展提供宏观指导和约束，明确了等级保护工作哟的基本内容、工作要求和实施计划，以及各部门工作职责分工等。关于该文件，下面理解正确的是（）
A.该文件是一个由部委发布的政策性文件，不属于法律文件
B.该文件适用于 2004 年的等级保护工作，其内容不能约束到 2005 年及之后的工作
C.该文件是一个总体性指导文件，规定所有信息系统都要纳入等级保护定级范围
D.该文件适用范围为发文的这四个部门，不适用于其他部门和企业等单位
答案：

51. 在某次信息安全应急响应过程中，小王正在实施如下措施：消除或阻断攻击源、找到并消除系统的脆弱性/漏洞、修改安全策略、加强防范措施、格式化被感染恶意程序的介质等。请问，按照 PDCERF 应急响应方法，这些工作应处于以下哪个阶段（）
A.准备阶段 B.检测阶段 C.遏制阶段 D.根除阶段
答案：

52. Linux 系统的安全设置中，对文件的权限操作是一项关键操作。通过对文件权限的设置，能够保障不同用户的个人隐私和系统安全。文件 fib.c 的文件属性信息如下图所示，小张想要修改其文件权限，为文件主增加执行权限，并删除组外其他用户的写权限，那么以下操作中正确的是（）

A.#chmod u+x, a-w fib.c B.#chmod ug+x, o-w fib.c C.#chmod 764 fib.c D.#chmod 467 fib.c
答案：
解释：在第一组权限上“为文件主增加执行权限”后变成了 RWX 即 111，即十进制 7；在第三组权限上“删除组外其他用户的写权限”后变成了 R--即 100，即十进制 4；而在第二组权限上中间的组的没有变即 RW-即 110，即十进制 6。

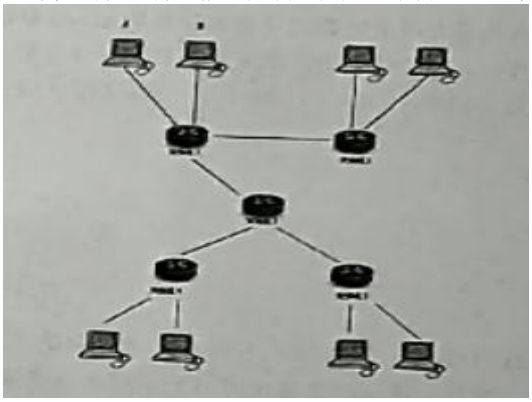
53. 关于信息安全事件管理和应急响应，以下说法错误的是：
A.应急响应是指组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施
B.应急响应方法，将应急响应管理过程分为遏制、根除、处置、恢复、报告和跟踪 6 个阶段
C.对信息安全事件的分级主要参考信息系统的重要程度、系统损失和社会影响三方面因素
D.根据信息安全事件的分级参考要素，可将信息安全事件划分为 4 个级别：特别重大事件（I 级）、重大事件（II 级）、较大事件（III 级）和一般事件（IV 级）
答案：

54. 恢复时间目标（RTO）和恢复点目标（RPO）是信息系统灾难恢复的重要概念，关于这两个值能否为零，正确的选项是（）
A. RTO 可以为 0，RPO 也可以为 0
B. RTO 可以为 0，RPO 不可以为 0
C. RTO 不可以为 0，但 RPO 可以为 0
D. RTO 不可以为 0，RPO 也不可以为 0
答案：

55. 下面有关软件安全问题的描述中，哪项应是由于软件设计缺陷引起的（）
A.设计了三层 WEB 架构，但是软件存在 SQL 注入漏洞，导致被黑客攻击后直接访问数据库
B.使用 C 语言开发时，采用了一些存在安全问题的字符串处理函数，导致存在缓冲区溢出漏洞
C.设计了缓存用户隐私数据机制以加快系统处理性能，导致软件在发布运行后，被黑客攻击获取到用户隐私数据
D.使用了符合要求的密码算法，但在使用算法接口时，没有按照要求生成密钥，导致黑客攻击后能破解并得到明文数据
答案：

