信息安全技术

初赛题库

一、判断题

1. OSI 安全框架是对 OSI 安全体系结构的扩展。（对）
2. OSI 安全框架目标是解决“开放系统”中的安全服务。 （对）
3. OSI 安全框架中的安全审计框架目的在于测试系统控制是否充分 （对）
4. OSI 安全框架中的安全审计框架描述了如何通过访问控制等方法来保护敏感数据，提出了机密性机制的分类方法，并阐述了与其他安全服务和机制的相互关系。 （错）
5. 访问控制的一个作用是保护敏感信息不经过有风险的环境传送 （对）
6. 数据机密性就是保护信息不被泄漏或者不暴露给那些未经授权的实体 （对）
7. 数据机密性服务可分为两种：数据的机密性服务和业务流机密性服务。前者使得攻击者无法通过观察网络中的业务流获得有用的敏感信息；后者使得攻击者无法从获得的数据中获知有用的敏感信息。 （错）
8. 密码技术是信息安全的核心技术和支撑性基础技术，是保护信息安全的主要手段之一 （对）
9. 密码技术是信息安全的核心技术和支撑性基础技术，是保护信息安全的唯一手段 （错）
10. 在实践中，访问控制功能只能由某一特定模块完成 （错）
11. 访问控制机制介于用户(或者用户的某个进程)与系统资源(包括应用程序、操作系统、防火墙、路由器、文件以及数据库等)之间。 （对）
12. 访问控制的作用只能防止部分实体以任何形式对任何资源进行非授权的访问 （错）
13. 侧信道技术指利用密码设备在密码算法执行过程中产生的其他信息，如能量消耗变化、电磁辐射变化等非通信信道物理信息分析的硬件安全技术，主要分为能量分析、计时分析、错误注入和电磁泄漏等几大类攻击技术 （对）
14. 物理与硬件安全是相对于物理破坏而言的 （对）
15. 网络安全技术主要包括网络攻击技术和网络防御技术 （对）

16. 网络安全技术只包括网络防御技术 （错）

17. 网络安全技术为网络提供了安全，同时实现了对网络中操作的监管。 （对）

18. 任何信息网络存在的目的都是为某些对象提供服务，我们常常把这些服务称为应用。（对）

19. 应用安全技术是指以保护特定应用为目的的安全技术 （对）

20. 鉴别提供了关于某个实体(如人、机器、程序、进程等)身份的保证，为通信中的对等实体和数据来源提供证明。 （对）

21. 数据完整性，是指保证数据在传输过程中没有被修改、插入或者删除。数据完整性服务就是通过技术手段保证数据的完整性可验证、可发现。 （对）

22. 数据完整性是指保证数据在传输过程中没有被修改、插入或者删除。 （对）

23. 安全服务必须依赖安全机制来实现，OSI 安全体系结构中提出的安全机制中，数字签名和非否认服务无关 （错）

24. OSI 安全体系结构中提出的安全服务中，非否认服务的目的是在一定程度上杜绝通信各方之间存在相互欺骗行为，通过提供证据来防止这样的行为 （对）

25. OSI 安全体系结构中提出的安全机制中，加密能够实现数据机密性服务，同时也能提供对业务流的保密，并且还能作为其他安全机制的补充。 （对）

26. OSI 安全体系结构中提出的八大安全机制之一的认证交换没有利用密码技术 （错）

27. 数据机密性就是保护信息不被泄漏或者不暴露给那些未经授权的实体。 （对）

28. OSI 安全体系结构中提出的安全机制中，认证服务的核心不是密码技术 （错）

29. 除了 OSI 安全体系结构中提出的安全机制之外，还有五种普遍采用的安全机制，它们是可信功能模块(可信软硬件系统部件)、安全标记、事件检测、安全审计跟踪以及安全恢复。（对）

30. 不可以使用数字签名机制来实现对等实体认证安全服务 （错）

31. OSI 安全体系结构的一个非常重要的贡献是实现了安全服务与网络层次之间的对应关系，传输层可提供认证、访问控制和部分数据机密性及完整性安全服务。 （对）

32. 在各个网络层次中，应用层不可以提供安全服务 （错）

33. 物理层之上能提供完整的业务流机密性安全服务 （错）

34. 系统安全是对于各种软件系统而言的，一个只有硬件的计算机是不能直接使用的，它需要各种软件系统来支持。 （对）

35. 信息网络还有一个共有的特性——数据，数据可以是信息处理的对象、信息处理的结果，

也可以是信息处理产生的命令。　　（对）

36. 系统安全技术是信息安全技术体系结构之一，系统安全技术就是数据库系统安全技术　　（错）

37. 密码体制是密码技术中最为核心的一个概念　（对）

38. 密码体制被定义为两对数据变换　　（错）

39. 公钥密码体制有两种基本的模型：一种是加密模型；另一种是认证模型　（对）

40. 现有的加密体制分成对称密码体制是和非对称密码体制　　（对）

41. 对称密码体制的特征是加密密钥和解密密钥完全相同　（对）

42. 为了安全，对称密码体制完全依赖于以下事实：在信息传送之前，信息的发送者和授权接受者共享一些秘密信息(密钥)。　　（对）

43. 《密码学新方向》一文中首次提出了非对称密码体制的假想　　（对）

44. RSA 系统是当前最著名、应用最广泛的公钥系统，大多数使用公钥密码进行加密和数字签名的产品及标准使用的都是 RSA 算法　（对）

45. 公钥密码体制算法用一个密钥进行加密，而用另一个不同但是有关的密钥进行解密　　（对）

46. 加密模型中，通过一个包含各通信方的公钥的公开目录，任何一方都可以使用这些密钥向另一方发送机密信息。　（对）

47. 对称密码的优势包括未知实体间通信容易和保密服务较强。　　（错）

48. 公钥密码体制的密钥管理方便，密钥分发没有安全信道的限制，可以实现数字签名和认证　（对）

49. 密码算法是用于加密和解密的数学函数，是密码协议安全的基础　　（对）

50. 主流的对称密码算法主要有 DES(Data Encryption Standard)算法，3DES(Triple DES)算法和 AES(Advanced Encryption Standard)算法　（对）

51. 非对称密码算法有 RSA 算法， DSA 算法和 ECC 算法　（对）

52. 密钥封装(Key Wrap)是一种密钥存储技术 （错）

53. 1975 年发布的 Diffie－Hellman 密钥交换协议，可以在不安全的通信信道中进行密钥交换　（对）

54. 如果密钥进行了更新，旧的密钥可以保留　　（错）

55. 实现数据完整性必须满足两个要求：一是数据完整性应该能被消息的接收者所验证；二是数据完整性应该与消息相关，即消息不同，所产生的附件数据也应该不同。　　（对）

56. 基于 Hash 函数的 HMAC 方法可以用于数据完整性校验（对）

57. 利用带密钥的 Hash 函数实现数据完整性保护的方法称为 MD5 算法 （错）

58. 基于 Hash 的数字签名方法是目前常用的数字签名方法 （对）

59. 对称密码体制和公钥密码体制都可以用来实现数字签名。 （对）

60. 密码模块是硬件、软件、固件或其组合，它们实现了经过验证的安全功能，包括密码算法和密钥生成等过程，并且在一定的密码系统边界之内实现。 （对）

61. 我国密码行业标准 GM/T 0028－2014 标准规定了三个要求递增的安全等级 （错）

62. 我国密码行业标准 GM/T 0028－2014 标准规定的安全要求涵盖了有关密码模块的安全设计、实现、运行与废弃的安全元素(域)。 （对）

63. 密码模块包括密码算法和密钥生成等过程 （对）

64. 量子密码学使用量子力学属性来执行加密任务。 （对）

65. 国内提出的被动式监控方法，是对信源安全性方面的研究(信源安全性属于量子密钥分配安全性)，采用真随机数技术和信源监控技术，已经使用初步原理实验进行了实现。（对）

66. 量子密码学将数据编码到量子的状态中，复制数据编码的量子态和读取数据的编码将会改变量子的状态，使得通信双方可以发现数据被窃听 （对）

67. 量子密钥分配使得通信双方生成一个其他方不可获取的共享随机密钥，该密钥可用于双方通信加密。 （对）

68. 访问控制是计算机安全的核心元素。 （对）

69. 访问控制机制介于用户(或者用户的某个进程)与系统资源(包括应用程序、操作系统、防火墙、路由器、文件以及数据库等)之间。 （对）

70. 访问控制实现了一个安全策略，该策略规定某个实例(如一个用户或者一个进程)可以访问哪些特定的系统资源，以及每个实例的权限类型。 （对）

71. 所有操作系统都应至少有一个基本的访问控制组件 （对）

72. 访问控制的基本要素包括主体、客体和控制策略 （错）

73. 访问控制策略一般分为自主访问控制和强制访问控制 （对）

74. 在访问控制的基本要素中，主体是指能够访问对象的实体。 （对）

75. 在访问控制的基本要素中，主体是指被访问的资源 （错）

76. 在访问控制的基本要素中，客体是一类实体，即被访问的资源。 （对）

77. 在访问控制的基本要素中，客体是指能够访问对象的实体 （错）

78. 访问控制策略决定在哪些情况下、由什么主体发起、什么类型的访问是被允许的，一般可以用一个授权数据库来实现。 （对）

79. 访问控制策略一般无法用一个授权数据库来实现。 （错）

80. 自主访问控制是基于请求者的身份以及访问规则来进行访问控制的。 （对）

81. 强制访问控制是基于对客体安全级别(该级别标明客体的敏感度和关键性)与主体安全级别(该级别标明主体有资格访问哪些客体)的比较来进行访问控制的。 （对）

82. 自主访问控制是基于请求者的身份以及访问规则来进行访问控制的。自主访问控制的安全性相对较低 （对）

83. 自主访问控制是基于请求者的身份以及访问规则来进行访问控制的。自主访问控制的安全性相对较高 （错）

84. 在自主访问控制中，主体有权对自身创建的客体(文件、数据表等访问对象)进行访问，并可将对这些客体的访问权限授予其他用户，还可收回授予其他用户的访问权限。 （对）

85. 在自主访问控制中，每个主体对自己拥有的对客体的访问权限可以使用一维矩阵或者权限列表来表示。 （对）

86. 使用一维矩阵表示访问控制时，会产生比较大的空间浪费 （对）

87. 在自主访问控制中，使用权限列表表示访问控制时，会产生比较大的空间浪费,因此一维矩阵成为访问控制的另一种表示方式 （错）

88. 基于角色的访问控制是基于主体在系统中承担的角色进行的访问控制 （对）

89. 基于角色的访问控制从控制主体的角度出发，根据管理中相对稳定的职权和责任划分来分配不同的角色 （对）

90. 在基于角色的访问控制中，大多数情况下一个系统里的角色集合是相对静态的 （对）

91. TCSEC 中,类 D 中的级别 D1 是最高安全级别，类 A 中的级别 A1 是最低安全级别 （错）

92. TCSEC 定义了七个等级(D1、C1、C2、B1、B2、B3、A1) （对）

93. TCSEC 主要针对的是分时多用户操作系统 （对）

94. TCSEC 定义的七个等级(D1、C1、C2、B1、B2、B3、A1)可分为四个类别 （对）

95. 物理与硬件安全是运行于物理设备之上的系统安全的基础，分为环境安全和设备安全。前者强调构成系统本身的各种部件，后者强调一个系统所处的外界环境 （错）

96. 信息网络的物理安全要从环境安全和设备安全两个角度来考虑。 （对）

97. 保障物理运行环境中设备的安全称为信息网络安全的最后一道防线。 （错）

98. 物理安全，是指在物理介质层次上对存储和传输的网络信息的安全保护，也就是保护计算机网络设备、设施、其他媒体免遭地震、水灾、火灾等事故以及人为导致的破坏的过程。（对）

99. 计算机场地可以选择在公共区域人流量比较大的地方。 （错）

100. 计算机场地可以选择在化工厂生产车间附近。 （错）

101. 计算机机房供电线路和动力、照明用电可以用同一线路。 （错）

102. 备用电路板或者元器件、图纸文件必须存放在防静电屏蔽袋内，使用时要远离静电敏感器件。 （对）

103.屏蔽室是一个导电的金属材料制成的大型六面体，能够抑制和阻挡电磁波在空气中传播。（对）

104. 计算机场地在正常情况下温度保持在 18—28 摄氏度。 （对）

105. 信息网络所使用的电子设备，往往对水、潮气比较敏感，当湿度超过一定标准后，可能会造成电子设备生锈短路而无法使用，合适状态是将场地湿度控制在 40%—65%。 （对）

106. 信息系统场地应该保持比较稳定的适合电子设备运行的温度，温度过高有可能引起局部短路或者燃烧，所以应有相对的温度控制系统，最好是完备的中央空调系统。 （对）

107. 由于传输的内容不同，电力线可以与网络线同槽铺设。 （错）

108. 接地线在穿越墙壁、楼板和地坪时应套钢管或其他非金属的保护套管，钢管应与接地线做电气连通。 （对）

109. 静电对电子设备的危害是不容忽视的，大量的静电积聚可能会导致磁盘读写错误，磁头损坏，计算机误操作等现象。 （对）

110. 现代的整个电子通信都是建立在电磁信号的基础上，而电磁场的开放性决定了对电磁信号进行检测和防护的必要。否则，攻击者有可能通过电磁信号截获、分析来进行破坏和取得机密信息。 （对）

111. 辐射泄漏以电磁波的形式由空中辐射出去，由计算机内部的各种传输线、信号处理电路、时钟电路、显示器、开关电路及接地系统、印刷电路板线路等产生。 （对）

112. 传导泄漏以电磁波的形式由空中辐射出去，由计算机内部的各种传输线、信号处理电路、时钟电路、显示器、开关电路及接地系统、印刷电路板线路等产生。 （错）

113. 传导泄漏通过各种线路传导出去，可以通过计算机系统的电源线，机房内的电话线、地

线等都可以作为媒介。　　（对）

114. 接地线在穿越墙壁、楼板和地坪时应套钢管或其他非金属的保护套管，钢管应与接地线做电气连通。　　（对）

115. 在信息网络中设备本身的价值比较高，有些不法分子可能会为了经济利益而对设备进行偷盗、毁坏。机房外部的网络设备，应采取加固防护等措施，必要时安排专人看管，以防止盗窃和破坏。　　（对）

116. 为了信息网络的运行，设备本身需要具有一定的防潮能力，一些电子设备在出厂前就由厂家进行了专门的防潮处理，能够在较高的湿度环境下工作。　（对）

117. 设备防静电主要是从环境上进行防护，操作人员也要有防静电意识，按照规范操作。在设备上尽量采用防静电材料。　（对）

118. 为了信息网络运行的设备安全，新添设备时应该先给设备或者部件做上明显标记，最好是明显的无法除去的标记，以防更换和方便查找赃物。　　（对）

119. 在现代社会，信息往往具有很高的价值，一些恶意竞争者可能会对存储信息的设备进行恶意的偷盗或者毁坏。对于一些重要设备可以考虑使用一些加锁或者特制的机箱，进一步加强防盗保护。　　（对）

120. TEMPEST 技术（Transient Electro Magnetic Pulse Emanation Standard，瞬态电磁辐射标准），是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取防辐射措施，从而达到减少计算机信息泄漏的最终目的。　（对）

121. 防电磁泄漏的另一项技术是干扰技术，是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取防辐射措施，从而达到减少计算机信息泄漏的最终目的。　（错）

122. 计算机电磁辐射干扰器大致可以分为两种：白噪声干扰器和相关干扰器。　　（对）

123. 防电磁辐射的干扰技术，是指把干扰器发射出来的电磁波和计算机辐射出来的电磁波混合在一起，以掩盖原泄漏信息的内容和特征等，使窃密者即使截获这一混合信号也无法提取其中的信息。　　（对）

124. 防止电子设备产生传导干扰和辐射干扰最好的方法是采用金属机壳对电磁场进行屏蔽，以及对电源输入电路用变压器进行隔离，并且对变压器也进行静电感应和磁感应屏蔽。（对）

125. 传导干扰，主要是电子设备产生的干扰信号通过导电介质或公共电源线互相产生干扰。（对）

126. 辐射干扰，是指电子设备产生的干扰信号通过空间把干扰信号传给另一个电子网络或电子设备。　　（对）

127. 为了避免造成信息泄漏，纸介质资料废弃应用碎纸机粉碎或焚毁。　（对）

128. 保存重要数据和关键数据的各类介质在废弃后要进行正确处理，比如纸介质用碎纸机粉碎或焚毁，删除磁介质上的数据。　（错）

129. 在安全性要求比较高的地方，要安装各种监视设备。在重要场所的进出口安装监视器，并对进出情况进行录像，对录像资料妥善存储保管，以备事后追查取证。　　（对）

130. 为了分析密码模块能量消耗的变化，二阶/高阶 DPA(Differential Power Analysis，差分能量分析)使用了统计方法(如均值差、相关系数)对能量消耗进行统计分析，从而获取密钥值。　　（错）

131. 能量分析攻击可以分为两大类，即简单能量分析(Simple Power Analysis，简称 SPA)和差分能量分析(Differential Power Analysis，简称 DPA)。　（对）

132. 计时分析攻击依赖于密码模块执行时间的精确测量与密码算法或过程有关的特殊数学操作之间的关系。　　（对）

133. 计时分析攻击不依赖于密码模块执行时间的精确测量，但依赖于密码算法或过程有关的特殊数学操作之间的关系。　　（错）

134. 计时分析攻击假定攻击者具有有关密码模块的设计知识。　（对）

135. 错误注入攻击使用外部力量，如对微波、极端温度和电压的控制，引发密码模块内部运行错误。　　（对）

136. 错误注入攻击使用内部力量，如对微波、极端温度和电压的控制，引发密码模块内部运行错误。　　（错）

137. 电磁泄漏攻击，是指对正在运行的密码模块和辅助设备发出的电磁信号进行远程或外部探测和接收。　　（对）

138. 针对侧信道攻击（利用非通信信道物理信息如能量消耗变化、电磁辐射变化进行分析攻击），尽管学术界和工业界提出了很多防御技术，但是目前尚无能够抵抗所有攻击方法的防御技术。　　（对）

139. 电磁泄漏攻击可以获得敲击键盘的信息、显示屏上显示的消息，以及其他形式的关键安全信息。　　（对）

140. 固件是一种密码模块的可执行代码，它存储于硬件并在密码边界内，在执行期间能动态地写或修改。　　（错）

141. 在电子系统和计算机系统中，固件一般指持久化的内存、代码和数据的结合体。（对）

142. 存储固件的硬件可以包括但不限于 PROM、EEPROM、FLASH、固态存储器、硬盘驱动等。（对）

143. 固件的数据和代码一般是在密码产品出厂之前就写入硬件中的，而当写入固件的代码中存在恶意代码时，硬件固件攻击也将发生。（对）

144. 无线传感器网络是由大量静止或移动的传感器节点以自组织和单跳的方式组成的一种监测网络。（错）

145. 经过近几年学术界对无线传感器网络的深入研究，当前无线传感器网络面临多种攻击技术，其中路由攻击是指攻击节点依照路由算法伪造或重放一个路由声明，声称攻击节点和基站之间有高质量的单跳路由，然后阻止或篡改被攻击区域中任一节点发出的数据包。（错）

146. 当前无线传感器网络仍然面临面临着多种攻击技术。其中选择性数据转发攻击，是指攻击者截取并控制某个节点后，为了避免被发现该节点已被攻破，故仅丢弃应转发报文中的一部分。（对）

147. 当前无线传感器网络仍然面临面临着多种攻击技术。其中槽洞攻击是指向无线传感器网络中通过发送大量错误路由报文的方式，非法拦截篡改路由信息，使得各个节点接收到大量的错误路由信息，从而降低整个网络的有效传输速度。（错）

148. 当前无线传感器网络仍然面临面临着多种攻击技术。其中虫洞攻击，是指两个或多个攻击节点进行的一种合谋攻击，通过压缩攻击节点间的路由，使得彼此成为邻居节点，从而将不同分区的节点距离拉近，破坏整个网络的正常分区。（对）

149. 当前无线传感器网络仍然面临面临着多种攻击技术。其中女巫攻击，是指攻击节点伪装成具有多个身份标识的节点，当通过该节点的一条路由遭到破坏时，网络会选择另一条路由，但由于其具有多重身份标识，实际上还是通过了该攻击节点。（对）

150. 当前无线传感器网络仍然面临面临着多种攻击技术。其中 Hello 洪泛攻击，是指攻击节点向全网广播 Hello 报文，网络中的节点收到 Hello 报文之后，使得每一个节点误以为攻击节点是自己的邻居节点。（对）

151. 网络攻击类型多种多样，且出现频繁、规模较大，如何有效阻止网络攻击，保护网络安全，成为网络安全技术的研究内容。网络安全技术是解决如何有效进行介入控制、如何保证数据传输的安全性等安全问题。（对）

152. 随着计算机技术的不断革新，网络攻击手段持续翻新，网络攻击备受攻击者青睐。因此网络安全成为个人用户、企事业单位乃至国家机关都非常重视的安全领域。网络安全技术，是指由网络管理者采用的安全规则和策略，用以防止和监控非授权的访问、误用、窃听、篡改计算机网络和对可访问资源的拒绝服务等行为　（对）

153. 网络攻击方式多种多样，从单一方式向多方位、多手段、多方法结合化发展。网络攻击根据攻击效果的不同可以分为四大类型。其中常见的拒绝服务攻击是对网络系统可用性的破坏　（对）

154. 通常，网络安全与网络攻击是紧密联系在一起的，网络攻击是网络安全研究中的重要内容，在进行网络安全研究的同时，也需要对网络攻击有所了解。常见的网络攻击多是攻击者利用网络通信协议(如 TCP/IP、HTTP 等)自身存在或因配置不当而产生的漏洞而发生的　（对）

155. 网络攻击方式多种多样，从单一方式向多方位、多手段、多方法结合化发展。网络攻击根据攻击效果的不同，基本可抽象划分为信息泄漏攻击、完整性破坏攻击、拒绝服务攻击和非法使用攻击四大类型。　（对）

156. 网络攻击根据攻击效果的不同可以分为四大类型。其中拒绝服务攻击是指攻击者在非授权的情况下，使用计算机或网络系统服务，从而使得网络系统提供错误的服务。　（错）

157. 网络攻击根据攻击效果的不同可以分为四大类型。其中非法使用攻击，是指攻击者通过强制占用有限的资源，如信道/带宽、存储空间等资源，使得服务器崩溃或资源耗尽而无法对外继续提供服务。　（错）

158. 网络攻击根据攻击效果的不同可以分为四大类型。其中完整性破坏攻击，是指攻击者在非授权的情况下，对用户的信息进行修改，如修改电子交易的金额。　（对）

159. 网络攻击根据攻击效果的不同可以分为四大类型。其中信息泄漏攻击，是指攻击者在非授权的情况下，非法获取用户的敏感信息　（对）

160. 网络攻击实施过程中涉及了多种元素。其中安全漏洞一般是程序漏洞，不可能是设计缺陷　（错）

161. 网络攻击实施过程中涉及了多种元素。其中攻击访问，是指攻击者对目标网络和系统进行合法、非法的访问，以达到针对目标网络和系统的非法访问与使用　（对）

162. 网络攻击实施过程中涉及了多种元素。其中攻击效果包括对网络系统和信息的机密性、完整性、可用性、可靠性和不可否认性的破坏　（对）

163. 网络攻击实施过程中涉及了多种元素。其中攻击意图包括挑战、获取情报、发动恐怖事

件、好奇、获取经济利益、报复等。　　（对）

164. 网络防御技术，是指为了确保网络系统的抗攻击能力，保证信息的机密性、完整性、可用性、可靠性和不可否认性而采取的一系列的安全技术　　（对）

165. 防火墙是网络防御技术中一个重要组成部分。它是一个只由计算机软件组成的系统，部署于网络边界，是内部网络和外部网络之前的连接桥梁　　（错）

166. 加密技术是网络防御技术中一个重要组成部分，它通过对数据进行某种变换，任意用户都能完成数据的反变换，恢复数据的明文形式，保证数据在传输、共享、存储过程中的安全。　　（错）

167. 网络攻击的方法、手段层出不穷，技术不断发展，难度也越来越大，网络防御也面临同样的问题，需要不断更新，才能更好地保障网络系统与信息的安全。其中备份容错技术通过将关键数据备份(本地备份、异地备份)，能够在系统瘫痪、数据错误、发生灾难后，及时按预定数据恢复系统程序和数据，尽量减少损失。　　（对）