56. 通过对称密码算法进行安全消息传输的必要条件是：
A. 在安全的传输信道上进行通信
B. 通讯双方通过某种方式，安全且秘密地共享密钥
C. 通讯双方使用不公开的加密算法
D. 通讯双方将传输的信息夹杂在无用信息中传输并提取
答案：

57. 某银行有 5 台交换机连接了大量交易机构的网路（如图所示），在基于以太网的通信中，计算机 A 需要与计算机 B 通信，A 必须先广播“ARP 请求信息”，获取计算机 B 的物理地址。没到月底时用户发现该银行网络服务速度极其缓慢。银行经调查后发现为了当其中一台交换机收到 ARP 请求后，会转发给接收端口以外的其他所有端口，ARP 请求会被转发到网络中的所有客户机上。为降低网络的带宽消耗，将广播流限制在固定区域内，可以采用的技术是（）

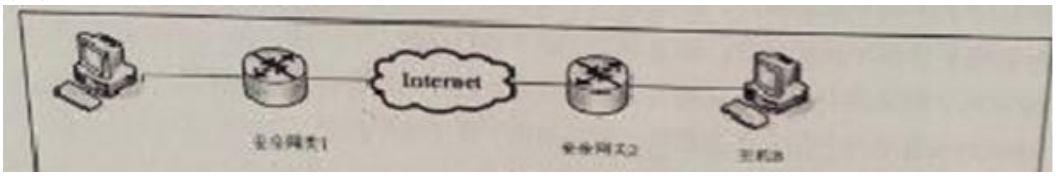


A.VLAN 划分　B.动态分配地址　C.设立入侵防御系统　D.为路由交换设备修改默认口令
答案：

58. Windows 系统下，哪项不是有效进行共享安全的防护措施？
A. 使用 netshare\\127.0.0.1\c$/delete 命令，删除系统中的 c$等管理共享，并重启系统
B. 确保所有的共享都有高强度的密码防护
C. 禁止通过“空会话”连接以匿名的方式列举用户、群组、系统配置和注册表键值
D. 安装软件防火墙阻止外面对共享目录的连接
答案：

59. 以下对 Windows 账号的描述，正确的是：
A. Windows 系统是采用 SID（安全标识符）来标识用户对文件或文件夹的权限
B. Windows 系统是采用用户名来标识用户对文件或文件夹的权限
C. Windows 系统默认会生成 administrator 和 guest 两个账号，两个账号都不允许改名和删除
D. Windows 系统默认生成 administrator 和 guest 两个账号，两个账号都可以改名和删除
答案：

60. 如图一所示:主机 A 和主机 B 需要通过 IPSec 隧道模式保护二者之间的通信流量,这种情况下 IPSec 的处理通常发生在哪二个设备中?



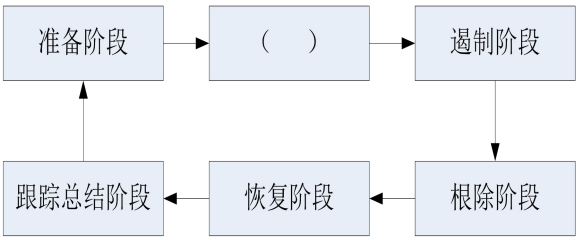
A. 主机 A 和安全网关 1;　B. 主机 B 和安全网关 2;　C. 主机 A 和主机 B 中;　D. 安全网关 1 和安全网关 2 中;
答案:

61. 以下关于代替密码的说法正确的是:
A. 明文根据密钥被不同的密文字母代替
B. 明文字母不变，仅仅是位置根据密钥发生改变
C. 明文和密钥的每个 bit 异或
D. 明文根据密钥作移位
答案:

62. AES 在抵抗差分密码分析及线性密码分析的能力比 DES 更有效，已经替代 DES 成为新的据加密标准。其算法的信息块长度和加密密钥是可变的，以下哪一种不是其可能的密钥长度?
A. 64bit　B. 128bit　C. 192bit　D. 256bit
答案:

63. 以下对 Windows 系统的服务描述，正确的是:
A. Windows 服务必须是一个独立的可执行程序
B. Windows 服务的运行不需要用户的交互登陆
C. Windows 服务都是随系统启动而启动，无需用户进行干预
D. Windows 服务都需要用户进行登陆后，以登录用户的权限进行启动
答案:

64. 为了能够合理、有序地处理安全事件，应事件制定出事件应急响应方法和过程，有助于一个组织在事件发生时阻止混乱的发生或是在混乱状态中迅速恢复控制，将损失和负面影响降至最低。PDCERF 方法论是一种防范使用的方法，其将应急响应分成六个阶段，如下图所示，请为图中括号空白处选择合适的内容（）

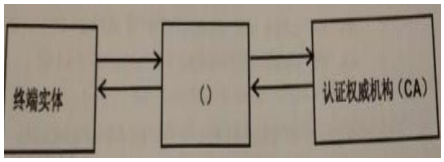


A. 培训阶段　B. 文档阶段　C. 报告阶段　D. 检测阶段
答案:

65. Alice 有一个消息 M 通过密钥 K2 生成一个密文 E（K2，M）然后用 K1 生成一个 MAC 为 C（K1，E（K2，M））， Alice 将密文和 MAC 发送给 Bob，Bob 用密钥 K1 和密文生成一个 MAC 并和 Alice 的 MAC 比较，假如相同再用 K2 解密 Alice 发送的密文，这个过程可以提供什么安全服务?
A. 仅提供数字签名　B. 仅提供保密性　C. 仅提供不可否认性　D. 保密性和消息完整性
答案:
解释：实现的安全服务包括保密性、完整性、身份鉴别、抗重放攻击。

66. 以下关于 windowsSAM(安全账号管理器)的说法错误的是:
A、安全账号管理器(SAM)具体表现就是%SystemRoot%\system32\config\sam
B、安全账号管理器(SAM)存储的账号信息是存储在注册表中
C、安全账号管理器(SAM)存储的账号信息 administrator 和 system 是可读和可写的
D、安全账号管理器(SAM)是 windows 的用户数据库系统进程通过 Security Accounts Manager 服务进行访问和操作
答案:

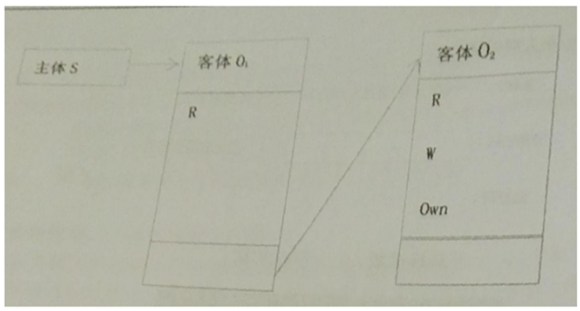
67. 公钥基础设施，引入数字证书的概念，用来表示用户的身份，下图简要的描述了终端实体（用户），从认证权威机构 CA 申请、撤销和更新数字证书的流程，请为中间框空白处选择合适的选项（）



A.证书库　　B.RA　　C.OCSP　　D .CRL 库
答案：

68. 常见密码系统包含的元素是：
A.明文，密文，信道，加密算法，解密算法　　C.明文，密文，密钥，加密算法，解密算法
B.明文，摘要，信道，加密算法，解密算法　　D.消息，密文，信道，加密算法，解密算法
答案：

69. 如图所示，主体 S 对客体 01 有读（R）权限，对客体 02 有读（R） 、写（）权限。该 图所示的访问控制实现方法是：



A.访问控制表（ACL）　　B.访问控制矩阵　　C.能力表（CL）　　D.前缀表（Profiles）
答案：

70. 社会工程学定位在计算机信息安全工作链的一个最脆弱的环节，即“人”这个环节上。这些社会工程黑客在某黑客大会上成功攻入世界五百强公司，其中一名自称是 CSO 杂志做安全调查，半小时内，攻击者选择了在公司工作两个月安全工程部门的合约雇员，在询问关于工作满意度以及食堂食物质量问题后，雇员开始透露其他信息，包括：操作系统、服务包、杀毒软件、电子邮件及浏览器。为对抗此类信息收集和分析，公司需要做的是（）
A、通过信息安全培训，使相关信息发布人员了解信息收集风险，发布信息最小化原则
B、减少系统对外服务的端口数量，修改服务旗标
C、关闭不必要的服务，部署防火墙、IDS 等措施
D、系统安全管理员使用漏洞扫描软件对系统进行安全审计
答案：