168. 防火墙按照概念划分，可分为四大类。其中包过滤防火墙支持对用户身份进行高级认证机制　　（错）

169. 基于软件的应用代理网关防火墙工作在应用层　　（对）

170. 应用代理网关防火墙具有审计跟踪和报警功能　　（对）

171. 状态检测防火墙通过建立动态 TCP 连接状态表对每次会话连接进行验证来实现网络访问控制功能。　　（对）

172. 防火墙按应用部署位置划分，可以分为边界防火墙、个人防火墙和分布式防火墙三大类。边界防火墙是传统的位于内部网络和外部网络边界的防火墙，作用是对内部网络和外部网络进行隔离，实施访问控制策略，从而保护内部网络。　　（对）

173. 防火墙按照软硬件结构划分，可以分为软件防火墙、硬件防火墙和芯片级防火墙三大类。芯片级防火墙通过专门设计的 ASIC 芯片逻辑进行软件加速处理。　　（错）

174. 网络处理器(Network Processor，简称 NP)是专门为处理网络数据包而设计的可编程处理器，其特点是内含多个数据处理引擎。基于网络处理器架构的防火墙上运行的操作系统通常是实时操作系统。　　（对）

175. 防火墙的目的是在内部网络和外部网络连接之间建立一个安全控制点，允许、拒绝或重新定向经过防火墙的数据流，实现对进出内部网络的网络通信的审计和控制。防火墙的通信带宽越宽，性能越低。　　（错）

176. 防火墙除了提供传统的访问控制功能外，或多或少地实现了一些增值功能，网络地址转

换便是其中之一。网络地址转换是用于将多个地址域映射到另一个地址域的标准方法（错）

177. 防火墙除了提供传统的访问控制功能外，或多或少地实现了一些增值功能，虚拟局域网便是其中之一。虚拟局域网是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术　　（对）

178. 防火墙除了提供传统的访问控制功能外，或多或少地实现了一些增值功能，双机热备便是其中之一。双机热备是在同一个网络节点使用两台配置相同的防火墙，一台作为主防火墙，处于正常工作状态，另一台作为备份机。　　（对）

179. 防火墙除了提供传统的访问控制功能外，或多或少地实现了一些增值功能，譬如防火墙能消除来自内部的威胁。　（错）

180. 防火墙策略不但指出防火墙处理诸如 Web、Email 或 Telnet 等应用程序通信的方式，还描述了防火墙的管理和更新方式。防火墙处理入站通信的缺省策略应该是阻止所有的数据包和连接　（对）

181. 大多数防火墙平台都使用规则集作为它们执行安全控制的机制。规则集的内容决定了防火墙的真正功能。防火墙规则集随着时间的增加会变得越来越简单　（错）

182. 防火墙是设置在内部网络与外部网络(如互联网)之间，实施访问控制策略的一个或一组系统，是访问控制机制在网络安全环境中的应用。防火墙应该阻止包含源路由的所有入站和出站数据包。　　（对）

183. 防火墙是设置在内部网络与外部网络(如互联网)之间，实施访问控制策略的一个或一组系统，是访问控制机制在网络安全环境中的应用。防火墙应该阻止包含直接广播地址的所有入站和出站数据包。　（对）

184. 部署防火墙环境时，绝不可将外部网络可访问的服务器放置在内部保护网络中（对）

185. 部署防火墙环境时，内部网络可以无限制地访问外部网络以及 DMZ　（对）

186. 部署防火墙环境时，DMZ 可以访问内部网络　（错）

187. 部署防火墙环境时，内部 DMZ 作为内外网络之间的一个联系点，必须位于两个防火墙之间　　（对）

188. 入侵检测(Intrusion Detection)技术是用于检测任何损害或企图损害系统的机密性、完整性或可用性等行为的一种网络安全技术　（对）

189. 入侵检测系统(IDS)由硬件和软件组成，用来检测系统或网络，以发现可能的入侵或攻击

的系统。　　（对）

190. 入侵检测(Intrusion Detection)技术是用于检测任何损害或企图损害系统的机密性、完整性或可用性等行为的一种网络安全技术。入侵检测系统不能使系统对入侵事件和过程作出实时响应。　　（错）

191. 入侵防御系统(IDS)提供一种被动的、实时的防护　（错）

192. 入侵检测是系统动态安全的核心技术之一。入侵检测系统能够单独防止攻击行为的渗透　　（错）

193. 基于网络的入侵检测系统一般通过在网络的数据链路层上进行监听来获得信息。企业部署基于网络的入侵检测系统时，必须确定入侵检测传感器的部署位置　　（对）

194. 入侵防御系统提供一种主动的、实时的防护，其设计旨在对常规网络通信中的恶意数据包进行检测，阻止入侵活动，预先对攻击性的数据包进行自动拦截，使它们无法造成损失，而不是简单地在检测到网络入侵的同时或之后进行报警。入侵检测系统的准确性主要包括三个指标，即检测率、误报(False Positive)率和漏报(False Negative)率　（对）

195. 入侵检测系统可以弥补安全防御系统中的安全漏洞和缺陷　（错）

196. 入侵防御系统是一种智能化的网络安全产品，不但能检测入侵行为的发生，而且能通过一定的响应方式，实时中止入侵行为的发生和发展，实时保护信息系统不受实质性的攻击。入侵防御系统使得入侵检测系统和防火墙走向了统一。只有以在线模式运行的入侵防御系统才能够实现实时的安全防护　　（对）

197. 基于网络的入侵防御系统可以基于任意的硬件平台　　（错）

198. 基于主机的入侵防御系统通过在主机和服务器上安装软件程序，防止网络攻击入侵操作系统以及应用程序。　（对）

199. 入侵防御系统实现实时检查和阻止入侵的原理在于其拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，入侵防御系统会创建一个新的过滤器。入侵防御系统可以用相同的过滤器针对不同的攻击行为　（错）

200. 网络安全扫描不仅能够扫描并检测是否存在已知漏洞，还可以发现一些可疑情况和不当配置　　（对）

201. 网络漏洞的存在实际上就是潜在的安全威胁，一旦被利用就会带来相应的安全问题。攻击者常采用网络漏洞扫描技术来探测漏洞，一旦发现，便可利用其进行攻击。通常所说的网络漏洞扫描，实际上是对网络安全扫描技术的一个俗称。　（对）

202. 基于网络的漏洞扫描器很容易穿过防火墙　　（错）

203. 基于网络的漏洞扫描器不能直接访问目标设备的文件系统，不能检测一些相关的漏洞。（对）

204. 基于主机的漏洞扫描器扫描目标设备漏洞的原理与基于网络的漏洞扫描器的原理不同，但二者的体系结构相似。 （错）

205.主机安全扫描技术一般是在主机上本地进行的，大部分情况下需要有主机的管理员权限。基于主机的漏洞扫描器一般采用客户机/服务器架构。 （对）

206. 基于网络的漏洞扫描器不包含网络映射功能 （错）

207. 漏洞(Vulnerability)，也叫脆弱点，是指在计算机硬件、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。漏洞数据库包含了各种操作系统的漏洞信息以及如何检测漏洞的指令。 （对）

208. 基于主机的漏洞扫描工具不需要在目标主机上安装一个代理或服务 （错）

209. 现在流行的漏洞扫描工具，根据其使用场合一般分为两大类：基于网络的漏洞扫描器和基于主机的漏洞扫描器。基于主机的漏洞扫描器通常会配置一个集中服务器作为扫描服务器，所有扫描的指令均通过服务器进行控制。 （对）

210. 网络安全扫描技术与防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。基于网络的漏洞扫描器能直接访问目标设备的文件系统 （错）

211. 基于网络的漏洞扫描器，就是通过网络来扫描远程计算机中的漏洞。基于网络的漏洞扫描器在操作过程中，不需要涉及目标设备的管理员 （对）

212. 网闸，又称安全隔离与信息交换系统，是使用带有多种控制功能的固态开关读写介质，连接两个独立网络的信息安全设备。网闸是一种采用硬件卡隔离方式的安全防护技术（错）

213. 网闸是一种采用物理隔离方式的安全防护技术。网闸技术是在保证两个网络安全隔离的基础上实现安全信息交换和资源共享的技术 （对）

214. 数据转播隔离利用转播系统分时复制文件的途径来实现隔离，即隔离设备首先与一端连通，将流入的数据复制并缓存，然后切断该端连通另一端，将数据发送出去。数据转播隔离不需要手工完成 （错）

215. 网闸，又称安全隔离与信息交换系统，是使用带有多种控制功能的固态开关读写介质，连接两个独立网络的信息安全设备。网闸一般由三部分构成，即内网处理单元、外网处理单元和专用隔离硬件交换单元。 （对）

216. 网闸，又称安全隔离与信息交换系统，是使用带有多种控制功能的固态开关读写介质，

连接两个独立网络的信息安全设备。第二代网闸不需要通过应用层数据提取与安全审查达到杜绝基于协议层的攻击和增强应用层安全效果。　（错）

217. 网闸从物理上隔离和阻断了具有潜在攻击可能的一切连接，使得黑客难以入侵、攻击和破坏，实现了高程度的安全。网闸一般由三部分构成，即内网处理单元、外网处理单元和专用隔离硬件交换单元。　（对）

218. 第一代网闸利用单刀双掷开关使得内外网的处理单元分时存取共享存储设备来完成数据交换，实现了在物理隔离情况下的数据交换。　（对）

219. 目前，国产的网闸产品可以满足可信网络用户与外部的文件交换、收发邮件、单向浏览、数据库交换等功能，同时已在电子政务中得到应用。在电子政务系统建设中要求在政府内网与外网之间用物理隔离，在政府内网与专网之间用逻辑隔离。　（错）

220. 拒绝服务攻击对于网络服务的可用性造成了致命性打击，它通常可以在短时间内造成被攻击主机或者网络的拥塞，使合法用户的正常服务请求无法到达服务网络中的关键服务器。智能的拒绝服务攻击工具可以实现多对一或者多对多的攻击方式　（对）

221. 拒绝服务攻击目前主要有五种攻击模式，其中分布式反射拒绝服务(Distributed Reflection Denial of Service，简称 DRDoS)攻击的原理是利用了 TCP 协议　（错）

222. 拒绝服务攻击的原理很简单，即充分利用合理的 TCP 来完成攻击的目的，目前，主要有五种攻击模式。分布式拒绝服务(DDoS)攻击是洪泛式拒绝服务攻击中一种更具威胁性的演化版本，它利用互联网集中式连接的特点　（错）

223. 拒绝服务攻击的目的是利用各种攻击技术使服务器或者主机等拒绝为合法用户提供服务。　（对）

224. Botnet 网络在国内大都被翻译为“僵尸网络”。Botnet 泛滥的一个直接结果就是它可以被用来发起超大规模的 DDoS 攻击，而且 Botnet 已经在网上被公开销售或者租用。　（对）

225. Botnet 网络在国内大都被翻译为“僵尸网络”。除了被用于组织 DDoS 攻击，Botnet 还可以被用来传播垃圾邮件、窃取用户数据、监听网络和扩散恶意病毒等。　（对）

226. Botnet 网络在国内大都被翻译为“僵尸网络”。Botnet 的显著特征是大量主机在用户不知情的情况下，被植入了控制程序，并且有一个地位特殊的主机或者服务器能够通过信道来控制其他的主机，这些被控制的主机就像僵尸一样听从主控者的命令。　（对）

227. 拒绝服务攻击与 Botnet 网络结合后攻击能力大大削弱　（错）

228. 流量控制是在网络流量达到一定阈值时，按照一定的算法丢弃所有报文　（错）

229. 目前，很多产品都声称可以检测和抵御拒绝服务攻击，这些方法虽然不能完全解决拒绝

服务攻击问题，但是可以在某种程度上检测或者减轻攻击的危害，最大限度地保证在攻击发生时，还能够为部分用户提供服务。Blackholing 技术实际上就是在攻击发生时将所有发往攻击目标的数据包抛弃　　（对）

230. 目前，很多产品都声称可以检测和抵御拒绝服务攻击，这些方法虽然不能完全解决拒绝服务攻击问题，但是可以在某种程度上检测或者减轻攻击的危害，最大限度地保证在攻击发生时，还能够为部分用户提供服务。Random Drop 技术抛弃所有发往攻击目标的数据包　　（错）

231. 流量控制是在网络流量达到一定阈值时，按照一定的算法丢弃部分报文　（对）

232. 认证是最重要的安全服务，其他安全服务在某种程度上需要依赖于它。　（对）

233. 保护数据安全的技术主要可分为两大类：一是采用密码技术对数据本身进行保护，如使用现代加密算法对数据进行加密以获得机密性，采用数字签名算法确保数据源的可靠性，采用杂凑算法和公钥算法保护数据完整性等；二是数据防护技术，通过在信息系统中应用相应的安全技术来保护数据本身免受破坏，　（对）

234. RADIUS 是利文斯顿事业(Livingston Enterprises)公司开发的一种网络协议。该协议为网络服务用户提供集中式的 AAA(认证、授权、账户)管理。IPS 和企业普遍采用 RADIUS 进行网络接入管理。它是主流身份鉴别协议　（对）

235. 安全性断言标记语言(Security Assertion Markup Language，简称 SAML)是一个基于 XML 的标准，用于在不同的安全域(security domain)之间交换认证和授权数据。它是主流身份鉴别协议　（对）

236. FIDO 是一种不依赖于口令来执行身份鉴别的协议规范。其协议针对不同的用户实例和应用场景，提供了两类不同的认证方式，即通用授权框架(Universal Authentication Framework，简称 UAF)和通用第二因素认证(Universal Second Factor，简称 U2F)。它是主流身份鉴别协议　（对）

237. Kerberos 是 MIT 研发的一种计算机网络认证协议，依赖于可信的第三方来生成票据以实现安全的认证。该协议面向客户端/服务器模型，能够在非安全的网络环境中提供双向认证。　（对）

238. Kerberos 是 MIT 研发的一种计算机网络认证协议，依赖于第三方来生成票据以实现安全的认证。目前，Windows 2000 及其后续操作系统、Mac OS X、Redhat Enterprise Linux 4 及其后续操作系统均用到了 Kerberos 认证协议。　（对）

239. Kerberos 能够在非安全的网络环境中提供双向认证　（对）

240. Kerberos 能够在非安全的网络环境中提供单向认证　　（错）

241. Kerberos 不是面向客户端/服务器模型　　（错）

242. Kerberos 是面向客户端/服务器模型　（对）

243. Kerberos 在协议过程中，对传输的消息采用对称加密算法加密，能够提高数据的机密性和完整性　　（对）

244. Kerberos 在协议过程中，对传输的消息采用非对称加密算法加密，能够提高数据的机密性和完整性　（错）

245. RADIUS 协议为网络服务用户提供集中式的 AAA(认证、授权、账户)管理，RADIUS 是一种面向客户端/服务器模型的协议　　（对）

246. RADIUS 为网络服务用户提供集中式的 AAA(认证、授权、账户)管理，RADIUS 不是面向客户端/服务器模型的协议　（错）

247. OpenID 是一种去中心化的以用户为中心的数字身份识别框架　　（对）

248. OpenID 是一种开放的服务，不需要一个中心的身份服务提供商，任何应用服务提供商都可以实现自己的 OpenID 服务，用户可以自由地选择在其信任的服务提供商处注册账号，并利用该 OpenID 服务登录访问所有支持该 OpenID 服务的第三方应用。（对）

249. OpenID 框架的核心是 OpenID 身份鉴别协议　（对）

250. OpenID 身份鉴别协议包括三个实体，即依赖方(RP)、终端用户、OpenID 提供方。　　（对）

251. OpenID 提供方的功能是身份鉴别和授权　（对）

252. OpenID 提供方的功能是鉴别　　（错）

253. OpenID 身份鉴别协议的参与方没有远程控制方　　（对）

254. OpenID 身份鉴别协议的参与方没有提供方　　（错）

255. OpenID 身份鉴别协议的参与方有提供方　（对）

256. OpenID 身份鉴别协议的参与方没有依赖方　　（错）

257. OpenID 身份鉴别协议的参与方有依赖方　（对）

258. 安全性断言标记语言是一个基于 XML 的标准，用于在不同的安全域(security domain)之间交换认证和授权数据。SAML 应用的实现由主体、服务提供者和身份提供者组成　（对）

259. SAML 应用的实现由主体、客体和身份提供者组成。　　（错）

260. SAML 应用的实现没有服务提供者。（错）

261. SAML 应用的实现没有身份提供者。（错）

262. SAML 应用的实现有服务提供者。　（对）

263. SAML 应用的实现有身份提供者。　（对）

264. SAML 就是一方向另一方发送 SAML 请求，然后另一方返回 SAML 响应。数据的传输以符合 SAML 规范的 XML 格式表示。连接中的任何一方都可以发起请求，根据身份不同，可以说是 IDP init 请求，或是 SP init 请求。（对）

265. SAML 应用的实现有主体。（对）

266. 在 SAML 协议通信中，通信实体之间只要存在信任关系，符合 SAML 接口和消息交互定义以及应用场景，就可相互通信。　（对）

267. 在 SAML 协议通信中，通信实体之间存在信任关系，符合 SAML 接口和消息交互定义以及应用场景，也可能不能相互通信。　（错）

268. FIDO 是一种不依赖于口令来执行身份鉴别的协议规范 （对）

269. FIDO 是一种依赖于口令来执行身份鉴别的协议规范　（错）

270. FIDO 协议使用标准的公钥密码技术提供强认证　（对）

271. FIDO 协议使用对称密码技术提供强认证 （错）

272. FIDO 协议中客户端的私钥只有在本地解锁后才能使用 （对）

273. FIDO 协议中客户端的私钥不解锁也能使用　（错）

274. 联合身份认证是将身份认证委托给外部身份提供者来完成认证的机制。　（对）

275. 联合身份认证是将身份认证委托给本地身份提供者来完成认证的机制。　（错）

276. PKI 是利用公开密钥技术所构建的、解决网络安全问题的、普遍适用的一种基础设施。（对）

277. PKI 是利用私钥技术所构建的、解决网络安全问题的、普遍适用的一种基础设施。（错）

278. PKI 通过延伸到用户本地的接口为各种应用提供安全的服务 （对）

279. PKI 通过服务器的接口为各种应用提供安全的服务 （错）

280. 数字证书根据其用途可以分为加密证书和签名证书　（对）

281. 数字证书根据其用途可以分为加密证书、签名证书和评估证书 （错）

282. 数字证书就是一个公钥信息和身份信息绑在一起、用 CA 的私钥签名后得到的数据结构（对）

283. 数字证书就是一个私钥信息和身份信息绑在一起、用 CA 的公钥签名后得到的数据结构（错）

284. 加密证书用来加密数据；签名证书用来证明身份 （对）

285. 加密证书用来加密数据；签名证书用来解密数据 （错）

286. 数字证书根据其用途可以分为解密证书和加密证书 （错）

287. 数字证书是将主体信息和主体的公开密钥通过 CA 的数字签名绑定在一起的一种数据结构。数字证书本身是可验证的，而且数字证书具有标准的格式。 （错）

288. PKI 提供的核心服务包括认证、完整性、密钥管理、简单机密性和非否认。这几项核心服务囊括了信息安全四个重要的要求，即真实性、完整性、保密性和不可否认性。（对）

289. PKI 利用对称的算法，提供密钥协商能力。同时，PKI 利用证书机构等提供密钥管理和简单的加密服务。 （错）

290. 数字证书本身是可验证的，而且数字证书具有标准的格式 （对）

291. 数字证书本身是不可验证的 （错）

292. 数字证书是由权威机构证书授权中心发行的，人们可以在网上用它来识别对方的身份。数字证书具有标准的格式。 （对）

293. 数字证书不具有标准的格式。 （错）

294. PKI 提供的核心服务包括认证、完整性、密钥管理、简单机密性和非否认。 （对）

295. PKI 提供的核心服务不包括认证 （错）

296. PKI 提供的核心服务包括认证 （对）

297. PKI 提供的核心服务不包括非否认。 （错）

298. PKI 提供的核心服务包括非否认。 （对）

299. PKI 提供的核心服务不包括完整性。 （错）

300. PKI 提供的核心服务包括完整性 （对）

301. PKI 提供的核心服务不包括密钥管理 （错）

302. PKI 提供的核心服务包括密钥管理。 （对）

303. PKI 提供的核心服务不包括简单机密性 （错）

304. PKI 提供的核心服务包括简单机密性。 （对）

305. PKI 是利用公开密钥技术所构建的、解决网络安全问题的、普遍适用的一种基础设施。PKI 提供的服务包括两个部分：基本服务和安全服务。 （对）

306. PKI 只提供安全服务。 （错）

307. PKI 只提供基础服务。 （错）

308. PKI 提供的完整性可以通过数字签名来完成，而这种完整性还提供了对称密码方法等不能提供的不可否认保障。 （对）

309. PKI 提供的完整性可以通过数字签名来完成，而这种完整性还提供了不对称密码方法等不能提供的不可否认保障。 （对）

310. PKI 利用非对称的算法，提供密钥协商能力。 （对）

311. PKI 利用对称的算法，提供密钥协商能力。 （错）

312. VPN 的基本思想是采用秘密通信通道，通过 PKI 的认证后，用加密的方法来实现保密、完整的通信。 （对）

313. VPN 的基本思想是采用公开通信通道，通过 PKI 的认证后，用加密的方法来实现保密、完整的通信。 （错）

314. 数字版权保护(Digital Right Management，简称 DRM)是指对数字知识产权的控制和管理。 （对）

315. 数字版权保护(Digital Right Management，简称 DRM)只涉及数字知识产权的控制。 （错）

316. DRM(Digital Right Management，数字版权保护）只涉及数字知识产权的管理 （错）

317. 基于客户端—服务器的数字版权管理系统中内容提供方必须有专用于管理内容供应的服务器。 （对）

318. 基于客户端—服务器的数字版权管理系统中内容提供方不必有专用于管理内容供应的服务器。 （错）

319. 基于 P2P 的数字版权管理系统不需要依靠服务器分发内容。 （对）

320. 基于 P2P 的数字版权管理系统需要依靠服务器分发内容。 （错）

321. 数字版权保护(Digital Right Management, 简称 DRM)系统需要对内容进行持续地保护，即持续地保护已经存在的内容。 （对）

322. 数字版权保护(Digital Right Management，简称 DRM)系统不需要对内容进行持续地保护。 （错）

323. 对 DRM(Digital Right Management，数字版权保护）的内容进行加密通常使用对称加密技术和非对称加密技术。 （对）

324. 对 DRM(Digital Right Management，数字版权保护）的内容进行加密只使用对称加密技术。 （错）

325. 对 DRM(Digital Right Management，数字版权保护）的内容进行加密只使用非对称加密

技术。　（错）

326. 在 DRM(Digital Right Management，数字版权保护）系统中，数字签名通常用于标记用户是否已购买授权。　（对）

327. 在数字版权保护(Digital Right Management，简称 DRM)系统中，数字签名不能用于标记用户是否已购买授权。　（错）

328. 在数字版权保护(Digital Right Management，简称 DRM)系统中，单向散列函数结合数字签名可以对内容进行完整性检验。　（对）

329. 在数字版权保护(Digital Right Management，简称 DRM)系统中，单向散列函数结合数字签名不可以对内容进行完整性检验。　（错）

330. 在 DRM 系统中，数字证书被用来验证或鉴别系统中涉及的实体身份。　（对）

331. 在数字版权保护(Digital Right Management，简称 DRM)系统中，数字证书不能用来验证或鉴别系统中涉及的实体身份。　（错）

332. 鲁棒水印的特点是改变嵌入水印的数据内容不会影响其中嵌入的水印信息。　（对）

333. 鲁棒水印的特点是改变嵌入水印的数据内容会破坏其中嵌入的水印信息。　（错）

334. 脆弱水印的特点是改变嵌入水印的数据内容不会影响其中嵌入的水印信息　（错）

335. 脆弱水印的特点是改变嵌入水印的数据内容会破坏其中嵌入的水印信息。　（对）

336. networking－layer 和 content－layer 的数据设置比较宽松，其数据可能会被用于多种目的　（对）

337. networking－layer 和 content－layer 的数据设置比较严格，其数据不能用于多种目的　（错）

338. 容灾，就是减少灾难事件发生的可能性以及限制灾难对关键业务流程所造成的影响的一整套行为　（对）

339. 恢复点目标 RPO 代表了当灾难发生后，数据的恢复程度和恢复时数据未丢失、正确且可用的数量。　（对）

340. 服务降级目标 SDO 代表了当灾难发生后，数据的恢复程度和恢复时数据未丢失、正确且可用的数量。　（错）

341. 服务降级目标 SDO 代表了灾难发生后业务恢复的程度，包括功能、性能的恢复，支持的用户数量等。　（对）

342. 恢复点目标 RPO 代表了灾难发生后业务恢复的程度，包括功能、性能的恢复，支持的用户数量等。　（错）

343. SHARE78 将容灾系统定义成七个层次。 （对）

344. SHARE78 将容灾系统定义成六个层次。 （错）

345. 备份系统的选择的原则是以很低的系统资源占用率和很少的网络带宽来进行自动而高速的数据备份。 （对）

346. 备份系统的选择的原则是以很高的系统资源占用率和很少的网络带宽来进行自动而高速的数据备份。 （错）

347. 备份系统的选择的原则是以很高的系统资源占用率和很高的网络带宽来进行自动而高速的数据备份。 （错）

348. 备份系统的选择的原则是以很低的系统资源占用率和很高的网络带宽来进行自动而高速的数据备份。 （错）

349. 进行系统数据备份的原因是尽量在系统崩溃以后能快速、简单、完全地恢复系统的运行。（对）

350. 系统数据备份，是指对与用户个人相关的一些应用数据的备份。 （错）

351. 累计备份与增量备份不同之处在于：增量备份是备份该天更改的数据，而累计备份的对象是从上次进行完全备份后更改的全部数据文件。 （对）

352. 累计备份，是指备份从上次进行完全备份后更改的全部数据文件。 （对）

353. 增量备份，是指备份从上次进行完全备份后更改的全部数据文件。 （错）

354. 累计备份，是指备份从该天更改的全部数据文件。 （错）

355. 同源安全策略要求来自不同源的“document”或脚本只能读取或设置当前“document”的某些属性。 （对）

356. 浏览器沙箱技术让不受信任的网页代码、JavaScript 代码在一个受到限制的环境中运行，从而保护本地桌面系统的安全。 （对）

357. 根据同源安全策略，a.com 网页中的脚本只能修改 a.com 网页中的内容。（对）

358. 如果没有同源安全策略，那么，当用户通过浏览器访问了某个恶意网站时，浏览器中同时打开的其他网页都是不安全的，恶意网站可以通过 JavaScript 脚本获取用户在其他网站上的用户信息、登录信息等。 （对）

359. 浏览器沙箱技术让不受信任的网页代码、JavaScript 代码在一个受到限制的环境中运行，从而保护本地桌面系统的安全。 （对）

360. 所有浏览器在沙箱基础上采用了多进程架构。 （错）

361. Cookie 是网站用于身份认证和会话跟踪而存储在用户本地终端上的数据。当用户需要

访问该网站时，需要将 Cookie 发送给服务端。　　（对）

362. Cookie 的数据是加密的，内容主要为 MD5 加密信息，包括用户 ID、有效时间等。（对）

363. 为了确保 Cookie 的安全，网站服务器应该为关键 Cookie 设置 HttpOnly 属性。通过设置 HttpOnly 属性，浏览器将禁止页面的 JavaScript 访问带有 HttpOnly 属性的 Cookie。（对）

364. 通过内容安全策略(Content Security Policy，简称 CSP)，开发者可以指定自己页面上的图片可以来自哪些网站，网页中可以加载哪些网址的 JavaScript 代码。。　（对）

365. 通用网关界面(Common Gateway Interface，简称 CGI)可以在网络服务器中运行内部应用程序。　　（错）

366. 跨站脚本攻击是常见的 Cookie 窃取方式。　　（对）

367. 跨站脚本攻击的危害是可以让攻击者绕过 Web 上的权限控制，通过间接的方式执行越权操作。　　（错）

368. 跨站请求伪造攻击的主要危害就是可以让攻击者绕过 Web 上的权限控制，通过间接的方式执行越权操作。　（对）

369. 用户访问网页时，所有的请求都是通过 HTTP 请求实现的。（对）

370. 用户访问网页时，所有的请求都是通过 HTTP GET 请求实现的。（错）

371. 在跨站请求伪造攻击中，攻击者伪装授权用户以访问授权网站。　　（对）

372. 跨站请求伪造攻击的主要危害就是可以让攻击者绕过 Web 上的权限控制，通过间接的方式执行越权操作　　（对）

373. 跨站请求伪造攻击的主要危害就是可以让攻击者绕过 Web 上的权限控制，通过直接的方式执行越权操作　　（错）

374. CSRF 攻击能够成功是因为同一浏览器发起的请求对于服务器来讲都是被授权的，如果在请求中加入只有浏览器中该源的网页可以获取的信息，服务器对其验证，就排除了浏览器中其他源的网页伪造请求的可能。　（对）

375. 服务器安全需要为不同的用户分配适当的用户账户，如 Web 服务器软件单独使用受限的操作系统账户。　　（对）

376. 服务器安全，是指在 Web 应用中服务器的安全，攻击者可以利用网站操作系统和 Web 服务程序的漏洞越权操作，非法窃取数据及植入恶意代码，使得网站访问用户蒙受损失。（对）

377. 服务器安全要保证的首先是服务器的物理安全；其次是系统及软件的安全，如操作系统、数据库系统的安全，应安装杀毒软件，及时修补软件漏洞；更进一步就是服务器的安全配置问题。 （对）

378. 服务器安全要保证的首先是系统及软件的安全，其次是服务器的物理安全。 （错）

379. 服务器安全配置首先需要为不同的用户分配适当的用户账户 （对）

380. 服务器安全配置要求关闭 Web 服务器软件的不必要的功能模块。 （对）

381. SQL 注入，是开发者在代码中使用 SQL 语句时，要先生成 SQL 语句，然后调用函数执行这条 SQL 语句。如果错误地直接将用户输入拼接到 SQL 语句中，就有可能产生非预期的结果，从而将用户输入当作 SQL 语句执行。 （对）

382. 针对数据库的攻击主要是 SQL 注入。 （对）

383. 如果输入的数据有固定的数据类型，检查数据类型也可以有效防止 SQL 注入。 （对）

384. 预编译语句指事先编译好 SQL 语句，绑定变量。这样能确保 SQL 语句结构，有效防止用户输入被当作 SQL 语句执行。 （对）

385. CGI 是运行在 Web 服务器上的一个应用，由用户输入触发，使网络用户可以访问远程服务器上相应类型的程序。 （对）

386. CGI 是运行在 Web 服务器上的一个应用，由服务器输入触发，使网络用户可以访问远程服务器上相应类型的程序。 （错）

387. 网站管理员没有对网站进行有效的管理和配置，可能会被攻击者利用进行网站攻击、获取权限，篡改网站 （对）

388. 防止网页被篡改最有效的方法就是使用安全的操作系统和应用程序，并且合理地进行配置。 （对）

389. 轮询检测防篡改技术存在着时间间隔，在这个时间间隔里，黑客完全可以攻击系统并使公众访问到被篡改的网页。 （对）

390. 轮询检测防篡改技术可以处理动态网页。 （错）

391. 在所有类型的操作系统中，任何形式的文件系统改动，操作系统都会迅速、准确地获取相应的事件。 （对）

392. 网页请求到达时，Web 应用引擎需要利用篡改检测模块来读取网页文件，篡改检测模块首先对即将访问文件进行完整性检查，根据检查结果决定如何反馈 Web 应用引擎，完成此次网络请求的处理。 （对）

393. 生产网页防篡改产品的公司通常是纯软件公司，对安全问题没有一个完整的把握，所以常常顾此失彼。　（对）

394. 随着互联网的迅速发展，大量不良信息不断涌现，已经给人们造成很大的危害。很多青少年因此而荒废学业，成为“网络海洛因”的受害者。　（对）

395. 为了提高工作效率，更好地利用网络资源，企业必须对员工在上班时间上网的情况进行管理，规范用户的上网行为。　（对）

396. 面对垃圾邮件的泛滥成灾，除了传统的基于 IP 包头信息的黑名单、白名单等过滤技术以外，各大安全厂商已经开始将内容过滤技术运用于对垃圾邮件的处理。　（对）

397. 在互联网骨干和每一个互联网访问的网络边缘(企业/学校网络边缘、网吧网络出口)部署内容过滤设备，可以有效地减少病毒对网络的侵害。　（对）

398. URL 过滤通常和黑名单、白名单技术相结合来决定是否禁止特定内容。　（对）

399. 事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等具有宣传性质的电子邮件是垃圾邮件。　（对）

400. 为了保证资金的安全和交易的真实性，银行通常会以邮箱验证码确认等形式与消费者进行交互以确保消费者在此笔交易是正确授权的。　（错）

401. 内核是操作系统最核心、最基础的构件，负责提供基础性、结构性的功能。　（对）

402. 壳(shell)是操作系统最核心、最基础的构件，负责提供基础性、结构性的功能。（错）

403. 壳程序包裹了与硬件直接交流的内核，将用户命令行解析为操作系统内部指令（对）

404. 应用程序建立在操作系统之上　（对）

405. 共享的实现指的是资源应该恰当地为用户获取，共享则需要保证资源的完整性和一致性（对）

406. 共享的实现指的是资源应该恰当地为用户获取，共享不需要保证资源的完整性和一致性（错）

407. 用户程序保护指的是每个用户的程序必须在安全的存储器区域内运行，这种保护还需要控制用户对程序空间受限制部分的访问　（错）

408. 存储器保护指的是每个用户的程序必须在安全的存储器区域内运行，这种保护还需要控制用户对程序空间受限制部分的访问　（对）

409. 对一般目标的定位和访问控制指的是提供给用户使用的一般对象必须受到控制，如允许

并行或同步的机制能够确保一个用户不致对其他用户产生干扰。　　（对）

410. 对象控制指的是提供给用户使用的一般对象必须受到控制，如允许并行或同步的机制能够确保一个用户不致对其他用户产生干扰。　（错）

411. 进程共享指的是正在执行的进程有时需要与其他进程通信或者需要使它们对共享资源的访问同步　（错）

412. 内部进程间通信的同步指的是正在执行的进程有时需要与其他进程通信或者需要使它们对共享资源的访问同步　（对）

413. 为了将无意或恶意的攻击所造成的损失降到最低限度，每个用户和程序必须按照“需知”原则，尽可能使用最小特权进行操作　　（对）

414. 为了将无意或恶意的攻击所造成的损失降到最低限度，每个用户和程序必须按照“需知”原则，尽可能使用最大特权进行操作　　（错）

415. 系统的设计应该小而简单，且直截了当，保护系统可以被穷举测试，或者被验证，因而可以信赖　　（对）

416. 系统的设计应该大而复杂，保护系统可以被穷举测试，或者被验证，因而可以信赖　（错）

417. Windows 系统的用户账号(User Accounts)安全是 Windows 系统安全的核心　　（对）

418. Windows 系统的用户账号有两种基本类型，即全局账号和本地账号　（对）

419. 全局账号有时又称为域账号。全局账号主要用于网络环境中的操作系统用户认证。　（对）

420. 本地账号有时又称为域账号。全局账号主要用于网络环境中的操作系统用户认证。　（错）

421. 本地账号是用户在本地域使用的账号，也是用户日常使用最频繁的系统本机账号。　（对）

422. 全局账号是用户在本地域使用的账号，也是用户日常使用最频繁的系统本机账号。　（错）

423. 计算机上设置的局域网参数被修改后，往往导致网络无法正常连接，遇到故障后，需要逐项检查才能解决问题。所以，保障网络连接安全的首要工作是严格网络设置权限　（对）

424. 远程访问服务从产生开始就存在一些安全隐患，但是不需要及时制订远程访问控制方案　（错）

425. 允许越多程序通过 Windows 防火墙通信，计算机将变得越易受攻击，允许例外就好像捅开一个穿过防火墙的洞 （对）

426. Linux 的开源软件开发方式更容易暴露错误，这是 Windows 不具备的优势（对）

427. Windows 具有易学易用性，同时需要兼容不安全的老版本的软件。这些对于系统安全也是一个不利的因素 （对）

428. UNIX 用一个用户名代表用户，用户名最多有 8 个字符，内部表示为一个 16 位的数字，即用户 ID(UID) （对）

429. UNIX 中，系统管理员应该把 Root 账号当成其个人账号 （错）

430. 特权用户可以变为任何别的用户，可以改变系统时钟，正是由于特权用户如此强大，它也成为 UNIX 的一个主要弱点。（对）

431. rwx－－－－－－表示属主有读、写和执行的权力，属组和其他人有读权 （错）

432. rwx－－－－－－表示属主有读、写和执行的权力，属组和其他人没有任何权利 （对）

433. UNIX 以树型结构组织文件系统，这个系统包括文件和目录 （对）

434. Linux 中的 top 命令是一个静态显示过程 （错）

435. Linux 中 who 命令主要用于查看当前在线上的用户情况，系统管理员可以使用 who 命令监视每个登录的用户此时此刻的所作所为 （对）

436. Linux 中的 ps 命令是一个静态显示过程 （对）

437. /etc/exports 文件是 NFS 系统的基本配置文件 （对）

438. 为了使用 NFS 服务，必须运行 rpc、portmap、daemon 等命令 （对）

439. DoS 攻击是一种对网络危害巨大的恶意攻击，其中，具有代表性的攻击手段包括 SYN 洪泛、ICMP 洪泛、UDP 洪泛等 （对）

440. Apache 服务器的安全缺陷主要表现在可以利用 HTTP 对其进行 DoS 攻击、导致缓冲区溢出攻击、让攻击者获得 Root 权限等 （对）

441. Android 基于 Linux 内核，保留了用户和组的概念，以及基于用户和组的访问控制机制 （对）

442. Android 中同一个应用程序的所有进程可以属于不同用户 （错）

443. 除了登录设备和用户添加方式之外，Android 基本继承了 Linux 在系统账号和访问控制方面的其他特征 （对）

444. Android 是一个以 windows 为基础的开放源代码的操作系统（错）

445. Android 软件层次结构自下而上分为操作系统层；程序库和 Android 运行环境；应用程序框架；应用程序四部分　　（对）

446. Android 沙箱机制是通过 Dalvik 虚拟机、Linux 的自主访问控制(DAC)和 Android Permission 机制实现的 （对）

447. Android Permission 机制定义了应用程序可以执行的一系列安全相关的操作　　（对）

448. Android 沙箱机制是为了实现不同应用程序进程之间的隔离 （对）

449. 数据库管理系统能够为用户及应用程序提供数据访问界面，并具有对数据库进行管理、维护等多种功能　（对）

450. 数据库管理系统除了要提供基于角色的操作权限控制外，还要提供对数据对象的访问控制　（对）

451. 数据库管理系统中存取权限 DR 表示 Drop，指的是删除关系里面的记录　（错）

452. 数据库用户的授权分为两种，即静态授权和动态授权　（对）

453. 一般意义上，可以把对数据库用户的静态授权理解为 DBMS 的隐性授权。即用户或数据库管理员对他自己拥有的数据，不需要有指定的授权动作就拥有全权管理和操作的权限　（对）

454. 一般意义上，可以把对数据库用户的动态授权理解为 DBMS 的隐性授权。即用户或数据库管理员对他自己拥有的数据，不需要有指定的授权动作就拥有全权管理和操作的权限　（错）

455. 数据库视图可以被看成虚拟表或存储查询　　（对）

456. 如果说用户登录数据库管理系统过程中的身份认证是一种事前的防范措施，审计也是类似的一种事前监督手段　　（错）

457. 数据库中，表是最小的加密单位　　（错）

458. 数据库中索引字段可以加密　　（错）

459. 数据库中关系运算的比较字段不能加密　（对）

460. 数据库中表间的连接码字段不能加密　　（对）

461.按照数据库系统的大小和数据库管理员所需的工作量，管理员不一定是一个单一的角色，可以细分数据库管理员的角色分工　（对）

462. 开发者(developer)是唯一一类需要特殊权限组完成自己工作的数据库用户 （对）

463. 数据库管理系统保护轮廓给出了数据库管理系统的安全功能要求包和安全保证要求包，这是保护轮廓的主要部分　（对）

464. 当前最受人关注的针对数据库的攻击方式是 SQL 注入攻击 （对）

465. 恶意代码，通常是指以隐秘的方式植入系统，对用户的数据、应用程序和操作系统的机密性、完整性和可用性产生威胁，或者破坏系统正常使用的一段代码。 （对）

466. 近年来手机恶意扣费软件影响十分恶劣，恶意扣费程序可在非用户授权的情况下消耗用户的手机资费。 （对）

467. Wannacry 勒索病毒等最新出现的病毒不需触发点即可传播。 （错）

468. 计算机病毒，是指通过修改其他程序进行“感染”，并对系统造成破坏的一段代码，但这种修改不具有自我复制的能力。 （错）

469. 计算机病毒中的感染机制指的是病毒散播和自我复制的方式。 （对）

470. 计算机病毒中的触发点指的是病毒激活或者传播病毒的事件或条件。 （对）

471. 计算机病毒中的负载指的是病毒感染后对数据、应用等造成破坏的代码。 （对）

472. 在触发阶段，计算机病毒被激活。 （对）

473. 在计算机病毒的传播阶段，计算机病毒将自身的拷贝附加在其他程序中，或者保存在磁盘上。为了躲避探测，计算机病毒可能改写不同的拷贝。 （对）

474. 在计算机病毒的传播阶段，计算机病毒执行破坏操作。 （错）

475. 计算机病毒一般具有传染性、破坏性、隐蔽性、寄生性和针对性。 （对）

476. 不同于一般的计算机病毒，单纯的木马不具备自我复制的能力，也不会主动感染系统中的其他组件。 （对）

477. 一般的木马均具备自我复制能力。 （错）

478. 木马利用恶意代码破坏受感染主机的计算资源和网络资源，然后通过网络将该段恶意代码感染大量的机器。 （错）

479. 蠕虫病毒经常会利用客户端和服务器的软件漏洞，获得访问其他计算机系统的能力 （错）

480. 僵尸程序可感染数以千计的主机，形成一对多控制的网络。 （对）

481. 网络嗅探是僵尸程序的一种典型应用，可以在肉鸡上进行网络嗅探，挖掘感兴趣的网络数据。 （对）

482. Rootkit 是指能够隐蔽地获取系统管理员(Administrator)或者 Root 权限的一系列程序，同时它会最大限度地隐藏自身存在。 （对）

483. Rootkit 仅可以访问操作系统的部分功能和服务 （错）

484. 所有 Rootkit 在系统重启后都会存在。 （错）

485. 基于虚拟机的 Rootkit 可以通过修改内核中的进程列表隐藏恶意代码进程的存在。（错）

486. 持久性存储类的 Rootkit 在系统重启之后，Rootkit 仍然存在。（对）

487. 基于内存的 Rootkit 存在持久性代码。（错）

488. 内核态类 Rootkit 在用户态截获应用程序接口的调用，并修改返回值。（错）

489. 用户态类 Rootkit 在内核态截获内核的本地接口。（错）

490. 基于虚拟机的 Rootkit 可以透明地截获并修改目标操作系统的状态。（对）

491. 外部模式类 Rootkit 运行在普通操作系统模式之外，如 BIOS 或者系统管理模式，因而能够直接访问硬件。（对）

492. 所有恶意代码都可以通过提升自身权限(如 Root)，进而随意修改、删除用户的数据、安装或删除设备上的任意应用。（错）

493. 若能阻止恶意程序注册广播接收器 Receiver，则恶意代码无法启动。（错）

494. 恶意应用若获取了 Root 权限，则该恶意应用就可以全面操控用户的设备。（对）

495. 计算机病毒引导部分是通过驻留内存、修改中断以及注册表等方式，将病毒主体加载到内存中。（对）

496. 磁盘引导扇区的病毒往往会占用系统原来引导程序的位置，一旦系统启动，就会获得执行权，然后将病毒的其他部分写入内存的特定地址并使之常驻内存，之后执行系统原来的引导程序。（对）

497. 计算机病毒可能干扰程序运行、破坏系统中的程序或数据、窃取信息等。（对）

498. 一旦远程控制类软件安装到用户设备上，它就会通过各种方式与攻击者取得联系，等待攻击者的远程控制指令。（对）

499. 很多系统破坏类代码需要先提升自身权限(如 Root)，然后就可以随意修改或删除用户的数据、安装或删除设备上的任意应用，给用户造成不可挽回的损失。（对）

500. 流氓软件类程序一般是强行安装的并难以卸载，即使卸载后也可能通过后台重新安装等方式恢复运行。（对）

501. 诈骗软件主要通过诈骗直接获取经济利益，主要有两种诈骗方式，其中包括向所有联系人发送包含银行账号、求助信息的伪造短信和向用户手机的收件箱插入虚假的未读信息，该信息包含中奖、求助、银行等通知，引导不明原因的用户上当。（对）

502. 恶意传播类软件在用户不知情或者没有明确授权的情况下，将自身及其他恶意代码进行扩散。（对）

503. 重打包攻击指的是反编译正常 APP 后嵌入恶意代码，将含恶意代码的 APP 发布到应商店，供用户下载。　　（对）

504. 更新攻击指的是反编译正常 APP 后嵌入恶意代码，将含恶意代码的 APP 发布到应商店，供用户下载。　　（错）

505. 下载攻击指的是反编译正常 APP 后嵌入恶意代码，将含恶意代码的 APP 发布到应商店，供用户下载。　　（错）

506. 利用系统事件触发恶意代码利用的是 Android 提供广播 broadcast 机制。（对）

507. 在 Android 系统收到短信后，会发送短信到来的有序广播，恶意代码可以通过注册接收器在其他程序接收信息之前将信息拦截，获取信息的内容和其中的指令，根据其中的指令完成恶意操作。　　（对）

508. 加壳，是指利用某些算法，对可执行程序进行压缩、加密。　　（对）

509. 与普通的压缩方式相同的是，加壳后的程序不能独立运行。　　（错）

510. 与普通的压缩方式不同，加壳后的程序可以独立运行，其解压或解密过程对用户透明。（对）

511. 一般来说，壳代码附加在原可执行程序上，在程序载入内存之后，壳代码优先于原可执行程序，获得执行权，由壳代码进行解压解密操作后，将执行权交给原可执行程序。（对）

512. 由于原代码以加密方式存在于磁盘上，只有在运行时在内存中还原，因而可以防止原程序被非法篡改。（对）

513. 加壳后的程序通常比原程序具有更大的输入表，导入大量链接库。为了满足这种要求，壳依赖的大量函数采用了动态加载方式。　　（错）

514. 通常情况下，可以将原程序加载到固定的内存地址中。so 或 dll 等动态链接库的加载地址并不确定，为了确保程序的正常运行，需要进行函数的重定位。（对）

515. 壳依赖的大量函数采用了静态加载方式，使得加壳后的程序通常比原程序具有更小的输入表。（错）

516. 压缩壳的主要目的是减小程序的大小，如 AS Protect、Armadillo 和 EXE Cryptor 等。（错）

517. 加壳通常需要修改原程序输入表的条目使得壳代码优先于原可执行程序获得执行权。（对）

518. 压缩壳的主要目的是减小程序的大小，如 UPX、PE Compat 和 AS Pack 等。　　（对）

519. 保护壳使用多种反追踪技术防止程序被调试和反编译，如 UPX、PE Compat 和 AS Pack 等。　　（错）

520. 保护壳使用多种反追踪技术防止程序被调试和反编译，如 AS Protect、Armadillo 和 EXE Cryptor 等。　（对）

521. 软件逆向工程通常包括两类：一类是从特定程序的完整代码出发，生成对应的程序结构、设计原理和算法思想的文档；另一类是从无源代码的程序出发，生成源程序、设计原理等。　　（对）

522. 扫描器是反病毒软件的核心，决定着反病毒软件的杀毒效果。大多数反病毒软件同时包含多个扫描器。　（对）

523. 通过下载或升级病毒库，能检测到未知的新病毒或者病毒变种。　　（错）

524.沙箱在物理主机上表现为一个或多个进程，因而可以在有效监控恶意代码行为的前提下，保证主机上的其他程序或者数据不被破坏。　（对）

525. 特征码扫描方式效率较高，但是缺点是不能检测到未知的新病毒或者病毒变种。　　（对）

526. 特征码扫描方式能检测到未知的新病毒或者病毒变种　（错）

527. 恶意行为分析通过对恶意样本的行为特征进行分析和建模，从中抽取恶意代码的行为特征，在应用执行过程中，判断应用的行为序列是否符合某些已知的恶意行为，若是，该应用可能包含恶意代码。　（对）

528. 正常行为分析是指对程序的安全行为序列进行分析和建模，为程序建立一个安全的行为库，当被检测应用的行为与预先建立的安全行为库存在差异时，则认为程序发生了异常行为。　　（对）

529. 正常行为分析是通过对恶意样本的行为特征进行分析和建模，从中抽取恶意代码的行为特征，在应用执行过程中，判断应用的行为序列是否符合某些已知的恶意行为。　（错）

530. 恶意行为分析是指对程序的安全行为序列进行分析和建模，为程序建立一个安全的行为库，当被检测应用的行为与预先建立的安全行为库存在差异时，则认为程序发生了异常行为。　　（错）