71. 基于 TCP 的主机在进行一次 TCP 连接时简要进行三次握手，请求通信的主机 A 要与另一台主机 B 建立连接时，A 需要先发一个 SYN 数据包向 B 主机提出连接请示，B 收到后，回复一个 ACK/SYN 确认请示给 A 主机，然后 A 再次回应 ACK 数据包，确认连接请求。攻击通过伪造带有虚假源地址的 SYN 包给目标主机，使目标主机发送的 ACK/SYN 包得不到确认。一般情况下，目标主机会等一段时间后才会放弃这个连接等待。因此大量虚假 SYN 包同时发送到目标主机时，目标主机上就会有大量的连接请示等待确认，当这些未释放的连接请示数量超过目标主机的资源限制时。正常的连接请示就不能被目标主机接受，这种 SYN Flood 攻击属于（）
A、拒绝服务攻击　　B、分布式拒绝服务攻击　　C、缓冲区溢出攻击　　D、SQL 注入攻击
答案：

72. 信息安全是国家安全的重要组成部分，综合研究当前世界各国信息安全保障工作，下面总结错误的是（）
A、各国普遍将与国家安全、社会稳定和民生密切相关的关键基础设施作为信息安全保障的重点
B、各国普遍重视战略规划工作，逐步发布网络安全战略、政策评估报告、推进计划等文件
C、各国普遍加强国际交流与对话，均同意建立一致的安全保障系统，强化各国安全系统互通
D、各国普遍积极推动信息安全立法和标准规范建设，重视应急响应、安全监管和安全测评
答案：

73. 公钥密码的应用不包括：
A、数字签名　　B、非安全信道的密钥交换　　C、消息认证码　　D、身份认证
答案：

74. hash 算法的碰撞是指：

A、两个不同的消息，得到相同的消息摘要　　C、消息摘要和消息的长度相同
B、两个相同的消息，得到不同的消息摘要　　D、消息摘要比消息长度更长
答案：

75. Windows 操作系统的注册表运行命令是：
A. Regsvr32　　B. Regedit　　C. Regedit.msc　　D. Regedit.mmc
答案：

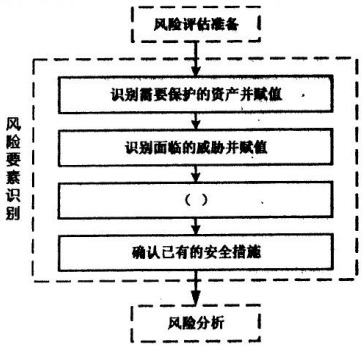
76. 视窗操作系统（Windows）从哪个版本开始引入安全中心的概念？
A. WinNT SP6　　B. Win2000 SP4　　C. WinXP SP2　　D. Win2003 SP1
答案：

77. DSA（数字签名算法）不提供以下哪种服务？
A、数据完整性　　B、加密　　C、数字签名　　D、认证
答案：

78. 在 Windows 文件系统中，_____支持文件加密。
A. FAT16　　B. NTFS　　C. FAT32　　D. EXT3
答案：

79. 相比 FAT 文件系统，以下那个不是 NTFS 所具有的优势？
A、NTFS 使用事务日志自动记录所有文件和文件夹更新，当出现系统损坏引起操作失败后，系统能利用日志文件重做或恢复未成功的操作。
B、NTFS 的分区上，可以为每个文件或文件夹设置单独的许可权限
C、对于大磁盘，NTFS 文件系统比 FAT 有更高的磁盘利用率。
D、相比 FAT 文件系统，NTFS 文件系统能有效的兼容 linux 下的 EXT3 文件格式。
答案：