531. 恶意代码检测中，基于行为的检测技术的缺点是容易发生误报现象，而且往往计算开销比较大，同时也不能检测某些模拟攻击。　　（对）

532. 基于特征码的扫描技术和基于行为的检测技术都需要执行潜在的恶意代码并分析它们的特征或行为，但是这可能会给系统带来安全问题。　（对）

533. 沙箱可以模拟代码运行所需要的真实环境，并且其安全隔离机制又能够防止恶意代码对系统的破坏。　　（对）

534. 在恶意代码检测技术中，沙箱技术会破坏主机上或其他程序数据。　（错）

535. 由于沙箱在物理主机上表现为一个或多个进程，因而可以在有效监控恶意代码行为的前提下，保证主机上的其他程序或者数据不被破坏。　　（对）

536. 恶意代码检测中，启发式检测技术是为了弥补特征码扫描技术无法检测未知病毒的缺陷而提出的。　（对）

537. 恶意代码检测中，特征码扫描技术可以检测未知病毒。　　（错）

538. 启发式检测就是把经验或者知识加入到反病毒软件中，使反病毒软件拥有“自我发现的能力或运用某种方式或方法去判定事物的知识和技能”。　　（对）

539. 启发式检测中恶意样本的采样不科学或者训练算法选择不合理，都会造成恶意程序的误报或漏报。　（对）

540. 恶意代码的静态分析方法，是指在不运行恶意代码的情况下，利用反汇编等分析工具，对给定程序的静态特征和功能模块进行分析的方法。　（对）

541. 恶意代码的静态分析方法包括脱壳、字符串匹配、反汇编和反编译方法等。　（对）

542. 恶意代码的动态分析方法，是指在不运行恶意代码的情况下，利用反汇编等分析工具，对给定程序的静态特征和功能模块进行分析的方法。　（错）

543. 通过动态分析方法能够获得恶意代码的结构、各模块关系、函数调用或者系统调用信息等，它是目前使用广泛的恶意代码分析方法。　　（错）

544. 恶意代码的静态分析方法，是指在虚拟机等沙箱中运行恶意代码，监视其行为，获得相应的执行路径和相关语义信息的方法。　（错）

545. 恶意代码的动态分析方法，是指在虚拟机等沙箱中运行恶意代码，监视其行为，获得相应的执行路径和相关语义信息的方法。　（对）

546. 恶意代码的静态分析方法可以获得相应的执行路径和相关语义信息的方法。　（错）

547. 恶意代码的动态分析可分为状态对比和行为跟踪两类方法。　　（对）

548. 恶意代码状态对比方法对程序执行前后、执行不同时刻的系统状态进行比较，从而分析获取程序的行为。　　（对）

549. 恶意代码状态对比方法状态变化分析的准确度高，同时能实时地跟踪程序执行中的变化轨迹。　（错）

550. 恶意代码行为跟踪方法可以动态地获取进程执行过程中的操作。　　（对）

551. 根据恶意代码的行为跟踪实现技术的不同大致可分为指令级和轻量级两类。其中指令级方法可以获取或修改寄存器状态、内存状态和其中的值，改变程序的控制流程。 （对）

552. 根据恶意代码的行为跟踪实现技术的不同大致可分为指令级和轻量级两类。其中轻量级方法采用系统调用钩子函数或者设备驱动过滤等技术提取程序行为。 （对）

553. 根据恶意代码的行为跟踪实现技术的不同大致可分为指令级和轻量级两类。其中轻量级方法可以获取或修改寄存器状态、内存状态和其中的值，改变程序的控制流程。 （错）

554. 根据恶意代码的行为跟踪实现技术的不同大致可分为指令级和轻量级两类。其中指令级方法采用系统调用钩子函数或者设备驱动过滤等技术提取程序行为。 （错）

555. 通过对软件采用可信的签名，使用者验证签名来确保所使用软件确实来自签发者。（对）

556. 代码签名技术是基于公钥密码体制和数字摘要的。 （对）

557. 数字摘要是保证消息完整性的一种技术。数字摘要将任意长度的消息转换为固定长度消息，该过程是双向的。 （错）

558. 数字摘要是保证消息完整性的一种技术。数字摘要将固定长度消息转换成任意长度的消息，该过程是双向的。 （错）

559. 数字摘要是保证消息完整性的一种技术。数字摘要将固定长度消息转换成任意长度的消息，该过程是单向的。 （错）

560. 数字摘要是保证消息完整性的一种技术。数字摘要将任意长度的消息转换为固定长度消息，而且该过程是单向的。 （对）

561. 代码签名基于 PKI 体系，包括签名证书私钥和公钥两部分，私钥用于代码的签名，公钥用于签名的验证。 （对）

562. ISO/IEC 21827 模型主要从风险、工程和信任度三个方面来分析安全的工程过程（对）

563. ISO/IEC 21827 模型从威胁、工程和信任度三个方面来分析安全的工程过程 （错）

564. ISO/IEC 21827 将安全工程服务提供者的能力划定为五个级别 （对）

565. ISO/IEC 21827 将安全工程服务提供者的能力划定为四个级别 （错）

566. SSAM (SSE－CMM Apprialsal)评估主要由三方构成，包括发起组织、评估组织及被评估组织 （对）

567. SSAM (SSE－CMM Apprialsal)评估主要由三方构成，包括发起组织、评估组织及监管组织 （错）

568. 从评估阶段上来看，SSAM(SSE－CMM Apprialsal)主要分为计划阶段、准备阶段、现场阶段和报告阶段。　　（对）

569. 从评估阶段上来看，SSAM(SSE－CMM Apprialsal)主要分为计划阶段、准备阶段、现场阶段　　（错）

570. 从评估类型上来看，SSAM (SSE－CMM Apprialsal)评估方法分为三方评估和自我评估两种。　　（对）

571. 从评估类型上来看，SSAM(SSE－CMM Apprialsal) 评估方法仅由三方评估。　（错）

572. 从评估类型上来看，SSAM(SSE－CMM Apprialsal) 评估方法仅由自我评估。　（错）

573. 网络安全等级保护的主要内容是依据重要性等级对信息以及信息载体进行有针对性的分级保护。　（对）

574. 网络安全等级保护的主要内容是依据风险性等级对信息以及信息载体进行有针对性的分级保护。　（错）

575.《信息安全等级保护管理办法》将信息系统的安全保护划分为五个等级。　　（对）

576.《信息安全等级保护管理办法》将信息系统的安全保护划分为三个等级。　　（错）

577. 信息系统安全包括业务信息安全和系统服务安全　（对）

578. 信息系统安全只包括系统服务安全　（错）

579. 信息系统安全只包括业务信息安全　（错）

580. 涉密网络需要与高安全等级网络区分开来　　（对）

581. 涉密网络等同于高安全等级网络区　（错）

582.《可信计算机系统评估准则》TCSEC 将安全要求由高到低分为四类　（对）

583.《可信计算机系统评估准则》TCSEC 将安全要求由高到低分为七类　（错）

584.《可信计算机系统评估准则》TCSEC 将安全级别由高到低分为七级　（对）

585.《可信计算机系统评估准则》TCSEC 将安全级别由高到低分为四级　（错）

586.《可信计算机产品评估准则》CTCPEC 沿袭《可信计算机系统评估准则》TCSEC 和《信息技术安全评估准则》ITSEC，将安全分为功能性要求和保证性要求两部分　　（对）

587.《可信计算机产品评估准则》CTCPEC 沿袭《可信计算机系统评估准则》TCSEC 和《信息技术安全评估准则》ITSEC，认为安全仅包括功能性要求　（错）

588.《可信计算机产品评估准则》CTCPEC 沿袭《可信计算机系统评估准则》TCSEC 和《信息技术安全评估准则》ITSEC，认为安全仅仅包含保证性要求　　（错）

589. 在 CC 评估方法中，评估的主要目的是证实评估目标所生成的安全性级别，其中必须包

含证实目标的安全特性。 （对）

590. 在 CC 评估方法中，评估的主要目的是证实评估目标所生成的安全性级别，但是不一定要证实目标的安全特性。 （错）

591. 在 CC 评估方法中，安全目标可以涉及一个或者多个安全轮廓 （对）

592. 在 CC 评估方法中，安全目标只能涉及一个安全轮廓 （错）

593. 在 CC 评估方法中，组件是一组不可再分的最小安全要求集合 （对）

594. 在 CC 评估方法中，组件是一组可再分的安全要求集合 （错）

595. 在 CC 标准的技术安全措施文档规范中，密码支持类由两个子类构成，分别规定了在密钥使用和密钥管理方面的相关规范细节。 （对）

596. 在 CC 标准的技术安全措施文档规范中，密码支持类仅由一个类构成，它规定了在密钥使用和密钥管理方面的相关规范细节。 （错）

597. CMVP(Cryptographic Module Validation Program)评估有两个目标：(1)保证安全模块实现的正确性和安全性；(2)为模块改进提供帮助。 （对）

598. CMVP(Cryptographic Module Validation Program)评估需要保证安全模块实现的正确性和安全性 （对）

599. CMVP(Cryptographic Module Validation Program)评估需要为模块改进提供帮助 （对）

600. 密码模块检测认证是信息安全检测认证体系的基础和开始 （对）

601. 在国际上比较通用的信息安全检测认证体系模型大致可以分为三个层次 （对）

602. 信息安全检测认证体系中，密码模块检测认证有统一的标准 （错）

603. 信息安全检测认证体系中，密码模块检测认证各国有不同的标准 （对）

604. 信息安全检测认证体系中，密码模块检测认证可以与信息安全产品检测认证工作相结合 （对）

605. 信息安全检测认证体系中，密码模块检测认证可以替代信息安全产品检测认证工作 （错）

606. 在产品和系统中使用密码模块(包含密码算法)来提供机密性、完整性、鉴别等安全服务 （对）

607. 密码算法验证是 CMVP(Cryptographic Module Validation Program)的先决条件。 （对）

608. 密码算法验证不是 CMVP(Cryptographic Module Validation Program)的先决条件。

（错）

609. 密码算法正确性检测(CAVP)不是 CMVP(Cryptographic Module Validation Program)必要的先决条件 （错）

610. 密码算法正确性检测(CAVP)是 CMVP(Cryptographic Module Validation Program)必要的先决条件 （对）

二、单选题

1. 网络传输层不可以提供哪种安全服务?

(A)对等实体认证 (B)访问控制 (C)非否认 (D)数据起源认证

答案：C

2. 硬件安全技术不包括以下哪种?

(A)侧信道技术 (B)硬件固件安全技术 (C)无线传感器网络安全技术 (D)VLAN

答案：D

3. 硬件安全技术不包括以下哪种?

(A)漏洞扫描 (B)硬件固件安全技术 (C)侧信道技术

(D)无线传感器网络安全技术

答案：A

4. 网络安全技术主要包括网络攻击技术和网络防御技术，不包含哪种技术?

(A)防火墙技术 (B)网络隔离技术 (C)入侵检测 (D)数据安全性技术

答案：D

5. 数据安全技术旨在保护信息系统中的数据不被非法访问、篡改、丢失和泄漏。数据安全技术无法提供（）

(A)数据的可用性 (B)数据的机密性 (C)数据的完整性 (D)数据的传输性

答案：D

6. 传统的 PKI 技术不提供什么服务?

(A)认证 (B)完整性保护 (C)密钥管理 (D)访问控制

答案：D

7. OSI 安全体系结构中提出的安全机制不包括?

(A)加密 (B)数字签名 (C)访问控制 (D)非否认

答案：D

8. OSI 安全体系结构中提出的安全机制中，认证服务需要什么技术?

(A)数据签名 (B)路由选择 (C)资源访问控制 (D)密码技术

答案：D

9. 除了 OSI 安全体系结构中提出的安全机制之外，哪个不是普遍采用的安全机制

(A)访问控制 (B)可信功能模块 (C)安全标记 (D)安全恢复

答案：A

10. 除了 OSI 安全体系结构中提出的安全机制之外，下面还有哪个是普遍采用的安全机制

(A)数字签名 (B)数据完整性 (C)认证交换 (D)安全审计跟踪

答案：D

11.关于安全服务与网络层次之间的对应关系，下面哪个网络层次不可以提供对等实体认证?

(A)链路层 (B)应用层 (C)传输层 (D)网络层

答案：A

12. 关于安全服务与网络层次之间的对应关系，哪个网络层次不提供安全服务

(A)物理层 (B)会话层 (C)应用层 (D)网络层

答案：B

13. 关于安全服务与网络层次之间的对应关系，会话层可以提供哪种安全服务

(A)数据完整性 (B)非否认 (C)数据起源认证 (D)不提供安全服务

答案：D

14. 软件安全技术是信息安全技术体系结构之一，现有的软件安全技术不包括?

(A)恶意代码分析与检测 (B)软件代码的安全 (C)操作系统检测 (D)软件缺陷与漏洞分析

答案：C

15. 信息安全管理是信息安全技术体系结构之一，现有的信息安全管理不包括?

(A)信息系统安全工程 (B)信息安全等级保护 (C)涉密网络分级保护 (D)网络安全设计

答案：D

16. 信息安全管理是信息安全技术体系结构之一，哪一个不是现有的信息安全管理的内容?

(A)安全风险评估 (B)信息安全等级保护 (C)访问控制检测 (D)信息系统安全工程

答案：C

17. 对抗暴力破解口令的最佳方法是?

(A)设置简单口令 (B)设置多个密码 (C)设置一个较长的口令以扩大口令的穷举空间 (D)经常换口令

答案：C

18. 密码体制被定义为（）数据变换

(A)一对 (B)两对 (C)三对 (D)四对

答案：A

19. 首次提出了非对称密码体制的假想的是（）

(A)《密码起源》 (B)《密码简史》 (C)《密码安全》 (D)《密码学新方向》

答案：D

20. 大多数使用公钥密码进行加密和数字签名的产品及标准使用的都是（）

(A)RSA 算法 (B)ASE 算法 (C)DES 算法 (D)IDEA 算法

答案：A

21. 用于加密和解密的数学函数是（）

(A)密码算法 (B)密码协议 (C)密码管理 (D)密码更新

答案：A

22. 密码协议安全的基础是（）

(A)密码安全 (B)密码算法 (C)密码管理 (D)数字签名

答案：B

23. 密钥封装(Key Wrap)是一种（）技术

(A)密钥存储 (B)密钥安全 (C)密钥分发 (D)密钥算法

答案：C

24. （）包括加密协议设计、密钥服务器、用户程序和其他相关协议

(A)密钥管理 (B)密钥安全 (C)密钥封装 (D)密钥算法

答案：A

25. 如果要增加攻击者攻破密钥的难度，需要进行（）

(A)密钥销毁 (B)密钥存储 (C)密钥更新 (D)密钥完整性校验

答案：C

26. 目前常用的数字签名方法是（）

(A)RSA 算法 (B)基于 Hash 的数字签名方法 (C)IDEA 算法 (D)DES 算法

答案：B

27. 我国密码行业标准 GM/T 0028－2014 规定了（）要求递增的安全等级

(A)两个 (B)三个 (C)四个 (D)五个

答案：C

28. 我国密码行业标准 GM/T 0028－2014 规定了四个要求递增的安全等级，其中（）提供了最低等级的安全要求

(A)一级 (B)二级 (C)三级 (D)四级

答案：A

29. 我国密码行业标准 GM/T 0028－2014 规定了四个要求递增的安全等级，其中（）是最高等级

(A)一级 (B)二级 (C)三级 (D)四级

答案：D

30. 访问控制是计算机安全的核心元素。访问控制机制介于哪两者之间（）

(A)用户和用户 (B)用户和系统资源 (C)用户和界面 (D)系统资源与系统资源

答案：B

31. 访问控制的主要目标不包括以下哪个选项（）

(A)防止未经授权的用户获取资源 (B)防止已经授权的用户获取资源 (C)防止合法用户以未授权的方式访问资源 (D)使合法用户经过授权后可以访问资源

答案：B

32. 访问控制的基本要素不包括以下哪个选项（）

(A)客体 (B)主体 (C)控制策略 (D)访问权限

答案：C

33. 在访问控制的基本要素中，能够访问对象的实体的是（）。

(A)客体 (B)控制策略 (C)主体 (D)访问权限

答案：C

34. 一般来说，（）是那些包含或者接收信息的实体

(A)客体 (B)控制策略 (C)主体 (D)访问权限

答案：A

35. 主体对客体的相关访问方式集合称为（）。

(A)客体 (B)控制策略 (C)主体 (D)访问权限

答案：D

36. 基于请求者的身份以及访问规则来进行访问控制的是（）。

(A)被动访问控制 (B)自主访问控制 (C)强制访问控制 (D)完全访问控制

答案：B

37. 基于对客体安全级别与主体安全级别的比较来进行访问控制的是（）。

(A)被动访问控制 (B)自主访问控制 (C)强制访问控制 (D)完全访问控制

答案：C

38. （）决定在哪些情况下、由什么主体发起、什么类型的访问是被允许的

(A)网络防御技术 (B)访问控制策略 (C)防火墙技术 (D)网络攻击

答案：B

39. 使用一维矩阵表示访问控制时，会产生比较大的空间浪费，因此访问控制的另一种表示方式是（）。

(A)权限映射 (B)二维矩阵 (C)有向图 (D)权限列表

答案：D

40. 在自主访问控制中，每个主体对自己拥有的对客体的访问权限可以使用一维矩阵或者（）来表示。

(A)权限映射 (B)二维矩阵 (C)有向图 (D)权限列表

答案：D

41. 在自主访问控制中表示访问控制时，会产生比较大的空间浪费的表达方式是（）

(A)权限映射 (B)一维矩阵 (C)有向图 (D)权限列表

答案：B

42. 在基于角色的访问控制中，主体和角色是（）的 关系

(A)一对一 (B)一对多 (C)多对一 (D)多对多

答案：D

43. 在基于角色的访问控制中，客体和角色是（）的 关系

(A)一对一 (B)一对多 (C)多对一 (D)多对多

答案：D

44. （）是基于主体在系统中承担的角色进行的访问控制是

(A)基于身份的访问控制　(B)基于权限的访问控制　(C)基于角色的访问控制　(D)基于用户的访问控制

答案：C

45. 能够从控制主体的角度出发，根据管理中相对稳定的职权和责任划分来分配不同的角色的是（）

(A)基于身份的访问控制　(B)基于权限的访问控制　(C)基于角色的访问控制　(D)基于用户的访问控制

答案：C

46. ITSEC 一共定义了（）个安全等级

(A)4 (B)5 (C)6 (D)7

答案：D

47. 关于 TCSEC 说法正确的是（）

(A)类 C 中的级别 C1 是最高安全级别(B)类 D 中的级别 D1 是最低安全级别　(C)类 D 中的级别 D1 是最高安全级别。(D)类 D 中的级别 A1 是最低安全级别

答案：B

48. TCSEC 一共定义了（）个等级

(A)5 (B)6 (C)7 (D)8

答案：C

49. 我国制定了强制性国家标准《计算机信息系统安全保护等级划分准则》，其中属于第五级的是（）

(A)用户自主保护级　(B)系统审计保护级　(C)安全标记保护级　(D)访问验证保护级

答案：D

50. 物理安全可以分为环境安全和设备安全两大类。以下不属于环境安全考虑事项的是()。

(A)场地安全　(B)防静电　(C)线路安全　(D)防电磁泄露

答案：D

51. 物理安全可以分为环境安全和设备安全两大类。以下不属于设备安全考虑事项的是()。

(A)设备防盗 (B)防电磁干扰 (C)线路安全 (D)防电磁泄露

答案：C

52. 以下不符合计算机场地规范要求的是（）。

(A)避开易发生火灾和爆炸的地区 (B)避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域 (C)避免低洼、潮湿及落雷区域 (D)避免居民区

答案：D

53. 计算机机房的耐火等级应不低于（）级。

(A)1 级 (B)2 级 (C)3 级 (D)4 级

答案：B

54. 对于环境的电磁防护可以从以下哪个方面入手（）

(A)采用距离防护的方法 (B)采用接地的方法 (C)采用屏蔽方法 (D)全正确

答案：D

55. 电源是电子设备运行的必要条件，持续稳定的电源供应是环境运行的基本保证。以下说法错误的是（）

(A)信息网络的供电线路应该和动力、照明用电分开 (B)特殊设备独占专有回路 (C)提供备份电路 (D)信息网络的供电线路和动力、照明用电共用

答案：D

56. 以下不符合防静电要求的是( )。

(A)穿合适的防静电衣服和防静电鞋 (B)在机房内直接更衣梳理 (C)用表面光滑平整的办公家具 (D)经常用湿拖布拖地

答案：B

57. 以下行为不符合对电子信息系统的雷电防护的是（）

(A)机房最好放在建筑物的中间位置 (B)设置安全防护地域屏蔽地，应采用阻抗大的导体。 (C)设置避雷电网 (D)一般以交界处的电磁环境有无明显的改变作为划分不同防雷区域的特征。

答案：B

58. 以下行为不符合对电子信息系统的雷电防护的是（）。

(A)机房建在距离大楼外侧 (B)机房内应设等电位连接网络 (C)设置安全防护地与屏蔽地 (D)在机房内布置设备的安放位置时，应该放在比较接近中心的位置，以与外墙特别是外墙立柱保持一定的距离。

答案：A

59. 以下不是为了减小雷电损失采取的措施有（）。

(A)设置避雷地网 (B)部署 UPS (C)设置安全防护地与屏蔽地 (D)根据雷击在不同区域的电磁脉冲强度划分，不同的区域界面进行等电位连接

答案：B

60. 以电磁波的形式由空中辐射出去，由计算机内部的各种传输线、信号处理电路、时钟电路等产生的数据信息泄露方式称为（）。

(A)辐射泄漏 (B)传导泄漏 (C)电信号泄漏 (D)媒介泄漏

答案：A

61. 通过各种线路传导出去，可以将计算机系统的电源线，机房内的电话线、地线等作为媒介的数据信息泄露方式称为（）。

(A)辐射泄漏 (B)传导泄漏 (C)电信号泄漏 (D)媒介泄漏

答案：B

62. 380V 电力电缆，容量小于 2kVA，与信号线缆平行敷设，最小净距为（）/mm

(A)150 (B)70 (C)300 (D)80

答案：A

63. 380V 电力电缆，容量小于 2kVA，有一方在接地的金属线槽或钢管中，最小净距为（）/mm

(A)150 (B)70 (C)300 (D)80

答案：B

64. 380V 电力电缆，容量大于 5kVA，与信号线缆平行敷设，最小净距为（）/mm

(A)150 (B)200 (C)300 (D)600

答案：D

65. 380V 电力电缆，容量 2~5kVA，与信号线缆平行敷设，最小净距为（）/mm

(A)150 (B)70 (C)300 (D)80

答案：C

66. 380V 电力电缆，容量小于 2kVA，双方方在接地的金属线槽或钢管中，最小净距为（）/mm

(A)10 (B)70 (C)300 (D)80

答案：A

67. 关于防电磁泄漏信息安全标准，以下由我国制定的是（）

(A)NACSIM5100 (B)NSTISSAM TEMPEST/1－91 (C)GGBB 1－1999 (D)GB 50343－2012

答案：C

68. TEMPEST 技术（Transient Electro Magnetic Pulse Emanation Standard，瞬态电磁辐射标准），是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取防辐射措施，从而达到减少计算机信息泄漏的最终目的。以包容式 TEMPEST 计算机为代表的是（）TEMPEST 技术。

(A)第一代 (B)第二代 (C)第三代 (D)第四代

答案：A

69. TEMPEST 技术（Transient Electro Magnetic Pulse Emanation Standard，瞬态电磁辐射标准），是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取防辐射措施，从而达到减少计算机信息泄漏的最终目的。以红黑分离式 TEMPEST 计算机为代表的是（）TEMPEST 技术。

(A)第一代 (B)第二代 (C)第三代 (D)第四代

答案：B

70. TEMPEST 技术（Transient Electro Magnetic Pulse Emanation Standard，瞬态电磁辐射标准），是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取防辐射措施，从而达到减少计算机信息泄漏的最终目的。以 SOFT－TEMPEST 技术为代表的是（）TEMPEST 技术。