80. 风险要素识别是风险评估实施过程中的一个重要步骤，小李将风险要素识别的主要过程使用图形来表示，如下图所示，请为图中空白框处选择一个最合适的选项()。

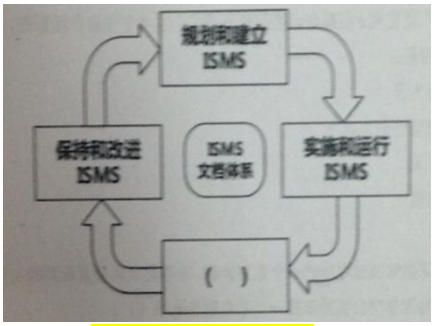


A. 识别面临的风险并赋值　　C. 制定安全措施实施计划
B. 识别存在的脆弱性并赋值　　D. 检查安全措施有效性
答案：

81. Windows NT 提供的分布式安全环境又被称为:
A、域（Domain）　　B、工作组　　C、对等网　　D、安全网
答案：

82. 在 Windows 系统中，管理权限最高的组是：
A. everyone　　B. administrators　　C. powerusers　　D. users
答案：

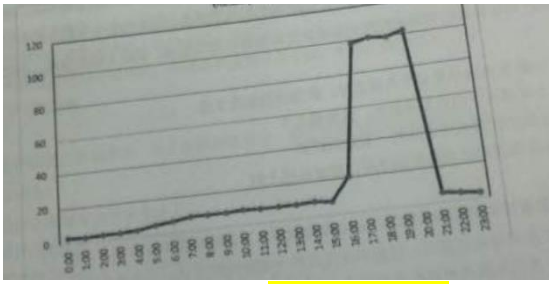
83. 小李去参加单位组织的信息安全培训后，他把自己对管理信息管理体系 ISMS 的理解画了一张图，但是他还存在一个空白处未填写，请帮他选择一个合适的选项（）



A. 监控和反馈 ISMS B. 批准和监督 ISMS C. 监视和评审 ISMS D. 沟通和咨询 ISMS
答案：

84. Windows 系统下，可通过运行_____命令打开 Windows 管理控制台。
A. regedit B. cmd C. mmc D. mfc
答案：

85. 下图是某单位对其主网站一天流量的监测图，如果该网站当天 17：00 到 20：00 之间受到攻击，则从图中数据分析，这种攻击可能属于下面什么攻击。

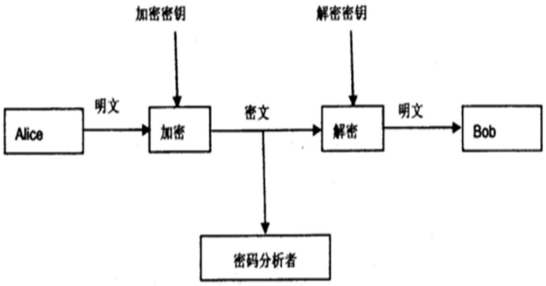


A. 跨站脚本攻击 B. TCP 会话劫持 C. IP 欺骗攻击 D. 拒绝服务攻击
答案：

86. 在 window 系统中用于显示本机各网络端口详细情况的命令是:
A. netshow B. netstat C. ipconfig D. Netview
答案：

87. 以下哪些问题或概念不是公钥密码体制中经常使用到的困难问题?
A、大整数分解 B、离散对数问题 C、背包问题 D、伪随机数发生器
答案：

88. 如下图所示，Alice 用 Bob 的密钥加密明文，将密文发送给 Bob，Bob 再用自己的私钥解密，恢复出明文以下说法正确的是：



A. 此密码体制为对称密码体制
B. 此密码体制为私钥密码体制
C. 此密码体制为单钥密码体制
D、此密码体制为公钥密码体制
答案：

89. 以下哪种公钥密码算法既可以用于数据加密又可以用于密钥交换?
A、DSS B、Diffie-Hellman C、RSA D、AES
答案：

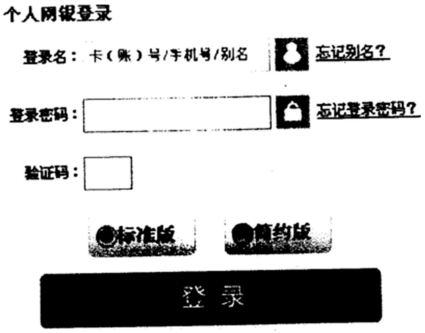
90. 在密码学的 Kerchhof 假设中，密码系统的安全性仅依赖于_____。