(A)第一代 (B)第二代 (C)第三代 (D)第四代

答案：C

71. 对电子产品的电磁兼容性标准描述正确的是( )。

(A)同一个国家是恒定不变的 (B)不是强制的 (C)各个国家不相同 (D)是滤波的

答案：C

72. 电磁干扰主要分为（）种。

(A)二 (B)三 (C)四 (D)五

答案：A

73. 在安全领域一直流传着一种观点：三分技术，（）分管理。

(A)三　(B)五　(C)七　(D)九

答案：B

74. 在安全领域一直流传着一种观点：（）分技术，七分管理。

(A)一　(B)三　(C)五　(D)九

答案：B

75. 以下不属于侧信道技术（利用非通信信道物理信息如能量消耗变化、电磁辐射变化进行分析攻击）的攻击技术是（）。

(A)能量分析　(B)计时分析　(C)错误注入　(D)干扰技术

答案：D

76. 以下属于硬件安全技术的有(　)。

(A)侧信道技术　(B)硬件固件安全技术　(C)无线传感器网络安全技术　(D) 均 属 于

答案：D

77. 为了分析密码模块能量消耗的变化，使用了统计方法对能量消耗进行统计分析从而获取密钥值的是（）差分能量分析

(A)一阶　(B)二阶　(C)三阶　(D)高阶

答案：A

78. 以下属于错误注入分析的是(　)。

(A)监视密码模块能量消耗的变化以发现指令的能量消耗模式　(B)密码模块的执行时间与密码算法的特殊数学操作之间的关系　(C)对微波、电压等的控制引发密码模块内部运行错误，进而进行错误、模式分析　(D)对正在运行的密码模块和辅助设备发出的电磁信号进行远程或外部探测和接收

答案：C

79. 下列关于固件的说法错误的是（）。

(A)在电子系统和计算机系统中，固件一般指持久化的内存、代码和数据的结合体。

(B)固件是一种密码模块的可执行代码，它存储于硬件并在密码边界内，在执行期间能动态地写或修改。　(C)存储固件的硬件可以包括但不限于 PROM、EEPROM、FLASH、固态存储器、硬盘驱动等。　(D)固件的数据和代码一般是在密码产品出厂之前就写入硬件中的，而当写入固件的代码中存在恶意代码时，硬件固件攻击也将发生。

答案：B

80. 下面关于无线传感器网络攻击技术说法错误的是（）。

(A)选择性数据转发攻击，是指攻击者截取并控制某个节点后，为了避免被发现该节点已被攻破，故仅丢弃应转发报文中的一部分。 (B)路由攻击，是指攻击节点依照路由算法伪造或重放一个路由声明，声称攻击节点和基站之间有高质量的单跳路由，然后阻止或篡改被攻击区域中任一节点发出的数据包。 (C)虫洞攻击，是指两个或多个攻击节点进行的一种合谋攻击，通过压缩攻击节点间的路由，使得彼此成为邻居节点，从而将不同分区的节点距离拉近，破坏整个网络的正常分区。 (D)女巫攻击，是指攻击节点伪装成具有多个身份标识的节点，当通过该节点的一条路由遭到破坏时，网络会选择另一条路由，但由于其具有多重身份标识，实际上还是通过了该攻击节点。

答案：B

81. 当前无线传感器网络面临多种攻击技术，其中（）是指向无线传感器网络中通过发送大量错误路由报文的方式，非法拦截篡改路由信息，使得各个节点接收到大量的错误路由信息，从而降低整个网络的有效传输速度。

(A)路由攻击 (B)选择性数据转发攻击 (C)槽洞攻击 (D)虫洞攻击

答案：A

82. 当前无线传感器网络面临多种攻击技术，其中（）是指攻击者截取并控制某个节点后，为了避免被发现该节点已被攻破，故仅丢弃应转发报文中的一部分。

(A)路由攻击 (B)选择性数据转发攻击 (C)槽洞攻击 (D)虫洞攻击

答案：B

83. 当前无线传感器网络面临多种攻击技术，其中（）是指攻击节点依照路由算法伪造或重放一个路由声明，声称攻击节点和基站之间有高质量的单跳路由，然后阻止或篡改被攻击区域中任一节点发出的数据包。

(A)路由攻击 (B)选择性数据转发攻击 (C)槽洞攻击 (D)虫洞攻击

答案：C

84. 当前无线传感器网络面临多种攻击技术，其中（）是指两个或多个攻击节点进行的一种合谋攻击，通过压缩攻击节点间的路由，使得彼此成为邻居节点，从而将不同分区的节点距离拉近，破坏整个网络的正常分区。

(A)路由攻击 (B)选择性数据转发攻击 (C)槽洞攻击 (D)虫洞攻击

答案：D

85. 当前无线传感器网络面临多种攻击技术，其中 () 是指攻击节点向全网广播 Hello 报文，

网络中的节点收到 Hello 报文之后，使得每一个节点误以为攻击节点是自己的邻居节点。

(A)女巫攻击 (B)Hello 洪泛攻击 (C)槽洞攻击 (D)虫洞攻击

答案：B

86. 当前无线传感器网络面临多种攻击技术，其中（）是指攻击节点伪装成具有多个身份标识的节点，当通过该节点的一条路由遭到破坏时，网络会选择另一条路由，但由于其具有多重身份标识，实际上还是通过了该攻击节点。

(A)女巫攻击 (B)Hello 洪泛攻击 (C)槽洞攻击 (D)虫洞攻击

答案：A

87. 当前无线传感器网络仍然面临面临着多种攻击技术。以下不属于无线传感器网络面临的攻击技术的是（）。

(A)路由欺骗攻击 (B)选择性数据转发攻击 (C)槽洞攻击 (D)错误注入攻击

答案：D

88. 以下（）为网络安全等级保护对物理与硬件安全的标准。

(A)《信息安全技术 信息系统物理安全技术要求》(B)《信息安全管理标准》 (C)《信息技术设备的安全》 (D)《计算机场地通用规范》

答案：A

89. 以下（）不是建筑物方面的标准

(A)《电子信息系统机房设计规范》 (B)《计算机场地通用规范》 (C)《建筑设计防火规范》 (D)《信息安全管理标准》

答案：D

90. （）是指攻击者在非授权的情况下，非法获取用户的敏感信息，如网络重要配置文件、用户账号

(A)信息泄漏攻击 (B)完整性破坏攻击 (C)拒绝服务攻击 (D)非法使用攻击

答案：A

91. （）是指攻击者在非授权的情况下，对用户的信息进行修改，如修改电子交易的金额。

(A)信息泄漏攻击 (B)完整性破坏攻击 (C)拒绝服务攻击 (D)非法使用攻击

答案：B

92. （）是指攻击者通过强制占用有限的资源，如信道/带宽、存储空间等资源，使得服务

器崩溃或资源耗尽而无法对外继续提供服务。

(A)信息泄漏攻击 (B)完整性破坏攻击 (C)拒绝服务攻击 (D)非法使用攻击

答案：C

93. （）是指攻击者在非授权的情况下，使用计算机或网络系统服务，从而使得网络系统提供错误的服务。

(A)信息泄漏攻击 (B)完整性破坏攻击 (C)拒绝服务攻击 (D)非法使用攻击

答案：D

94. （）是网络攻击的发起者，也是网络攻击的受益者

(A)攻击者 (B)安全漏洞 (C)被攻击者 (D)攻击工具

答案：A

95. （）是指存在于网络系统中的、可被攻击者利用从而执行攻击的安全缺陷

(A)攻击者 (B)安全漏洞 (C)被攻击者 (D)攻击工具

答案：B

96. （）是指攻击者对目标网络实施攻击的一系列攻击手段、策略与方法

(A)攻击者 (B)安全漏洞 (C)被攻击者 (D)攻击工具

答案：D

97. （）是指攻击者对目标网络和系统进行合法、非法的访问

(A)攻击者 (B)安全漏洞 (C)攻击访问 (D)攻击工具

答案：C

98. 下列不属于网络防御技术的是（）

(A)防火墙技术 (B)访问控制技术 (C)加密技术 (D)拒绝服务技术

答案：D

99. （）用于对计算机或用户的身份进行鉴别与认证

(A)防火墙技术 (B)访问控制技术 (C)加密技术 (D)身份认证技术

答案：D

100. （）用于对计算机或用户对于资源的访问权限进行鉴别与限制

(A)防火墙技术 (B)访问控制技术 (C)加密技术 (D)身份认证技术

答案：B

101. （）通过在网络系统中收集信息并进行分析，以发现网络系统中违反安全策略的行为和攻击

(A)防火墙技术　(B)访问控制技术　(C)入侵检测技术　(D)身份认证技术

答案：C

102. 防火墙设置在（）

(A)内网内　(B)内网与外网之间　(C)任意网络　(D)不同网络区域边界

答案：D

103. 防火墙按照概念划分，不包括（）

(A)软件防火墙　(B)应用代理网关防火墙　(C)状态检测防火墙　(D)自适应代理网关防火墙

答案：A

104. 包过滤防火墙可通过简单地在（）上添加过滤规则实现

(A)路由器　(B)网关　(C)物理层　(D)中继

答案：A

105. 从实现原理上分，防火墙的技术包括四大类。其中包过滤防火墙工作在哪个层（）

(A)物理层　(B)网络层　(C)应用层　(D)会话层

答案：B

106. 下列不属于防火墙硬件结构划分的是（）

(A)协议安全防火墙　(B)软件防火墙　(C)硬件防火墙　(D)芯片级防火墙

答案：A

107. 防火墙按应用部署位置划分不包括（）

(A)边界防火墙　(B)个人防火墙　(C)分布式防火墙　(D)集中式防火墙

答案：D

108. 下列不属于软件防火墙缺点的是（）

(A)代码庞大　(B)安装成本高　(C)售后支持成本高　(D)漏洞多

答案：D

109. 防火墙按性能划分不包括（）

(A)十兆级防火墙　(B)千兆级防火墙　(C)万兆级防火墙　(D)十万兆级防火墙

答案：D

110. 防火墙的功能不包括（）

(A)数据包状态检测过滤　(B)应用代理　(C)网络地址转换　(D)防止内网病毒传播

答案：D

111. 应用代理是防火墙提供的主要功能之一，其中应用代理的功能不包括（）

(A)鉴别用户身份 (B)访问控制 (C)阻断用户与服务器的直接联系 (D)防止内网病毒传播

答案：D

112. 数据包内容过滤是防火墙提供的主要功能之一，其中数据包内容过滤功能不包括（）

(A)URL 地址和关键字过滤 (B)阻止不安全内容的传输 (C)防止 Email 炸弹(D)检查通过防火墙的所有报文的数据内容

答案：D

113. 防火墙不支持哪种接入模式（）

(A)透明 (B)网关 (C)分布 (D)混合

答案：C

114. 防火墙不阻止下列哪种网络数据包（）

(A)来自未授权的源地址且目的地址为防火墙地址的所有入站数据包 (B)源地址是内部网络地址的所有入站数据包 (C)包含 ICMP 请求的所有入站数据包(D)来自授权的源地址

答案：D

115. 大多数防火墙平台都使用（）作为它们执行安全控制的机制

(A)不规则集 (B)数据集 (C)规则集 (D)IP 地址

答案：C

116. （）是防火墙环境设计者的基本原则。

(A)保持简单原则 (B)设备专用原则 (C)深度防御原则 (D)注意内部威胁原则

答案：A

117. 防火墙选购要点不包括（）。

(A)安全性 (B)高效性 (C)价格高 (D)配置方便性

答案：C

118. 通常情况下，下列哪种关于防火墙的说法不对？（）

(A)内部网络可以无限制地访问外部网络以及 DMZ (B)DMZ 可以访问内部网络 (C)外部网络可以访问 DMZ 的服务器的公开端口 (D)外部网络不能访问内部网络以及防火墙

答案：B

119. 防火墙环境下各种应用服务器的放置不必遵守以下哪种原则（）。

(A)通过边界路由过滤设备保护外部网络可访问的服务器，或者将它们放置在外部 DMZ 中 (B)绝不可将外部网络可访问的服务器放置在内部保护网络中 (C)根据外部服务器的敏感程度和访问方式，将它们放置在内部防火墙之后 (D)尽量隔离各种服务器，防止一个服务器被攻破后危及其他服务器的安全

答案：C

120. 入侵检测系统不包括下面哪个功能模块（）

(A)信息源 (B)包过滤 (C)分析引擎 (D)响应

答案：B

121. 入侵检测系统的主要作用不包括（）

(A)抗 DoS/DDoS 攻击 (B)对入侵事件和过程作出实时响应 (C)防火墙的合理补充 (D)系统动态安全的核心技术之一

答案：A

122. 入侵防御系统的作用不包括（）

(A)对常规网络通信中的恶意数据包进行检测 (B)阻止入侵活动 (C)预先对攻击性的数据包进行自动拦截 (D)进行网络访问控制

答案：D

123. CIDF 将入侵检测系统分成四组件，不包括

(A)事件产生器 (B)事件关系库 (C)事件分析器 (D)响应单元

答案：B

124. 入侵检测系统按收集的待分析的信息来源分类不包括

(A)基于主机的入侵检测系统 (B)基于网络的入侵检测系统 (C)基于物理层的入侵检测系统 (D)基于应用的入侵检测系统

答案：C

125. 入侵检测系统的发展趋势不包括

(A)分布式入侵检测 (B)网络层入侵检测 (C)应用层入侵检测 (D)智能入侵检测

答案：B

126. 下列不属于入侵防御系统种类的是（）

(A)基于主机的入侵防御系统　(B)基于应用的入侵防御系统　(C)基于网络的入侵防御系统　(D)基于协议的入侵防御系统

答案：D

127. 目前入侵检测系统的成熟技术不包括（）

(A)网络识别　(B)特征匹配　(C)协议分析　(D)异常检测

答案：A

128. 以下关于漏洞的说法错误的是（）

(A)漏洞的分类方法很多，也没有统一的标准。　(B)漏洞具有时间与空间特性　(C)系统的环境变量发生变化时产生的漏洞为开放式协议漏洞　(D)程序在实现逻辑中没有考虑一些意外情况为异常处理疏漏

答案：C

129. 漏洞按成因分类不包括（）

(A)输入验证错误　(B)访问验证错误　(C)输出验证错误　(D)异常处理的疏漏

答案：C

130. 一次完整的网络安全扫描不包括以下哪个阶段（）

(A)发现目标主机或网络　(B)根据检测到的漏洞看能否解决　(C)发现目标后进一步搜集目标信息　(D)根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞

答案：B

131. 下面哪个不属于端口扫描的经典方法（）

(A)TCP 全连接扫描　(B)TCP 半连接扫描　(C)IP 反转标识扫描　(D)FTP 跳跃扫描

答案：C

132. 一次完整的网络安全扫描可以分为三个阶段。网络安全扫描的第一阶段是（）

(A)发现目标后进一步搜集目标信息　(B)发现目标主机或网络。　(C)根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。　(D)进行端口扫描

答案：B

133. 一次完整的网络安全扫描可以分为三个阶段。网络安全扫描的第二阶段是（）

(A)发现目标后进一步搜集目标信息　(B)发现目标主机或网络。　(C)根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。　(D)进行端口扫描

答案：A

134. 一次完整的网络安全扫描分为三个阶段。网络安全扫描的第三阶段是（）

(A)发现目标后进一步搜集目标信息 (B)发现目标主机或网络。 (C)根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。 (D)进行端口扫描

答案：C

135. 基于网络的漏洞扫描器的组成部分不包括（）

(A)漏洞数据库模块 (B)用户配置控制台模块 (C)发现漏洞模块 (D)当前活动扫描知识库模块

答案：C

136. 基于网络的漏洞扫描器不具有如下哪个优点（）

(A)价格便宜 (B)维护简便 (C)不需要实时监督 (D)能直接访问目标设备的文件系统

答案：D

137. 第一代隔离技术是（）

(A)硬件卡隔离 (B)完全的物理隔离 (C)数据转播隔离 (D)空气开关隔离

答案：B

138. 第二代隔离技术是（）

(A)硬件卡隔离 (B)完全的物理隔离 (C)数据转播隔离 (D)空气开关隔离

答案：A

139. 第三代隔离技术是（）

(A)硬件卡隔离 (B)完全的物理隔离 (C)数据转播隔离 (D)空气开关隔离

答案：C

140. 第四代隔离技术是（）

(A)硬件卡隔离 (B)完全的物理隔离 (C)数据转播隔离 (D)空气开关隔离

答案：D

141. （）是一种实现网络隔离技术的设备。

(A)入侵检测技术 (B)隔离网闸 (C)路由器 (D)网关

答案：B

142. 下列关于拒绝服务攻击说法错误 的是（）

(A)来自网络的拒绝服务攻击可以分为停止服务和消耗资源两类 (B)拒绝服务攻击的目的是利用各种攻击技术使服务器或者主机等拒绝为合法用户提供服务 (C)停止服务意味

着毁坏或者关闭用户想访问的特定的服务　　(D)停止服务是目前最流行的拒绝服务攻击方式

答案：D

143. 下列有关拒绝服务攻击说法错误的是（）

(A)拒绝服务攻击的目的是利用各种攻击技术使服务器或者主机等拒绝为合法用户提供服务　　(B)来自网络的拒绝服务攻击可以分为停止服务，开始服务和消耗资源三类　　(C)消耗资源是目前最流行的拒绝服务攻击方式　(D)拒绝服务攻击中的 90%是 SYN 洪泛攻击

答案：B

144. 来自网络的拒绝服务攻击可以分为停止服务和消耗资源两类。攻击特点不包括以下哪个（）

(A)多源性、特征多变性　　(B)攻击目标与攻击手段多样性　(C)隐蔽性　(D)开放性

答案：D

145. 拒绝服务攻击数据包中会经常改变的属性不包括以下哪个（）

(A)源 IP 地址 (B)源端口　　(C)目的 IP 地址　　(D)其他 IP 头参数

答案：C

146. 下列关于 Botnet 说法错误 的是（）

(A)用 Botnet 发动 DDoS 攻击　　(B)Botnet 的显著特征是大量主机在用户不知情的情况下，被植入了控制程序　　(C)拒绝服务攻击与 Botnet 网络结合后攻击能力大大削弱　(D)Botnet 可以被用来传播垃圾邮件、窃取用户数据、监听网络和扩散恶意病毒等

答案：C

147. 下列不能做到检测和抵御拒绝服务攻击的是（）

(A)弱口令检查　　(B)TCP SYN Cookie　　(C)TCP 状态检测　(D)HTTP 重定向

答案：A

148. （）是一种基于协议特征分析的 DoS/DDoS 检测技术

(A)弱口令检查　　(B)TCP SYN Cookie　　(C)TCP 状态检测　(D)HTTP 重定向

答案：B

149. （）技术的基本思想是利用均衡负载等技术提高服务器系统的处理能力或者网络带宽，使得服务器在接收大量攻击数据包的情况下仍然可以提供服务。

(A)Over－provisioning(超量供应)　(B)TCP SYN Cookie　(C)TCP 状态检测　(D)HTTP 重定向

答案：A

150. （）是 DoS/DDoS 发生时针对 Web 服务器的保护

(A)弱口令检查　(B)TCP SYN Cookie　(C)TCP 状态检测　(D)HTTP 重定向

答案：D

151. （）技术在 DoS/DDoS 攻击发生时将所有发往攻击目标的数据包抛弃

(A)Blackholing　(B)Random Drop　(C)Over－provisioning(超量供应)　(D)HTTP 重定向

答案：A

152. （）技术在攻击发生时随机地抛弃一些发往攻击目标的数据包

(A)Blackholing　(B)Random Drop　(C)TCP 状态检测　(D)Over－provisioning(超量供应)

答案：B

153. 哪个方法不能应对针对口令的字典攻击？

(A)定期更换口令　(B)设置复杂密码　(C)预设口令　(D)设置锁定阈值

答案：C

154. 哪个不是基于动态口令的认证技术的优点？

(A)不确定性　(B)动态性　(C)一次性　(D)可重复性

答案：D

155. （）身份鉴别技术依赖于特殊的硬件设备来提取生物特征信息，且其准确性和稳定性与传统的认证技术相比相对较低

(A)基于生物特征　(B)主流的身份鉴别　(C)基于用户知识的身份鉴别技术　(D)典型的身份鉴别系统

答案：A

156. 哪个是基于生物特征的认证技术的缺陷？（）

(A)难以提取　(B)依赖于特殊的硬件设备　(C)生物特征很多　(D)生物特征很复杂

答案：B

157. RADIUS 服务器不可通过（）方式来认证用户

(A)CHAP 认证(B)PAP 认证　(C)端到端认证　(D)UNIX 登录

答案：C

158. OpenID 身份鉴别协议的参与方没有（）？

(A)OpenID 提供方 (B)远程控制方　(C)依赖方　(D)终端用户

答案：B

159. OpenID 提供方的功能是?

(A)提供申明 (B)执行身份鉴别 (C)响应用户信息 (D)授权

答案：D

160. 下面哪个不是 SAML(Security Assertion Markup Language，安全性断言标记语言)应用的实现组成?

(A)主体 (B)服务提供者　(C)审查者　(D)身份提供者

答案：C

161. SAML(Security Assertion Markup Language，安全性断言标记语言)不包括哪些声明

(A)属性声明 (B)访问申明 (C)认证声明 (D)授权声明

答案：B

162. FIDO 协议提供了（）认证方式?

(A)通用授权框架 (B)访问控制 (C)非否认　(D)数据完整性框架

答案：A

163. 身份鉴别系统解决方案不包含?

(A)单点登录 (B)多因素认证　(C)联合身份 (D)单因素认证

答案：D

164. 单点登录(Single Sign On，简称 SSO)是目前比较流行的企业业务整合的解决方案之一。主要的单点登录协议不包括（）？

(A)基于 Kerberos 的单点登录协议　(B)基于 FIDO 的单点登录协议　(C)基于 SAML 的单点登录协议　(D)基于 OpenID 的单点登录协议

答案：B

165. PKI 系统组成不包含?

(A)评估机构 (B)认证机构 (C)注册机构 (D)证书撤销列表发布者

答案：A

166. PKI 系统中，下面哪个不是终端实体?

(A)PKI 证书的主体 (B)终端用户或者系统 (C)PKI 证书的使用者　(D)证书撤销列表发布

者

答案：D

167. PKI 系统中，终端实体不包含?

(A)PKI 证书的主体(B)终端用户或者系统 (C)PKI 证书的使用者 (D)数字证书与密钥对

答案：D

168. PKI 系统组成不包括?

(A)终端实体 (B)认证机构 (C)注册机构 (D)SSL

答案：D

169. PKI 提供的核心服务不包括?

(A)认证 (B)完整性 (C)密钥管理 (D)访问控制

答案：D

170. PKI 提供的核心服务不包括哪个信息安全的要求?

(A)访问安全性 (B)真实性 (C)完整性 (D)保密性

答案：A

171. PKI 提供的最基本的服务是（）

(A)认证 (B)完整性 (C)密钥管理 (D)简单机密性

答案：A

172. PKI 认证方式特别适合于（）的用户群。

(A)大规模网络和大规模用户群 (B)小规模网络和小规模用户群 (C)大规模网络和小规模用户群 (D)小规模网络和大规模用户群

答案：A

173. PKI 技术的典型应用不包括?

(A)安全电子邮件 (B)匿名登陆 (C)安全 Web 服务 (D)VPN 应用

答案：B

174. PKI 部署是一个复杂的问题，PKI 技术的部署不需要考虑?

(A)组织信任体系的目标 (B)资源引进和资源外包 (C)安全应用 (D)个人意愿

答案：D

175. 基于客户端—服务器的数字版权管理系统优点是?

(A)不需要依靠服务器分发内容 (B)不会导致服务器崩溃 (C)每个用户都可以使用

(D)集中管理内容的提供源

答案：D

176. 基于 P2P 的数字版权管理系统优点是？

(A)不需要依靠服务器分发内容 (B)不会导致服务器崩溃 (C)任何人都可以成为数字内容的提供者 (D)集中管理内容的提供源

答案：C

177. 实现数字版权保护系统的版权保护功能的关键是？

(A)采用合适的侦听技术 (B)采用合适的密码技术 (C)采用合适的获得数字内容授权的技术 (D)采用有效的防篡改机制

答案：B

178. 数字版权保护系统中的密码技术没有？

(A)对称与非对称加密 (B)数字签名和单向散列函数 (C)数字证书 (D)访问控制

答案：D

179. 数字水印的特征没有？

(A)不需要带外传输 (B)透明性 (C)稳定性 (D)安全性

答案：C

180. 数字水印的特征没有？

(A)不需要带外传输 (B)透明性 (C)鲁棒性 (D)稳定性

答案：D

181. 数字水印的分类没有？

(A)鲁棒水印和脆弱水印 (B)安全水印和不安全水印 (C)对称水印和非对称水印 (D)隐藏水印和非隐藏水印

答案：B

182. 数字水印的分类没有？

(A)鲁棒水印和脆弱水印 (B)公有水印和私有水印 (C)安全水印和不安全水印 (D)隐藏水印和非隐藏水印

答案：C

183. 数字水印的应用没有？

(A)完整性保护 (B)版权保护 (C)拷贝保护 (D)拷贝追踪

答案：A

184. 隐私信息泄漏不包括?

(A)身份泄漏 (B)连接泄漏 (C)内容泄漏 (D)内存泄漏

答案：D

185. 社交网络的数据分层不包含?

(A)appliction－layer (B)activity－layer (C)registration－layer (D)networking － layer

答案：A

186. 社交网络的数据分层中哪一层包含可以唯一识别用户身份的信息?

(A)appliction－layer (B)activity－layer (C)registration－layer (D)networking － layer

答案：C

187. 衡量容灾系统的主要目标不包括?

(A)恢复点目标 (B)恢复时间目标 (C)网络恢复目标 (D)本地恢复目标

答案：D

188. 数据备份策略不包括?

(A)完全备份 (B)增量备份 (C)累计备份 (D)部分备份

答案：D

189. 以保护特定应用为目的的安全技术指的是（）。

(A)应用安全技术 (B)物理安全技术 (C)网络安全技术 (D)数据安全技术

答案：A

190. 根据同源安全策略，a.com 网页中的脚本只能修改（）网页中的内容。

(A)a.com (B)ab.com (C)b.com (D)be.com

答案：A

191. 能够让不受信任的网页代码、JavaScript 代码在一个受到限制的环境中运行，从而保护本地桌面系统的安全的是（）。

(A)同源安全策略 (B)浏览器沙箱 (C)XSS 过滤 (D)基于信任访问

答案：B

192. Cookie 的信息是加密的，内容主要为( )加密信息。

(A)XSS (B)HASH (C)MD5 (D) RSA

答案：C

193. Web 服务器可以使用（）严格约束并指定可信的内容来源。

(A)内容安全策略 (B)同源安全策略 (C)访问控制策略 (D)浏览器沙箱

答案：A

194. 跨站脚本攻击的主要防御手段为输入检查和（）。

(A)输出检查 (B)验证码 (C)反 XSS 令牌 (D)请求检查

答案：A

195. 下列关于跨脚本攻击说法错误的是（）。

(A)跨站脚本(XSS)攻击，是指攻击者在 HTML 内容注入恶意脚本代码，从而绕过浏览器的安全检测，获取 Cookie、页面内容等敏感信息。 (B)针对 XSS 攻击的防御手段主要分两类，即输入检查和输出检查。 (C)输入检查，是指对用户的输入进行检查，检查用户的输入是否符合一定规则。 (D)最常见的输入检查方式是对网页内容进行编码。

答案：D

196. 下面不属于跨站请求伪造攻击防御的是（）。

(A)验证码 (B)请求检查 (C)反 CSRF 令牌 (D)输出检查

答案：D

197. 在提交请求时要求（），确保了请求确实是用户提交的而不是 CSRF 攻击自动提交的。

(A)用户请求输入 (B)验证码 (C)请求检查 (D)反 CSRF 令牌

答案：B

198. （）指 HTTP 请求的发起者，在 HTTP 中该字段指明该请求是由哪个源(可简单理解为哪个网站)发起

(A)请求 (B)验证码 (C)输入检查 (D)反 CSRF 令牌

答案：A

199. （）不属于常见的网页篡改技术

(A)木马植入 (B)病毒攻击 (C)侵入漏洞 (D)限制管理员权限

答案：D

200. 网页防篡改技术主要分为两类，阻止黑客入侵和阻止黑客反入侵。以下不属于阻止黑客入侵行为的是（）。

(A)对管理员的权限进行限制 (B)对网页请求参数进行验证 (C)安装病毒防火墙 (D)轮询检测

答案：D

201. 网页防篡改技术主要分为两类，阻止黑客入侵和阻止黑客反入侵。以下不属于阻止黑客反入侵行为的是（）。

(A)对管理员的权限进行限制　(B)轮询检测　(C)事件触发技术　(D)核心内嵌技术

答案：A

202. 下列技术中利用一个网页读取和检测程序，通过周期性地从外部逐个访问网页来判断网页合法性的是（）。

(A)轮询检测　(B)事件触发技术　(C)核心内嵌技术　(D)对网页请求参数进行验证

答案：A

203. （）利用这些事件，通过特定的高效算法对网页文件的修改行为进行合法性检查。

(A)轮询检测　(B)事件触发技术　(C)核心内嵌技术　(D)对网页请求参数进行验证

答案：B

204. 将篡改检测模块嵌入用户的 Web 服务器中的是（）。

(A)轮询检测　(B)事件触发技术　(C)核心内嵌技术　(D)对网页请求参数进行验证

答案：C

205. （）不属于内容过滤的三个具体方面。

(A)过滤互联网请求　(B)过滤流入的内容　(C)过滤流出的内容　(D)过滤不良信息

答案：D

206. 阻止用户浏览不适当的内容或站点指的是（）。

(A)过滤互联网请求　(B)过滤流入的内容　(C)过滤流出的内容　(D)过滤不良信息

答案：A

207. 阻止潜在的攻击进入用户的网络系统指的是（）。

(A)过滤互联网请求　(B)过滤流入的内容　(C)过滤流出的内容　(D)过滤不良信息

答案：B

208. 阻止敏感数据的泄漏指的是（）。

(A)过滤互联网请求　(B)过滤流入的内容　(C)过滤流出的内容　(D)过滤不良信息

答案：C

209. 不属于基于内容的过滤技术的是（）。

(A)关键字过滤技术　(B)URL 过滤　(C)机器学习技术　(D)启发式内容过滤技术

答案：B

210. 基于源的过滤技术通过内容的来源进行过滤，以下属于基于源的过滤技术的有（）

(A)IP 包过滤　(B)内容分级审查　(C)关键字过滤　(D)启发式内容过滤

答案：A

211. （）属于基于内容的过滤技术

(A)IP 包过滤　(B)内容分级审查　(C)URL 过滤　(D)DNS 过滤

答案：B

212. 下列基于内容的过滤技术中在我国没有得到广泛应用的是(　)。

(A)内容分级审查　(B)关键字过滤技术　(C)启发式内容过滤技术　(D)机器学习技术

答案：A

213. 垃圾邮件过滤技术主要是通过电子邮件的源或者内容进行过滤，（）属于垃圾邮件过滤技术的一种。

(A)安全 DNS　(B)内容分级检查　(C)加密　(D)白名单

答案：D

214. 下列不属于垃圾邮件过滤技术的是（）。

(A)软件模拟技术　(B)贝叶斯过滤技术　(C)关键字过滤技术　(D)黑名单技术

答案：A

215. 会让一个用户的删除操作去警告其他许多用户的垃圾邮件过滤技术是(　)。

(A)黑名单　(B)白名单　(C)实时黑名单　(D)分布式适应性黑名单

答案：D

216. 不需要经常维护的垃圾邮件过滤技术是（）。

(A)指纹识别技术　(B)简单 DNS 测试　(C)黑名单技术　(D)关键字过滤

答案：B

217. 针对垃圾邮件问题，对 SMTP 进行改进和完善是当前关注的重点，（）属于 SMTP 改进

技术

(A)白名单　(B)反向查询技术　(C)指纹识别技术　(D)简单 DNS 测试

答案：B

218. 以下不属于邮件服务器的安全管理的是（）。

(A)SMTP 身份认证(B)病毒过滤　(C)安全审计　(D)DNS 测试

答案：D

219. SSL 协议提供用户和商户之间交换电子支付信息的安全通道，但不保证支付（）。

(A)信息的机密性　(B)信息的完整性　(C)持卡人的合法性　(D)非否认性

答案：D

220. 下列关于操作系统的说法错误的是（）

(A)操作系统在概念上一般分为两部分，即内核(Kernel)和壳(Shell)　(B)在通用操作系统中，壳(Shell)实现一些操作，如同步、进程间通信、信息传递及中断处理　(C)应用程序建立在操作系统之上　(D)操作系统是计算机系统的基础，它负责进行处理器管理、存储管理、文件管理、设备管理和作业管理等

答案：B

221. 常见的操作系统不包括（）

(A)Windows　(B)UNIX/Linux(C)Android　(D)OSI

答案：D

222. 作为操作系统最核心、最基础的构件，负责提供基础性、结构性的功能的是（）。

(A)内核　(B)壳(shell)　(C)外核　(D)中核

答案：A

223. （）包裹了与硬件直接交流的内核，将用户命令行解析为操作系统内部指令

(A)内核　(B)壳(shell)　(C)外核　(D)中核

答案：B

224. 下列不属于操作系统安全要素的是（）

(A)用户认证　(B)内部进程间通信的同步　(C)共享的实现　(D)模式识别

答案：D

225. 操作系统的( )指的是操作系统必须识别请求访问的每个用户，并要查明该用户与其声称的身份是否相符，最普遍的认证机制是用户名 + 密码。

(A)用户认证　(B)文件和 I/O 设备的访问控制　(C)共享的实现　(D)存储器保护

答案：A

226. 操作系统的( )指的是每个用户的程序必须在安全的存储器区域内运行，这种保护还需要控制用户对程序空间受限制部分的访问

(A)用户认证 (B)文件和 I/O 设备的访问控制 (C)共享的实现 (D)存储器保护

答案：D

227.操作系统的( )指的是操作系统必须保护用户和系统文件，防止未经授权的用户进行访问。类似地，I/O 设备的使用也必须受到保护

(A)用户认证 (B)文件和 I/O 设备的访问控制 (C)共享的实现 (D)存储器保护

答案：B

228. 操作系统的( )指的是提供给用户使用的一般对象必须受到控制，如允许并行或同步的机制能够确保一个用户不致对其他用户产生干扰

(A)用户认证 (B)文件和 I/O 设备的访问控制 (C)共享的实现 (D)对一般目标的定位和访问控制

答案：D

229. 操作系统的( )指的是所有用户都期望系统提供 CPU 的使用和其他服务，以使任何用户不会无限期地缺乏服务。硬件时钟结合调度规则可以提供这种公平性

(A)保证公平服务 (B)文件和 I/O 设备的访问控制 (C)共享的实现 (D)对一般目标的定位和访问控制

答案：A

230. 操作系统的( )指的是正在执行的进程有时需要与其他进程通信或者需要使它们对共享资源的访问同步

(A)保证公平服务 (B)内部进程间通信的同步 (C)共享的实现 (D)对一般目标的定位和访问控制

答案：B

231. 操作系统的( )指的是资源应该恰当地为用户获取，共享则需要保证资源的完整性和一致性

(A)用户认证 (B)文件和 I/O 设备的访问控制 (C)共享的实现 (D)存储器保护

答案：C

232. 我国制定了强制性国家标准《计算机信息系统安全保护等级划分准则》，其中属于第一级的是（）

(A)用户自主保护级　(B)系统审计保护级　(C)结构化保护级　(D)访问验证保护级

答案：A

233. 我国制定了强制性国家标准《计算机信息系统安全保护等级划分准则》，其中属于第二级的是（）

(A)用户自主保护级　(B)系统审计保护级　(C)结构化保护级　(D)访问验证保护级

答案：B

234. 我国制定了强制性国家标准《计算机信息系统安全保护等级划分准则》，其中属于第三级的是（）

(A)用户自主保护级　(B)系统审计保护级　(C)结构化保护级　(D)安全标记保护级

答案：D

235. 我国制定了强制性国家标准《计算机信息系统安全保护等级划分准则》，其中属于第四级的是（）

(A)用户自主保护级　(B)系统审计保护级　(C)结构化保护级　(D)安全标记保护级

答案：C

236. 不属于设计安全操作系统应该遵循的原则的是（）

(A)最小特权　(B)基于许可的模式　(C)保护机制的经济性　(D)最大特权

答案：D

237. （）原则指的是为了将无意或恶意的攻击所造成的损失降到最低限度，每个用户和程序必须按照需知原则，尽可能使用最小特权进行操作

(A)最小特权　(B)基于许可的模式　(C)保护机制的经济性　(D)最大特权

答案：A

238. （）原则指的是系统的设计应该小而简单，且直截了当，保护系统可以被穷举测试，或者被验证，因而可以信赖

(A)最小特权　(B)基于许可的模式　(C)保护机制的经济性　(D)最大特权

答案：C

239. （）原则指的是默认的条件应该是拒绝访问，保守的设计应标识哪些应该是可存取的，

而不是标识哪些是不可存取的

(A)最小特权 (B)基于许可的模式 (C)保护机制的经济性 (D)最大特权

答案：B

240. Windows 系统中，用户组(包括本地用户组和域用户组)的使用策略不包括（）

(A)在域控制器上创建全局组 (B)给本地组授予相应的用户权限和资源许可 (C) 将 本地组放到全局组中 (D)在域中创建用户，并将其放到相应的全局组中

答案：C

241. Windows 系统的（）安全是 Windows 系统安全的核心

(A)用户账号 (B)应用程序 (C)硬件 (D)主机

答案：A

242. Windows 系统中的 （）是指一种可以包含任何用户账号的内建组

(A)全局组 (B)本地组 (C)特殊组 (D)来宾组

答案：C

243. Windows 系统中的 （）不仅可以使用本域的资源，还可以使用其他域的资源

(A)全局组 (B)本地组 (C)特殊组 (D)来宾组

答案：A

244. Windows 系统中的 （）由计算机创建，组内的成员由所在计算机的目录数据库定义，并且可以赋予组内成员一定的用户权限和对资源的访问许可

(A)全局组 (B)本地组 (C)特殊组 (D)来宾组

答案：B

245. Windows 屏蔽网络设置的方法不包括以下哪种（）

(A)禁用网上邻居属性 (B)取消网络访问权限 (C)隐藏网上邻居 (D)禁止开机启动

答案：D

246. 能帮助阻止计算机病毒和蠕虫进入用户的计算机，可以准许或取消某些连接请求的是()

(A)Windows 防火墙 (B)应用程序 (C)网上邻居 (D)windows 内核

答案：A

247. 如果需要使用多重特权用户账号,第一步是（）

(A)创建多重特权用户账号 (B)为每个特权用户创建一个普通用户账号 (C)以 root 身份登录到系统中 (D)指导每一位特权用户以普通用户身份登录到系统

答案：A

248. UNIX 系统中,运行内核程序的进程处于（）

(A)来宾态　(B)核心态　(C)访问态　(D)用户态

答案：B

249. UNIX 系统中,运行核外程序的进程处于（）

(A)来宾态　(B)核心态　(C)访问态　(D)用户态

答案：D

250. UNIX 系统中,用户程序可以通过系统调用进入核心态，运行系统调用后，又返回（）

(A)来宾态　(B)核心态　(C)访问态　(D)用户态

答案：D

251. 下列不属于标准的 UNIX 粒度划分进行控制的是（）

(A)特权用户　(B)属主　(C)属组　(D)其他人

答案：A

252. UNIX 以（）组织文件系统，这个系统包括文件和目录

(A)链表结构　(B)树型结构　(C)数组结构　(D)图型结构

答案：B

253. UNIX 以树型结构组织文件系统，这个系统包括文件和目录。rw－r－－r－－中的 r 表示（）

(A)读权　(B)写权　(C)执行权　(D)任何权利

答案：A

254. UNIX 以树型结构组织文件系统，这个系统包括文件和目录。rw－r－－r－－中的 w 表示（）

(A)读权　(B)写权　(C)执行权　(D)任何权利

答案：B

255. UNIX 以树型结构组织文件系统，这个系统包括文件和目录。rwxr－－r－－中的 x 表示（）

(A)读权　(B)写权　(C)执行权　(D)任何权利

答案：C

256. UNIX 中的 backup 用来完成（）

(A)UNIX 文件的备份　(B)UNIX 文件的解压　(C)UNIX 文件的压缩　(D)UNIX 文件的删除

答案：A

257. UNIX 系统提供了几条功能强大的命令，用于文件系统的备份和恢复，下面不具有这些功能的命令是（）

(A)backup　(B)cpio　(C)tar　(D)chmod

答案：D

258. Linux 系统提供了一些查看进程信息的系统调用，下面不具有上述功能的命令是（）

(A)who　(B)ps　(C)top　(D)cd

答案：D

259. Linux 中的（）命令和 ps 命令的基本作用相同，即显示系统当前的进程及其状态。但是该命令是一个动态显示过程

(A)who　(B)ps　(C)top　(D)cd

答案：C

260. UNIX/Linux 环境下最流行的 Web 服务器是 Apache 服务器。不属于 Apache 服务器的安全缺陷的是（）

(A)可以利用 HTTP 对其进行 DoS 攻击　(B)导致缓冲区溢出攻击　(C)让攻击者获得 Root 权限　(D)攻击者植入木马病毒

答案：D

261. DoS 攻击是一种对网络危害巨大的恶意攻击，其中，具有代表性的攻击手段不包括（）

(A)SYN 洪泛　(B)ICMP 洪泛 (C)UDP 洪泛　(D)Apache 洪泛

答案：D

262. 下列说法错误的是（）

(A)Android 基于 Linux 内核，保留了用户和组的概念　(B)Android 保留了 Linux 基于用户和组的访问控制机制　(C)Android 具体的访问控制与 Unix/Linux 访问控制相同

(D)Android 用户的添加方式与 Linux 相同

答案：D

263. Android 使用（）作为操作系统

(A)Windows (B)Chrome OS (C)Linux (D)Mac

答案：C

264. （）指的是基于寄存器的虚拟机 Dalvik

(A)操作系统层 (B)Android 运行环境 (C)应用程序框架 (D)应用程序

答案：B

265. （）指 Android 为应用程序开发者提供的 APIs，包括各种各样的控件

(A)操作系统层 (B)Android 运行环境 (C)应用程序框架 (D)应用程序

答案：C

266. Android 应用程序通常指的是以 APK 包形式下载至手机终端的应用，包内还包含各种（）

(A)描述文件 (B)框架文件 (C)Manifest 文件 (D)资源文件

答案：D

267. Android 系统把 Permission 划分为不同的安全级别，其中最低的是（）

(A)normal (B)dangerous (C)signature (D)signature or system

答案：A

268. Android 中含有多种隔离机制，其中（）是为了实现不同应用程序进程之间的隔离

(A)黑箱机制 (B)白箱机制 (C)沙箱机制 (D)暗箱机制

答案：C

269. （）能够为用户及应用程序提供数据访问界面，并具有对数据库进行管理、维护等多种功能

(A)数据库 (B)数据库管理系统 (C)数据库软件 (D)数据库界面

答案：B

270. 数据库中插入语句所使用的数据操纵语言是（）

(A)insert (B)alter (C)truncate (D)update

答案：A

271. GRANT INSERT，UPDATE，DELETE

ON authors

TO Mary

这个 SQL 语句表示（）

(A)修改表名 (B)修改表的列类型 (C)收回相应权限 (D)授予相应权限

答案：D

272. REVOKE CREATET ABLE，CREATE DEFAULT

FROM Mary，John

这个 SQL 语句表示（）

(A)修改表名 (B)修改表的列类型 (C)收回相应权限 (D)授予相应权限

答案：C

273. 数据库中的数据库级别所拥有的访问功能是（）

(A)判断用户能否使用、访问数据库里的数据对象，包括表、视图、存储过程 (B)判断用户能否访问关系里面的内容 (C)判断用户能否访问关系中的一行记录的内容 (D)判断用户能否访问表关系中的一个属性列(字段)的内容

答案：A

274. 数据库中的表级所拥有的访问功能是（）

(A)判断用户能否使用、访问数据库里的数据对象，包括表、视图、存储过程 (B)判断用户能否访问关系里面的内容 (C)判断用户能否访问关系中的一行记录的内容 (D)判断用户能否访问表关系中的一个属性列(字段)的内容

答案：B

275. 数据库中的行级所拥有的访问功能是（）

(A)判断用户能否使用、访问数据库里的数据对象，包括表、视图、存储过程 (B)判断用户能否访问关系里面的内容 (C)判断用户能否访问关系中的一行记录的内容 (D)判断用户能否访问表关系中的一个属性列(字段)的内容

答案：C

276. 数据库中的属性级访问控制所拥有的控制用户访问数据对象的粒度大小为（）

(A)判断用户能否使用、访问数据库里的数据对象，包括表、视图、存储过程 (B)判断用户能否访问关系里面的内容 (C)判断用户能否访问关系中的一行记录的内容 (D)判断用户能否访问表关系中的一个属性列(字段)的内容

答案：D

277. 以下哪个不属于关系数据库管理系统（）

(A)Oracle (B)MySQL (C)SQL Server (D)Hbase

答案：D

278. （）是指验证用户的身份是否真实、合法。

(A)用户身份鉴别 (B)用户角色 (C)数据库授权 (D)数据库安全

答案：A

279. 在数据库管理系统中，数据对象的存取权限 R 表示（）

(A)更新数据 (B)读数据 (C)向关系中添加记录 (D)删除关系里面的记录

答案：B

280. 在数据库管理系统中，数据对象的存取权限 U 表示（）

(A)更新数据 (B)读数据 (C)向关系中添加记录 (D)删除关系里面的记录

答案：A

281. 在数据库管理系统中，数据对象的存取权限 A 表示（）

(A)更新数据 (B)读数据 (C)改关系的属性 (D)删除关系里面的记录

答案：C

282. 在数据库管理系统中，数据对象的存取权限 D 表示（）

(A)更新数据 (B)读数据 (C)改关系的属性 (D)删除关系里面的记录

答案：D

283. 在数据库管理系统中，数据对象的存取权限 DR 表示（）

(A)更新数据 (B)读数据 (C)删除关系 (D)删除关系里面的记录

答案：C

284. 数据库管理系统 DBMS 对于用户的访问存取控制的隔离原则指的是（）

(A)用户的权限不受限制 (B)用户只能存取他自己所有的和已经取得授权的数据对象

(C)用户只能按他所取得的数据存取方式存取数据，不能越权 (D)用户可以越权

答案：B

285. 数据库管理系统 DBMS 对于用户的访问存取控制的控制原则指的是（）

(A)用户的权限不受限制 (B)用户只能存取他自己所有的和已经取得授权的数据对象

(C)用户只能按他所取得的数据存取方式存取数据，不能越权 (D)用户可以越权

答案：C

286. 数据库中的权限分配在数据库中可以用（）表示

(A)权限点 (B)权限向量 (C)权限校验矩阵 (D)权限图型结构

答案：C

287. 数据库中，CREATE VIEW titleview 这个 SQL 语句指的是（）

(A)创建数据库　(B)创建表　(C)创建视图　(D)创建分区

答案：C

288. 下列关于数据库加密的应用特点描述错误的是（）

(A)数据库数据是共享的　(B)数据库关系运算中参与运算的最小单位是字段　(C)数据库密码系统应采用对称密钥　(D)库名、表名、记录名、字段名都应该具有各自的子密钥

答案：C

289. 数据库关系运算中参与运算的最小单位是（）

(A)数据库　(B)表　(C)记录　(D)字段

答案：D

290. 数据库中最小的加密单位是（）

(A)数据库　(B)表　(C)记录　(D)字段

答案：D

291. 数据库中分组用 SQL 语句（）来实现

(A)select (B)sum　(C)group by　(D)order by

答案：C

292. 数据库管理系统保护轮廓（DBMS.PP）明确了三种数据库资产，不属于这三种的是（）

(A)安全数据　(B)数据库客体　(C)控制数据　(D)审计数据

答案：A

293. 有关数据库加密，下面说法不正确的是（）

(A)索引字段不能加密　(B)关系运算的比较字段不能加密　(C)字符串字段不能加密　(D)表间的连接码字段不能加密

答案：C

294. 关于用户角色，下面说法正确的是（）

(A)SQL Server 中，数据访问权限只能赋予角色，而不能直接赋予用户　(B)角色与身份认证无关　(C)角色与访问控制无关　(D)角色与用户之间是一对一的映射关系

答案：A

295. 以下防范措施不能防范 SQL 注入攻击的是（）

(A)配置 IIS　(B)在 Web 应用程序中，将管理员账号连接数据库 (C)去掉数据库不需要

的函数、存储过程　　(D)检查输入参数

答案：B

296. 一个典型的计算机病毒的生命周期包括（）个阶段。

(A)二　　(B)三　　(C)四　　(D)五

答案：C

297. 一个典型的计算机病毒的生命周期不包括以下（）阶段。

(A)休眠阶段　(B)传播阶段　(C)触发阶段　(D)预备阶段

答案：D

298. 以下关于木马错误的是（）。

(A)木马(Trojan)是一种提供正常功能的程序，但是一旦触发，就会在后台执行未经授权的操作或破坏行为　　(B)与一般的计算机病毒相同，单纯的木马具备自我复制能力。　(C)单纯的木马不会主动感染系统中的其他组件。　　(D)木马通过某些方式吸引用户下载并安装，在执行时在计算机系统中打开接口，为攻击者窃取信息、破坏或远程操作目标主机提供方便。