A．明文　　B．密文　　C．密钥　　D．信道
答案：

91. 在 Windows XP 中用事件查看器查看日志文件，可看到的日志包括？
A．用户访问日志、安全性日志、系统日志和 IE 日志　　C．网络攻击日志、安全性日志、记账日志和 IE 日志
B．应用程序日志、安全性日志、系统日志和 IE 日志　　D．网络链接日志、安全性日志、服务日志和 IE 日志
答案：

92. 操作系统安全的基础是建立在：
A、安全安装　　B、安全配置　　C、安全管理　　D、以上都对
答案：

93. 某用户通过账号，密码和验证码成功登陆某银行的个人网银系统，此过程属于以下哪一类：

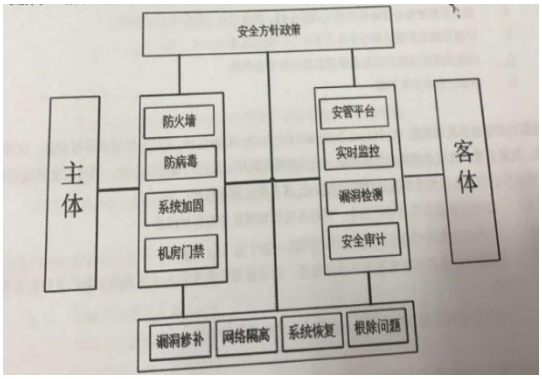


A. 个人网银和用户之间的双向鉴别　　C. 个人网银系统对用户身份的单向鉴别
B. 由可信第三方完成的用户身份鉴别　　D. 用户对个人网银系统 合法性 单向鉴别
答案：

94. windows 文件系统权限管理作用访问控制列表（Access Control List.ACL）机制，以下哪个说法是错误的：
A．安装 Windows 系统时要确保文件格式使用的是 NTFS,因为 Windows 的 ACL 机制需要 NTFS 文件格式的支持
B．由于 windows 操作系统自身有大量的文件和目录，因此很难对每个文件和目录设置严格的访问权限，为了作用上的便利，Windows 上的 ACL 存在默认设置安全性不高的问题
C．windows 的 ACL 机制中，文件和文件夹的权限是与主体进行关联的，即文件夹和文件的访问权限信息是写在用户数据库中
D．由于 ACL 具有很好的灵活性，在实际使用中可以为每一个文件设定独立的用户的权限答案：

95. 下列关于 kerckhof 准则的说法正确的是：
A、保持算法的秘密性比保持密钥的秘密性要困难的多　　B、密钥一旦泄漏，也可以方便的更换
C、在一个密码系统中，密码算法是可以公开的，密钥应保证安全　　D、公开的算法能够经过更严格的安全性分析
答案：

96. 小李是某公司系统规划师，某天他针对公司信息系统的现状，绘制了一张系统安全建设规划图，如下图所示。请问这个图形是依据下面哪个模型来绘制的（ ）



A. PDR　　B. PPDR　　C. PDCA　　D. IATF
答案：

97. 信息发送者使用_____进行数字签名。
A、己方的私钥　　B、己方的公钥　　C、对方的私钥　　D、对方的公钥

答案：

98. 根据 BEII—lapadula 模型安全策略，下图中写和读操作正确的是：

A.可读可写 B.可读不可写 C.可写不可读 D.不可读不可写
答案：

99. 以下列出了 MAC 和散列函数的相似性,哪一项说法是错误的？
A、MAC 和散列函数都是用于提供消息认证
B、MAC 的输出值不是固定长度的，而散列函数的输出值是固定长度的
C、MAC 和散列函数都不需要密钥
D、MAC 和散列函数都不属于非对称加密算法
答案：

1） MAC：消息验证、完整性校验、抗重放攻击；输出不固定的；MAC 需密钥；不是非对称。
2） 哈希：消息验证、完整性校验；输出是固定的；不需要密钥；不是非对称。

100. 操作系统是作为一个支撑软件,使得你的程序或别的应用系统在上面正常运行的一个环境。操作系统提供了多的管理功能,主要是管理系统的软件资源和硬件资源。操作系统软件自身的不安全性,系统开发设计的不周而下的破绽,都给网络安全留下隐患。某公司网络维护师为实现该公司操作系统的安全目标,按书中所学建立了的安全机制,这些机制不包括（）
A.标识与鉴别
B.访问控制
C.权限管理
D.网络云盘存取保护
答案：