答案：B

299. 僵尸程序通过感染数以千计的主机，形成（）控制的网络。

(A)一对一　　(B)一对多　　(C)多对一　　(D)多对多

答案：B

300. RootKit 根据其特点分类不包括（）

(A)持久性存储　　(B)基于内存　(C)用户态　　(D)内部模式

答案：D

301. 计算机病毒，是指通过修改其他程序进行感染，并对系统造成破坏的一段代码，（）不属于计算机病毒的特性。

(A)传染性　　(B)破坏性　　(C)隐蔽性　　(D)可用性

答案：D

302. 计算机病毒，是指通过修改其他程序进行感染，并对系统造成破坏的一段代码，（）不属于计算机病毒的组成部分。

(A)引导部分　(B)传染部分　(C)休眠部分　(D)干扰或破坏部分

答案：C

303. 计算机病毒，是指通过修改其他程序进行感染，并对系统造成破坏的一段代码，（）不

属于计算机病毒的组成部分。

(A)引导部分 (B)传染部分 (C)触发部分 (D)干扰或破坏部分

答案：C

304. 以下不属于 Android 平台的恶意代码入侵形式的是（）。

(A)重打包 (B)更新攻击 (C)下载攻击 (D)病毒攻击

答案：D

305. 下列不属于 Android 恶意软件的攻击目的的是（）。

(A)提升权限 (B)远程控制 (C)恶意吸费 (D)逃避检测

答案：D

306. 按照壳的目的和作用，加壳工具可以分为（）类。

(A)二 (B)三 (C)四 (D)五

答案：A

307. 以下关于软件逆向工程说法错误的是（）。

(A)恶意软件开发者利用逆向工程定位操作系统和应用程序的漏洞，并利用该漏洞开发恶意软件。 (B)防病毒软件开发者利用逆向工程分析恶意软件的步骤、行为和对系统造成的破坏，进而提出防范机制。 (C)很多应用程序使用公有加解密算法，可利用逆向工程分析其算法的实现细节和缺陷。 (D)如果某些软件进行了特殊的设计或具备难以实现的功能，其竞争者可能通过对组件的逆向，在自己的产品中推出同样的功能。

答案：C

308.根据检测目标的不同，恶意代码的检测方法可以分为基于主机的检测和基于网络的检测。其中，（）属于基于主机的检测方式。

(A)基于蜜罐检测 (B)基于深度包检测 (C)基于沙箱技术检测 (D)基于区域的检测

答案：C

309.根据检测目标的不同，恶意代码的检测方法可以分为基于主机的检测和基于网络的检测。其中，（）属于基于网络的检测方式。

(A)基于特征码的扫描技术 (B)基于行为的检测 (C)基于沙箱技术的检测 (D)基于蜜罐的检测

答案：D

310. 通过对恶意代码的静态分析方法不能够获得（）信息。

(A)恶意代码的结构　(B)恶意代码各模块关系　(C)函数调用信息　(D)运行状态

答案：D

311.（）不符合一个完善的签名必须的要求

(A)签名是可信和可验证的，任何人都可以验证签名的有效性。(B)签名是不可伪造的，除了合法签名者之外，任何人伪造签名都是困难的。　(C)签名是不可复制的。　(D)签名是不唯一的。

答案：D

312.代码签名技术能够保证软件发布者身份的合法性。一个基本的签名过程不包括（)。

(A)应用发布者向 CA 申请数字证书。(B)发布者开发出代码，先计算代码 Hash 值，然后采用签名工具和自己的私钥对该 Hash 值签名，从而生成一个包含软件代码、发布者证书、代码签名的软件包。　(C)用户通过各种途径获取软件包，并验证证书的有效性。　(D)用户验证结束以后更新数字证书。

答案：D

313.基于结构度量的技术，是指利用源代码中的结构信息计算源代码之间相似度的技术，一般来说分为（）步。

(A)二　(B)三　(C)四　(D)五

答案：A

314.ISO/IEC 21827 将安全工程服务提供者的能力划定为（）个级别

(A)二　(B)三　(C)四　(D)五

答案：D

315.ISO/IEC 21827 针对安全工程实践评估标准的模型不涵盖（）方面的内容?

(A)项目生命周期　(B)整个组织阶段　(C)与网络的规范交互　(D)与其他规范之间的交互作用

答案：C

316.从评估阶段上来看，SSAM(SSE－CMM Apprialsal)不包括?

(A)计划阶段　(B)准备阶段　(C)现场阶段　(D)反馈阶段

答案：D

317.《信息安全等级保护管理办法》将信息系统的安全保护划分为（）个等级。

(A)三　(B)四　(C)五　(D)六

答案：C

318. 网络安全等级保护实施过程中应该遵循的四项基本原则不包含?

(A)自主保护原则 (B)重点保护原则 (C)同步建设原则 (D)整体优化原则

答案：D

319. 业务信息安全被破坏时所侵害的客体的侵害程度为?

(A)轻微损害 (B)一般损害 (C)严重损害 (D)特别严重损害

答案：A

320. 系统服务安全被破坏时所侵害的客体的侵害程度不包含?

(A)轻微损害 (B)一般损害 (C)严重损害 (D)特别严重损害

答案：A

321. 分级保护针对的是涉密信息系统，划分等级不包括?

(A)秘密 (B)机密 (C)绝密 (D)公开

答案：D

322.《涉及国家秘密的信息系统分级保护管理规范》规定了涉密信息系统分级保护管理必须遵循的原则不包括（）

(A)规范定密，准确定级 (B)依据标准，同步建设 (C)突出重点，确保核心 (D)明确责任，定点追责

答案：D

323.《涉及国家秘密的信息系统分级保护管理规范》规定了涉密信息系统分级保护管理必须遵循原则不包括（）

(A)规范定密，准确定级 (B)依据标准，同步建设 (C)突出重点，确保核心 (D)明确责任，定点追责

答案：D

324.《可信计算机系统评估准则》TCSEC 将安全要求由高到低分为（）类

(A)二 (B)三 (C)四 (D)五

答案：C

325.《可信计算机系统评估准则》TCSEC 将安全级别由高到低分为（）个等级

(A)四 (B)五 (C)六 (D)七

答案：D

326. CC 准则评估办法主要针对计算机安全产品和系统，其关键概念不包括?

(A)评估对象 (B)保护轮廓 (C)安全目标 (D)应用功能需求

答案：D

327. CC 准则评估办法主要针对计算机安全产品和系统，其关键概念不包括?

(A)评估对象 (B)保护轮廓 (C)安全目标 (D)访问控制

答案：D

328. CC 标准是信息技术安全评价的通用准则，其核心概念是?

(A)评估对象 (B)保护轮廓 (C)安全目标 (D)安全功能需求

答案：B

329. 在 CC 标准的技术安全措施文档规范中，密码支持类的密码功能不包括?

(A)身份认证 (B)数据机密性 (C)完整性保护 (D)访问控制

答案：D

330. 在 CC 标准的技术安全措施文档规范中，密码支持类的密码功能不包括?

(A)身份认证 (B)访问控制 (C)完整性保护 (D)数字签名

答案：B

331. 信息安全检测认证体系中，密码模块检测认证与信息安全产品检测认证工作的关系是?

(A)结合 (B)替代 (C)补充 (D)没有关系

答案：A

332. 信息安全检测认证体系的基础和开始是（）

(A)信息系统安全检测认证 (B)信息安全产品检测认证 (C)CC 标准 (D)密码检测认证

答案：D

333. 在产品和系统中使用密码模块(包含密码算法)无法提供哪些安全服务

(A)机密性 (B)完整性 (C)鉴别 (D)访问控制

答案：D

334. 在产品和系统中使用（）来提供机密性、完整性、鉴别等安全服务

(A)应用模块 (B)密码模块 (C)网络模块 (D)设备模块

答案：B

335. （）是 CMVP(Cryptographic Module Validation Program)必要的先决条件

(A)通用准则评估和认证计划(CCEVS) (B)密码算法正确性检测(CAVP) (C)FIPS PUB 标准

(D)NVLAP

答案：B

336. （）是 CMVP(Cryptographic Module Validation Program)必要的先决条件

(A)通用准则评估和认证计划(CCEVS) (B)密码算法正确性检测(CAVP) (C)FIPS PUB 标准 (D)NVLAP

答案：B

337. （）在 CMVP(Cryptographic Module Validation Program)评估中发挥核心作用

(A)通用准则评估和认证计划(CCEVS) (B)密码算法正确性检测(CAVP) (C)FIPS PUB 标准 (D)NIST/CSE

答案：D

338. （）在 CMVP(Cryptographic Module Validation Program)评估中发挥核心作用

(A)通用准则评估和认证计划(CCEVS) (B)密码算法正确性检测(CAVP) (C)FIPS PUB 标准 (D)NIST/CSE

答案：D

339. 信息系统管理的目标是为企业、单位和组织提供最终的决策支持，信息系统的管理不包括?

(A)信息系统开发管理 (B)运行管理 (C)维护管理 (D)风险管理

答案：D

340. 信息系统管理的目标是为企业、单位和组织提供最终的决策支持，信息系统的管理不包含?

(A)风险管理 (B)运行管理 (C)维护管理 (D)安全管理

答案：A

341. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估的基本要素不包括?

(A)要保护的信息资产 (B)信息资产的脆弱性 (C)信息资产面临的威胁 (D)运维风险

答案：D

342. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估的基本要素不包括?

(A)要保护的信息资产 (B)信息资产的脆弱性 (C)信息资产面临的威胁 (D)已经度过

的风险

答案：D

343. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中业务战略与资产是什么关系

(A)依赖 (B)暴露 (C)拥有 (D)增加

答案：A

344. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中脆弱性与资产是什么关系

(A)依赖 (B)暴露 (C)拥有 (D)增加

答案：B

345. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中资产价值与资产是什么关系

(A)依赖 (B)暴露 (C)拥有 (D)增加

答案：C

346. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中资产价值与风险是什么关系

(A)依赖 (B)暴露 (C)拥有 (D)增加

答案：D

347. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中安全措施与风险是什么关系

(A)依赖 (B)降低 (C)拥有 (D)增加

答案：B

348. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中安全措施与威胁是什么关系

(A)依赖 (B)降低 (C)拥有 (D)抗击

答案：D

349. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中安全需求与威胁是什么关系

(A)依赖 (B)降低 (C)导出 (D)抗击

答案：C

350. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估中残留风险与安全事件是什么关系？

(A)依赖 (B)降低 (C)导出 (D)可能诱发

答案：D

三、多选题

1. 下面哪些是 OSI 安全框架的内容？
   (A)认证框架 (B)访问控制框架 (C)确认框架 (D)机密性框架 (E)非否认框架
   答案：ABDE
2. OSI 安全框架中的机密性框架描述了下列哪些内容
   (A)保护敏感数据 (B)机密性机制的分类方法 (C)开放系统互连中非否认的相关概念 (D)与其他安全服务机制的关系 (E)开放系统互连中完整性的相关概念
   答案：ABD
3. 网络传输层可以提供哪些安全服务？
   (A)对等实体认证 (B)访问控制 (C)鉴别 (D)数据起源认证 (E)加密
   答案：ABCDE
4. 硬件安全技术，是指用硬件的手段保障计算机系统或网络系统中的信息安全的各种技术，主要包括以下哪几种？
   (A)侧信道技术 (B)硬件固件安全技术 (C)无线传感器网络安全技术 (D)局域网安全技术 (E)链路安全技术
   答案：ABC
5. 网络安全在攻击和防御层面包含哪些技术？
   (A)防火墙技术 (B)网络隔离技术 (C)入侵检测 (D)入侵防御技术 (E)网络漏洞扫描技术
   答案：ABCDE
6. 网络安全技术主要包括哪些技术？
   (A)网络防御技术 (B)访问控制技术 (C)数据安全性技术 (D)认证技术 (E)网络攻击技术
   答案：AE
7. 传统的 PKI 系统包括哪些基本组件（）？
   (A)终端实体 (B)认证机构 (C)注册机构 (D)证书资料库 (E)密钥管理中心
   答案：ABCDE
8. 信息网络中机密性服务有哪几种？
   (A)数据机密性服务 (B)结构机密性服务 (C)业务流机密性服务 (D)链路机密性服务 (E)认证机密性服务
   答案：AC
9. OSI 安全体系结构中提出的安全机制包括？
   (A)加密 (B)数字签名 (C)访问控制 (D)非否认 (E)路由控制
   答案：ABDE
10. 除了 OSI 安全体系结构中提出的安全机制之外，还有哪些普遍采用的安全机制
    (A)访问控制 (B)可信功能模块 (C)安全标记 (D)安全恢复 (E)数据完整性
    答案：BCD

11. 关于安全服务与网络层次之间的对应关系，下面哪些网络层次可以提供数据起源认证？

(A)物理层 (B)网络层 (C)传输层 (D)会话层 (E)应用层

答案：BCE

12. 关于安全服务与网络层次之间的对应关系，下面哪些网络层次可以提供对等实体认证？

(A)链路层 (B)物理层 (C)传输层 (D)网络层 (E)应用层

答案：CDE

13. 关于安全服务与网络层次之间的对应关系，哪些网络层次提供的服务是一样的

(A)物理层 (B)网络层 (C)传输层 (D)表示层 (E)应用层

答案：BC

14. 系统安全技术是信息安全技术体系结构之一，系统安全技术主要包括？

(A)操作系统安全技术 (B)支持设备安全技术 (C)数据库系统安全技术 (D)网络安全技术 (E)访问安全技术

答案：AC

15. 软件安全技术是信息安全技术体系结构之一，现有的软件安全技术包括？

(A)恶意代码分析与检测 (B)访问控制检测 (C)操作系统检测 (D)软件缺陷与漏洞分析 (E)软件代码的安全

答案：ADE

16. 信息安全管理是信息安全技术体系结构之一，现有的信息安全管理包括？

(A)信息系统安全工程 (B)信息安全等级保护 (C)涉密网络分级保护 (D)密码模块测评 (E)信息安全系统管理

答案：ABCDE

17. 下列属于公钥密码体制基本模型的是（）

(A)认证模型 (B)非否认模型 (C)机密性模型 (D)加密模型 (E)公开模型

答案：AD

18. 现有的公钥密码体制中使用的密钥包括

(A)公开密钥 (B)私有密钥 (C)对称密钥 (D)口令 (E)非否

答案：AB

19. 下列属于对称密码机制的是（）

(A)DES 算法 (B)RSA 算法 (C)AES 算法 (D)IDEA 算法 (E)SSL 算法

答案：ABD

20. 实现数据完整性必须满足两个要求,分别是（）

(A)数据完整性应该能被消息的接收者所验证 (B)数据在通信前后必须是安全的 (C)数据完整性应该与消息相关，即消息不同，所产生的附件数据也应该不同。 (D)数据不能丢失 (E)数据排列整齐

答案：AC

21. 可以用来实现数字签名的有（）。

(A)对称密码体制 (B)公钥密码体制 (C)密码安全 (D)密码协议 (E)实体协议

答案：AB

22. 计算机安全的主要目标是（）

(A)防止未经授权的用户获取资源 (B)防止已经授权的用户获取资源 (C)防止合法用户以未授权的方式访问资源 (D)使合法用户经过授权后可以访问资源 (E)尽可能开放

答案：ACD

23. 访问控制的基本要素包括以下（）

(A)客体 (B)主体 (C)控制策略 (D)访问权限 (E)检测

答案：ABD

24. 访问控制策略一般分为以下几类（）

(A)被动访问控制 (B)自主访问控制 (C)强制访问控制 (D)完全访问控制 (E)客体访问控制

答案：BC

25. 在自主访问控制中，每个主体对自己拥有的对客体的访问权限可以使用（）来表示

(A)权限映射 (B)一维矩阵 (C)有向图 (D)权限列表 (E)权限图

答案：BD

26. 关于 TCSEC 说法正确的是（）

(A)类 A 中的级别 A1 是最高安全级别 (B)类 D 中的级别 D1 是最低安全级别 (C)类 D 中的级别 D1 是最高安全级别。(D)类 A 中的级别 A1 是最低安全级别 (E)类 A 中的级别 A1 是系统必须达到的级别

答案：AB

27. 关于 TCSEC 说法不正确的是（）

(A)类 A 中的级别 A1 是最高安全级别 (B)类 D 中的级别 D1 是最低安全级别 (C)类 D 中的级别 D1 是最高安全级别。(D)类 A 中的级别 A1 是最低安全级别 (E)类 A 中的级别 A1 是系统必须达到的级别

答案：CDE

28. 信息网络的物理安全可以分为（）和（）两大类。

(A)环境安全 (B)设备安全 (C)软件安全 (D)线路安全 (E)场地安全

答案：AB

29. 物理安全可以分为环境安全和设备安全两大类。以下属于环境安全考虑事项的是（）。

(A)防雷击 (B)防静电 (C)防火防水 (D)防电磁泄露 (E)防电磁干扰

答案：ABC

30. 物理安全可以分为环境安全和设备安全两大类。以下属于设备安全考虑事项的是（）。

(A)设备防盗 (B)防毁 (C)线路安全 (D)防电磁泄露 (E)介质安全

答案：ABDE

31. 以下符合计算机场地规范要求的是（）。

(A)避开易发生火灾和爆炸的地区，如油库、加油站和其他易燃物附近。(B)避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域，如大型化工厂、加工厂附近。 (C)避免低洼、潮湿及落雷区域。 (D)避开附近有强电场和强磁场的区域。 (E)避免在建筑物的高层以及用水设备的下层或隔壁。

答案：ABCDE

32. 物理安全可以分为环境安全和设备安全两大类。以下属于设备安全考虑事项的是（）。

(A)场地选址 (B)场地防火 (C)场地防水、防潮 (D)场地温度控制 (E)场地电源供应

答案：ABCDE

33. 计算机场地防火主要包括（）。

(A)材料防火 (B)防火隔离 (C)报警系统 (D)灭火系统 (E)粉尘含量

答案：ABCDE

34. 为保计算机场地安全，火灾自动报警、自动灭火系统部署应注意( )。

(A)避开可能招致电磁干扰的区域或设备 (B)具有不间断的专用消防电源 (C)留备用电源 (D)具有自动和手动两种触发装置 (E)不需要备用电源

答案：ABCD

35. 以下关于场地安全的说法正确的是（）

(A)强噪声会对工作人员的生理和心理健康带来危害，计算机场地应避开强震动源和强噪声源区域。 (B)信息网络所使用的电子设备，往往对水、潮气比较敏感，合适状态是将场地湿度控制在 30%—75%。 (C)信息系统场地应该保持比较稳定的适合电子设备运行的温度，温度过高有可能引起局部短路或者燃烧，所以应有相对的温度控制系统。 (D)因为电子设备中有很多金属，容易被腐蚀，所以计算机场地应避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域。 (E)电源是电子设备运行的必要条件，持续稳定的电源供应是环境运行的基本保证。

答案：ACDE

36. 电源是电子设备运行的必要条件，持续稳定的电源供应是环境运行的基本保证。以下说法正确的是（）。

(A)提供紧急情况供电，配置抵抗电压不足的设备，包括基本的 UPS、改进的 UPS、多级 UPS 和应急电源(发电机组)等。 (B)特殊设备独占专有回路。 (C)防止电源线干扰，包括中断供电、异常状态供电(指连续电压过载或低电压)、电压瞬变、噪声(电磁干扰)，以及由于核爆炸或雷击等引起的设备突然失效事件； (D)物理安全电缆布放距离尽量长而整齐，通信电缆与电力电缆应分别在不同路由敷设，由动力机房至主机房的电源线、信号线不得穿越或穿入空调通风管道。 (E)设置电源保护装置，如金属氧化物可变电阻、硅雪崩二极管、气体放电管、滤波器、电压调整变压器、避雷针和浪涌滤波器等。

答案：ABCE

37. 静电的危害有( )。

(A)导致磁盘读写错误，损坏磁头，引起计算机误动作 (B)造成电路击穿 (C)电击，影响工作人员身心健康 (D)吸附灰尘 (E)可能造成电路毁坏

答案：ABDE

38. 为了减小雷电损失，可以采取的措施有( )。

(A)机房内应设等电位连接网络 (B)部署 UPS (C)在做好屏蔽措施的基础上，做好穿越防雷区域界面上不同线路的保护。 (D)保护装置靠近被保护设备，保护元件两端采用双绞线，使得耦合回路的总面积减少，减弱磁场耦合效应。 (E)信号处理电路

答案：ACD

39. 计算机及其外部设备携带的数据信息可以通过（）和（）两种方式泄漏出去。

(A)辐射泄漏 (B)传导泄漏 (C)电信号泄漏 (D)媒介泄漏 (E)光线泄露

答案：AB

40. 会导致电子设备电磁泄漏的有( )。

(A)显示器 (B)开关电路及接地系统 (C)计算机系统的电源线 (D)机房内的电话线 (E)信号处理电路

答案：ABCDE

41. 为了防止一些电子产品产生的电磁干扰影响或破坏其他电子设备的正常工作，一般的干扰抑制方法有（）

(A)加入滤波器　(B)采用带屏蔽层的变压器　(C)采用压敏电阻等吸波器件　(D)加强电路制作工艺　(E)过滤

答案：ABCD

42. 防止设备电磁辐射可以采用的措施有(　)

(A)屏蔽　(B)滤波　(C)尽量采用低辐射材料和设备　(D)内置电磁辐射干扰器　(E)清洗

答案：ABCD

43. 对于存储重要信息的介质废弃后应正确处理，其中磁介质的报废处理应(　)。

(A)直接丢弃　(B)砸碎丢弃　(C)反复多次擦写　(D)专用强磁工具清除　(E)仅删除数据

答案：CD

44. 三分技术，七分管理。只有合适的管理才能实现目标的安全，物理安全的管理应做到(　)。

(A)所有相关人员都必须进行相应的培训，明确个人工作职责　(B)制定严格的值班和考勤制度　(C)在重要场所的进出口安装监视器　(D)安排人员定期检查各种设备的运行情况　(E)在重要场所的进出口对进出情况进行录像

答案：ABCDE

45. 侧信道技术（利用非通信信道物理信息如能量消耗变化、电磁辐射变化进行分析攻击）主要分为以下哪几类攻击技术（）

(A)能量分析　(B)计时分析　(C)错误注入　(D)电磁泄露　(E)干扰技术

答案：ABCD

46. 分析密码模块两处/多处能量消耗的变化，使用统计方法对能量消耗进行分析，从而获取密钥值的能量分析方法是(　)。

(A)简单能量分析　(B)差分能量分析　(C)一阶 DPA　(D)二阶/高阶 DPA (E)三阶 DPA

答案：BD

47. 以下属于无线传感器网络面临的攻击技术的是（）。

(A)路由欺骗攻击　(B)选择性数据转发攻击　(C)槽洞攻击　(D)虫洞攻击　(E)错误注入攻击

答案：ABCD

48. 以下（）为建筑物方面的标准

(A)《通信建筑工程设计规范》　(B)《计算机场地安全要求》　(C)《建筑设计防火规范》　(D)《信息技术设备的安全》　(E)《信息安全管理标准》

答案：ABC

49. 以下（）为针对建筑物方面的标准。

(A)《电子信息系统机房设计规范》　(B)《信息安全管理标准》　(C)《计算机场地通用规范》　(D)《入侵探测器 第 3 部分：室内用微波多普勒探测器》　(E)《计算机场地通用规范》

答案：ACDE

50. 以下（）为针对设备安全方面的标准。

(A)《信息设备电磁泄漏发射限值》　(B)《信息设备电磁泄漏发射测试方法》　(C)《信息安全管理标准》　(D)《入侵探测器 第 3 部分：室内用微波多普勒探测器》　(E)《信息安全技术 信息系统物理安全技术要求》

答案：ABC

51. 网络攻击类型多种多样，且出现频繁、规模较大，攻击者可以采取多种网络攻击方式。

下列属于网络攻击类型的是（）

(A)信息泄漏攻击 (B)完整性破坏攻击 (C)拒绝服务攻击 (D)非法使用攻击 (E)钓鱼网站

答案：ABCD

52. 网络攻击实施过程中涉及的主要元素有（）

(A)攻击者 (B)安全漏洞 (C)攻击访问 (D)攻击工具 (E)攻击效果

答案：ABCDE

53. 下列属于网络防御技术的是（）

(A)防火墙技术 (B)访问控制技术 (C)加密技术 (D)拒绝服务技术 (E)开放端口技术

答案：ABC

54. 防火墙按照概念划分，包括（）

(A)包过滤防火墙 (B)应用代理网关防火墙 (C)状态检测防火墙 (D)硬件防火墙 (E)协议防火墙

答案：ABC

55. 防火墙按照软硬件结构划分,包括（）

(A)协议安全防火墙 (B)软件防火墙 (C)硬件防火墙 (D)芯片级防火墙 (E)规则防火墙

答案：BCD

56. 防火墙的功能包括（）

(A)数据包状态检测过滤 (B)应用代理 (C)网络地址转换 (D)病毒检测 (E)漏洞扫描

答案：ABCD

57. 防火墙应该阻止下列哪种网络数据包（）

(A)来自未授权的源地址且目的地址为防火墙地址的所有入站数据包 (B)源地址是内部网络地址的所有入站数据包 (C)包含 ICMP 请求的所有入站数据包(D)来自授权的源地址 (E)所有 IP 地址

答案：ABC

58. （）是防火墙环境构建准则。

(A)保持简单原则 (B)设备专用原则 (C)深度防御原则 (D)注意内部威胁原则 (E)忽略外部威胁

答案：ABCD

59. 入侵检测技术是用于检测任何损害或企图损害系统的哪些特性的一种网络安全技术（）

(A)机密性 (B)复用性 (C)完整性 (D)可用性 (E)开放性

答案：ACD

60. 下列属于入侵检测系统的模型的是

(A)Denning 模型 (B)LT 模型 (C)CIDF 模型 (D)IC 模型 (E)OSI 模型

答案：AC

61. 下列属于入侵防御系统种类的是（）

(A)基于主机的入侵防御系统 (B)基于应用的入侵防御系统 (C)基于网络的入侵防御系统 (D)基于协议的入侵防御系统 (E)基于用户的入侵防御系统

答案：ABC

62. 以下关于漏洞的说法正确的是（）

(A)漏洞的分类方法很多　(B)漏洞具有时间与空间特性　(C)系统的环境变量发生变化时产生的漏洞为开放式协议漏洞　(D)程序在实现逻辑中没有考虑一些意外情况为异常处理疏漏　(E)漏洞目前没有统一的分类标准。

答案：ABDE

63. 基于网络的漏洞扫描器的组成部分包括（）

(A)漏洞数据库模块　(B)用户配置控制台模块　(C)发现漏洞模块　(D)当前活动扫描知识库模块　(E)网闸模块

答案：ABD

64. 基于主机的漏洞扫描器一般具有如下哪些功能（）

(A)重要资料锁定　(B)弱口令检查　(C)系统日志和文本文件分析　(D)扫描引擎模块　(E)防火墙模块

答案：ABC

65. 基于网络的漏洞扫描器具有如下哪些优点（）

(A)价格便宜　(B)维护简便　(C)不需要实时监督　(D)能直接访问目标设备的文件系统　(E)容易穿过防火墙

答案：ABC

66. 网络隔离可以采用（）方式

(A)逻辑隔离　(B)分层隔离　(C)物理隔离　(D)区块隔离　(E)入侵检测

答案：AC

67. （）不是实现网络隔离技术的设备。

(A)防火墙　(B)隔离网闸　(C)路由器　(D)网关　(E)入侵检测

答案：ACDE

68. 下列关于拒绝服务攻击说法正确的是（）

(A)来自网络的拒绝服务攻击可以分为停止服务和消耗资源两类　(B)拒绝服务攻击的目的是利用各种攻击技术使服务器或者主机等拒绝为合法用户提供服务　(C)停止服务意味着毁坏或者关闭用户想访问的特定的服务　(D)停止服务是目前最流行的拒绝服务攻击方式　(E)开放服务是目前最流行的拒绝服务攻击方式

答案：ABC

69. 下列关于 Botnet 说法正确的是（）

(A)用 Botnet 发动 DDoS 攻击　(B)Botnet 的显著特征是大量主机在用户不知情的情况下，被植入了控制程序　(C)拒绝服务攻击与 Botnet 网络结合后攻击能力大大削弱　(D)Botnet 可以被用来传播垃圾邮件、窃取用户数据等　(E)Botnet 可以被用来监听网络和扩散恶意病毒等

答案：ABD

70. 下列能做到检测和抵御拒绝服务攻击的是（）

(A)强口令检查　(B)TCP SYN Cookie　(C)TCP 状态检测　(D)HTTP 重定向　(E)root 检查

答案：BCD

71. 针对口令的攻击方法可分为?

(A)暴力破解　(B)字典攻击　(C)软件攻击　(D)肩窥攻击　(E)钓鱼攻击

答案：ABDE

72. 应对字典攻击应该怎么办?

(A)定期更换口令　(B)设置复杂密码　(C)预设口令　(D)使用方便记忆的密码　(E)在多个系统中使用相同的口令

答案：AB

73. 基于动态口令的认证技术的优点是什么？
(A)不确定性 (B)动态性 (C)一次性 (D)可重复性 (E)抗窃听性
答案：ABCE

74. 基于生物特征的认证技术的缺陷是什么？
(A)难以提取 (B)依赖于特殊的硬件设备 (C)生物特征很多 (D)生物特征可能会发生变化 (E)生物特征很复杂
答案：BD

75. 主流身份鉴别协议有哪些？
(A)Kerberos (B)OpenID (C)RADIUS (D)SAML (E)FIDO
答案：ABCDE

76. 与 OpenID 身份鉴别协议无关的是（）？
(A)提供授权请求 (B)执行身份鉴别 (C)响应用户信息 (D)授权 (E)请求用户信息
答案：BD

77. 安全性断言标记语言(Security Assertion Markup Language，简称 SAML)应用的实现由（）组成
(A)主体 (B)服务提供者 (C)审查者 (D)记录者 (E)身份提供者
答案：ABE

78. 安全性断言标记语言(Security Assertion Markup Language，简称 SAML)的基本部分包括（）？
(A)绑定 (B)配置 (C)元数据 (D)认证上下文 (E)协议
答案：ABCDE

79. 安全性断言标记语言(Security Assertion Markup Language，简称 SAML)包括哪些声明
(A)属性声明 (B)访问申明 (C)认证声明 (D)授权声明 (E)控制申明
答案：ACD

80. 安全性断言标记语言(Security Assertion Markup Language，简称 SAML)不包括哪些声明
(A)身份声明 (B)访问申明 (C)假装声明 (D)授权声明 (E)属性声明
答案：ABC

81. FIDO 协议提供了（）认证方式？
(A)通用授权框架 (B)访问控制 (C)通用第二因素认证 (D)数据完整性框架 (E) 加 密
答案：AC

82. 身份鉴别系统解决方案有哪些？
(A)单点登录 (B)多因素认证 (C)联合身份 (D)单因素认证 (E)加密
答案：ABC

83. 单点登录系统主要有？
(A)基于服务端凭据缓存的单点登录系统 (B)基于令牌的单点登录系统 (C)基于加密的单点登录系统 (D)基于 PKI 的单点登录系统 (E)基于客户端凭据缓存的单点登录系统
答案：BDE

84. 单点登录系统不包括？
(A)基于服务端凭据缓存的单点登录系统 (B)基于指令的单点登录系统 (C)基于客户

端凭据缓存的单点登录系统　(D)基于 PKI 的单点登录系统　(E)基于令牌的单点登录系统

答案：AB

85. 单点登录系统不包括?

(A)基于服务端凭据缓存的单点登录系统 (B)基于令牌的单点登录系统　(C)基于电脑端凭据缓存的单点登录系统　(D)基于 PKI 的单点登录系统　(E)基于令牌的单点登录系统

答案：AC

86. 主要的单点登录协议有（）?

(A)基于 Kerberos 的单点登录协议　(B)基于 FIDO 的单点登录协议　(C)基于 SAML 的单点登录协议　(D)基于 OpenID 的单点登录协议　(E)基于 RADIUS 的单点协议

答案：ACD

87. 主要的单点登录协议不包含?

(A)基于 TCP 的单点登录协议　(B)基于 FIDO 的单点登录协议　(C)基于 SAML 的单点登录协议　(D)基于 OpenID 的单点登录协议　(E)基于 Kerberos 的单点登录协议

答案：AB

88. 网上支付的多因素身份鉴别技术主要有?

(A)静态口令 + 动态口令认证　(B)静态口令 + 数字证书认证　(C)静态口令 + 手机验证码认证　(D)静态口令 + 生物特征认证　(E)静态口令 + 联合认证

答案：ABC

89. PKI 系统组成有哪些?

(A)终端实体 (B)认证机构 (C)注册机构 (D)证书撤销列表发布者　(E)数字证书与密钥对

答案：ABCDE

90. 终端实体可以分为哪些?

(A)PKI 证书的主体(B)终端用户或者系统 (C)PKI 证书的使用者 (D)证书撤销列表发布者 (E)数字证书与密钥对

答案：ABC

91. 数字证书根据其用途可以分为?

(A)传播证书 (B)解密证书 (C)加密证书 (D)签名证书 (E)管理证书

答案：BC

92. PKI 提供的核心服务包括?

(A)认证 (B)完整性　(C)密钥管理 (D)简单机密性　(E)非否认

答案：ABCDE

93. PKI 提供的核心服务包括了哪些信息安全的要求。

(A)访问安全性　(B)真实性　(C)完整性　(D)保密性　(E)不可否认性

答案：BCDE

94. PKI 技术的典型应用有?

(A)安全电子邮件 (B)匿名登陆 (C)安全 Web 服务 (D)VPN 应用 (E)网上商业或政务行为

答案：ACDE

95. PKI 部署是一个复杂的问题，PKI 技术的部署需要考虑?

(A)组织信任体系的目标　(B)资源引进和资源外包　(C)安全应用 (D)资金和技术投入 (E)个人意愿

答案：ABCD

96. 数字版权保护(Digital Rights Management,DRM)的基本要求包括?

(A)防止未经授权的侦听 (B)防止未经授权的修改 (C)识别不同的获得数字内容授权的用户 (D)采用有效的防篡改机制来保护数据 (E)保护内容的使用权

答案：ABCDE

97. 数字版权保护系统的基本要求包括?

(A)防止未经授权的侦听 (B)防止未经授权的修改 (C)识别不同的获得数字内容授权的用户 (D)采用有效的防篡改机制来保护数据和内容的使用权 (E)

答案：ABCD

98. 数字版权保护系统中的密码技术有?

(A)对称与非对称加密 (B)数字签名和单向散列函数 (C)数字证书 (D)访问控制 (E)鉴别

答案：ABC

99. 数字水印的特征有?

(A)不需要带外传输 (B)透明性 (C)鲁棒性 (D)安全性 (E)稳定性

答案：ABCD

100. 数字水印的分类有?

(A)鲁棒水印和脆弱水印 (B)公有水印和私有水印 (C)对称水印和非对称水印 (D)隐藏水印和非隐藏水印 (E)安全水印和不安全水印

答案：ABCD

101. 数字水印的应用有?

(A)完整性保护 (B)版权保护 (C)拷贝保护 (D)拷贝追踪 (E)安全性追踪

答案：BCD

102. 无论是社交网络还是云计算，如果隐私策略设置不当，将会造成隐私信息泄漏。隐私信息泄漏有几种类型?

(A)身份泄漏 (B)连接泄漏 (C)内容泄漏 (D)内存泄漏 (E)虚拟泄漏

答案：ABC

103. 社交网络的数据分层有几种?

(A)appliction－layer (B)activity－layer (C)registration－layer (D)networking － layer (E)content－laye

答案：BCDE

104. 衡量容灾系统的主要目标包括?

(A)恢复点目标 (B)恢复时间目标 (C)网络恢复目标 (D)服务降级目标 (E)本地恢复目标

答案：ABCD

105. 容灾技术有哪些类型?

(A)数据备份 (B)应用恢复技术 (C)网络恢复技术 (D)数据恢复技术 (E)访问控制

答案：BCD

106. 容灾技术的类型不包括?

(A)数据备份 (B)应用恢复技术 (C)网络恢复技术 (D)数据恢复技术 (E)访问控制

答案：AE

107. 备份系统的选择的原则是以很低的（）和很少的（）来进行自动而高速的数据备份。

(A)服务器数量 (B)系统资源占用率 (C)任务数量 (D)网络带宽 (E)使用频率

答案：BD

108. 数据备份主要分成以下几种类型?

(A)基于主机备份 (B)基于局域网备份 (C)无服务器备份 (D)基于存储局域网备份 (E)零影响备份

答案：ABCDE

109. 数据备份策略主要分成以下几种形式?

(A)完全备份 (B)增量备份 (C)累计备份 (D)混合应用 (E)部分备份

答案：ABCD

110. 跨站请求伪造攻击防御主要有（）。

(A)验证码 (B)请求检查 (C)反 CSRF 令牌 (D)输出检查 (E)端口开放

答案：ABC

111. 下列属于防御 SQL 注入的基本方式的有（）。

(A)使用预编译语句 (B)使用存储过程 (C)检查数据类型 (D)使用安全编码函数 (E)端口开放

答案：ABCD

112. 下列属于常见的网页篡改技术的是（）。

(A)木马植入 (B)病毒攻击 (C)窃听管理员的用户名和口令 (D)阻止黑客反侵入 (E)阻止黑客入侵

答案：ABC

113. 篡改技术可以利用各种漏洞进行木马植入，然后利用木马程序进行文件篡改。通常可供利用的漏洞包括（）。

(A)操作系统漏洞 (B)数据库漏洞 (C)Web 服务器漏洞 (D)Web 应用程序漏洞 (E)安全设置

答案：ABCD

114. 网页防篡改技术主要分为两类，阻止黑客入侵和阻止黑客反入侵。以下属于阻止黑客入侵行为的是（）。

(A)对管理员的权限进行限制 (B)对网页请求参数进行验证 (C)轮询检测 (D)事件触发技术 (E)核心内嵌技术

答案：AB

115. 网页防篡改技术主要分为两类，阻止黑客入侵和阻止黑客反入侵。以下属于阻止黑客反入侵行为的是（）。

(A)对管理员的权限进行限制 (B)对网页请求参数进行验证 (C)轮询检测 (D)事件触发技术 (E)核心内嵌技术

答案：CDE

116. 网页防篡改技术主要分为（）。

(A)阻止黑客侵入 (B)阻止黑客反侵入 (C)SQL 注入 (D)木马植入 (E)窃听

答案：AB

117. 以下属于进行内容过滤目的的是（）。

(A)阻止不良信息对人们的侵害 (B)规范用户的上网行为，提高工作效率 (C)防止敏感数据的泄漏 (D)遏制垃圾邮件的蔓延 (E)减少病毒对网络的侵害

答案：ABCDE

118. 以下属于安全电子交易(Secure Electronic Transaction，简称 SET)协议包含的实体的是（）。

(A)持卡人 (B)发卡机构 (C)商户 (D)银行 (E)支付网关

答案：ABCDE

119. 安全电子交易(Secure Electronic Transaction，简称 SET)协议较好地解决了电子交易信息的（）。

(A)机密性　(B)完整性　(C)身份认证　(D)非否认性　(E)开放性

答案：ABCD

120. 常见的操作系统有

(A)Windows　(B)UNIX/Linux(C)Android　(D)OSI　(E)IIS

答案：ABC

121. 操作系统在概念上一般包含（）

(A)内核　(B)壳(shell)　(C)外核　(D)中核　(E)中间层

答案：AB

122. 下列属于操作系统安全要素的是（）

(A)用户认证　(B)内部进程间通信的同步　(C)共享的实现　(D)模式识别　(E)应用程序

答案：ABC

123. 设计安全操作系统应该遵循以下一些原则（）

(A)最小特权　(B)基于许可的模式　(C)保护机制的经济性　(D)最大特权　(E)全局开放

答案：ABC

124. 用户组(包括本地用户组和域用户组)的使用策略包括（）

(A)在域控制器上创建全局组　(B)给本地组授予相应的用户权限和资源许可　(C)将本地组放到全局组中　(D)在域中创建用户，并将其放到相应的全局组中　(E)在域控制器上创建本地组

答案：ABD

125. windows 屏蔽网络设置的方法包括以下哪种（）

(A)禁用网上邻居属性　(B)取消网络访问权限　(C)隐藏网上邻居　(D)禁止开机启动　(E)禁止网络连接

答案：ABC

126. 属于 UNIX 系统具有两个执行态的是（）

(A)来宾态　(B)核心态　(C)访问态　(D)用户态　(E)网络态

答案：BD

127. UNIX 以树型结构组织文件系统，这个系统包括文件和目录。rw－r－－r－－表示（）

(A)属主有读、写权　(B)属组和其他人有读权　(C)属主有读、写、执行权　(D)属组和其他人有读、写权　(E)属主和其他人有读、写、执行权

答案：AB

128. 关于 rw－r－－r－－说法错误的是（）

(A)属主有读、写权　(B)属组和其他人有读权　(C)属主有读、写、执行权　(D)属组和其他人有读、写权　(E)属主有读、写、执行权

答案：CDE

129. UNIX 中有两种 NFS 服务器，分别是（）

(A)基于内核的 NFS Daemon　(B)基于壳(shell)的 NFS Daemon (C)旧的用户空间 Daemon (D)壳的空间 Daemon　(E)访问控制列表(Access Control Lists)

答案：AC

130. UNIX 系统提供了几条功能强大的命令，用于文件系统的备份和恢复，下面具有这些功能的命令是（）

(A)backup (B)cpio (C)tar (D)chmod (E)root

答案：ABC

131. Linux 系统提供了一些查看进程信息的系统调用，下面具有上述功能的命令是（）

(A)who (B)ps (C)top (D)cd (E)root

答案：ABC

132. 属于 Apache 服务器的安全缺陷的是（）

(A)可以利用 HTTP 对其进行 DoS 攻击 (B)导致缓冲区溢出攻击 (C)让攻击者获得 Root 权限 (D)攻击者植入木马病毒 (E)Apache 洪泛

答案：ABC

133. Android 权限对于用户手机安全至关重要，Android Permission 主要分为（）两类

(A) built－in Permission (B)behind-in Permission (C)用户自定义 Permission (D)全局 Permission (E)应用 Permission

答案：AC

134. 近年来诸如 12306、Bilibili 视频网站等大型公司均爆出数据库泄露事件，公民隐私受到了严峻的挑战。保证数据库的安全涉及以下几个任务（）

(A)防止对数据未经授权的存取 (B)防止事务回退 (C)防止未经授权的人员删除和修改数据 (D)监视对数据的访问和更改等使用情况 (E)扩大用户权限

答案：ACD

135. 数据库管理系统 DBMS 对于用户的访问存取控制有以下两个基本原则（）

(A)隔离原则 (B)反转原则 (C)合并原则 (D)控制原则 (E)排斥原则

答案：AD

136. 下面属于数据库视图可以实现的功能是（）

(A)将用户限定在表中的特定行上 (B)将用户限定在特定列上 (C)将多个表中的列连接起来 (D)聚合信息而非提供详细信息 (E)创建分区

答案：ABCD

137. 下列关于数据库加密的范围描述正确的是（）

(A)数据库文件索引字段不能加密 (B)数据库关系运算的比较字段不能加密 (C)数据库表间的连接码字段可以加密 (D)只能对数据库中的数据进行部分加密 (E)数据库密码系统应采用不对称密钥

答案：ABD

138. 数据库管理系统保护轮廓（DBMS.PP）明确了三种数据库资产，分别是（）

(A)安全数据 (B)数据库客体 (C)控制数据 (D)审计数据 (E)用户数据

答案：BCD

139. 对于 SQL 注入攻击，可以采取以下哪些防范措施（）

(A)配置 IIS (B)在 Web 应用程序中，不要以管理员账号连接数据库 (C)去掉数据库不需要的函数、存储过程 (D)检查输入参数 (E)在 Web 应用程序中，将管理员账号连接数据库

答案：ABCD

140. 恶意代码的泛滥给用户的信息和财产安全造成了巨大危害，恶意代码主要分类包含（）等。

(A)计算机病毒 (B)木马 (C)蠕虫 (D)僵尸程序 (E)内核套件

答案：ABCDE

141. 一个典型的计算机病毒的生命周期包括以下（）阶段。

(A)休眠阶段 (B)传播阶段 (C)触发阶段 (D)执行阶段 (E)预备阶段

答案：ABCD

142. 蠕虫病毒通常通过各种方式将自身的拷贝或者自身的部分功能模块传播到其他计算机系统中。以下为蠕虫病毒传播方式的是（）。

(A)网络连接 (B)USB、CD、DVD 等共享媒体 (C)邮件 (D)Web 服务器 (E)共享文件

答案：ABCDE

143. 僵尸程序可以破坏系统的（）和（）。

(A)完整性 (B)可用性 (C)独立性 (D)可靠性 (E)有效性

答案：AB

144. 僵尸程序的典型应用包括（）

(A)分布式拒绝服务供给 (B)发送垃圾邮件 (C)键盘记录 (D)破坏电脑文件 (E)网络嗅探

答案：ABCE

145. RootKit 根据其特点分类包括（）。

(A)持久性存储 (B)基于内存 (C)用户态 (D)内部模式 (E)内核态

答案：ABCE

146. 计算机病毒，是指通过修改其他程序进行感染，并对系统造成破坏的一段代码，计算机病毒的特性包括（）。

(A)传染性 (B)破坏性 (C)隐蔽性 (D)针对性 (E)寄生性

答案：ABCDE

147. 计算机病毒，是指通过修改其他程序进行感染，并对系统造成破坏的一段代码，（）属于计算机病毒的组成部分。

(A)引导部分 (B)传染部分 (C)休眠部分 (D)干扰或破坏部分 (E)触发部分

答案：ABD

148. Android 恶意代码给用户的隐私信息安全、财产安全和设备安全造成了极大的威胁，以下属于 Android 恶意代码类别的是（）。

(A)恶意扣费类 (B)远程控制类 (C)隐私窃取类 (D)系统破坏类 (E)流氓软件类

答案：ABCDE

149. 被恶意扣费类软件感染之后，它会在后台执行各种扣费操作，消耗用户的资费，给用户造成巨大的经济损失。以下为常见的扣费操作的是（）。

(A)定制 SP 服务短信 (B)后台自动拨打电话 (C)后台频繁联网消耗流量 (D)后台自动发送短信 (E)窃取用户通信和短信

答案：ABCD

150. 以下属于 Android 平台的恶意代码入侵形式的是（）。

(A)重打包 (B)更新攻击 (C)下载攻击 (D)病毒攻击 (E)注入攻击

答案：ABC

151. 以下为 Android 恶意代码触发条件的是（）。

(A)利用系统事件触发 (B)利用短信触发 (C)利用系统时钟触发 (D)利用通话触发 (E)利用网络触发

答案：AB

152. 下列属于 Android 恶意软件的攻击目的的是（）。

(A)提升权限 (B)远程控制 (C)恶意吸费 (D)逃避检测 (E)收集用户隐私信息

答案：ABCE

153. 通过加壳可以实现下列目的（）。

(A)版权保护 (B)逃避检测 (C)压缩 (D)远程控制 (E)提升权限

答案：ABC

154. 加壳后的程序加载到内存执行的步骤包括（）。

(A)获得壳自身需要的 API (B)解密或者解压原程序 (C)重定位 (D)HOOK API (E)跳转到原程序入口

答案：ABCDE

155. 按照壳的目的和作用，加壳工具可以分为（）。

(A)压缩壳 (B)保护壳 (C)扩展壳 (D)控制壳 (E)扩充壳

答案：AB

156. 根据检测目标的不同，恶意代码的检测方法可以分为（）。

(A)基于主机的检测 (B)基于网络的检测 (C)基于宿主的检测 (D)基于区域的检测 (E)基于应用的检测

答案：AB

157.根据检测目标的不同，恶意代码的检测方法可以分为基于主机的检测和基于网络的检测。其中，（）属于基于主机的检测方式。

(A)基于特征码的扫描技术 (B)基于行为的检测 (C)基于沙箱技术的检测 (D)基于启发式检测 (E)基于深度包检测

答案：ABCD

158. SSAM(SSE－CMM Apprialsal)是专门基于 SSE－CMM 的评估方法，用于评估一个信息安全工程组织的工程过程能力和成熟度所需的相关信息和指南。SSAM 评估主要由哪些构成?

(A)发起组织 (B)评估组织 (C)被评估组织 (D)监管组织 (E)投资组织

答案：ABC

159. 从评估阶段上来看，SSAM(SSE－CMM Apprialsal)主要分为?

(A)计划阶段 (B)准备阶段 (C)现场阶段 (D)报告阶段 (E)反馈阶段

答案：ABCD

160. 信息系统安全等级保护实施过程中应该遵循的四项基本原则是?

(A)自主保护原则 (B)重点保护原则 (C)同步建设原则 (D)动态调整原则 (E)整体优化原则

答案：ABCD

161. 信息系统定级由哪些方面决定?

(A)网络 (B)业务信息安全 (C)系统服务安全 (D)访问安全 (E)数据安全

答案：BC

162. 信息系统定级能够有效地衡量受侵害客体的类型与对客体的侵害程度。信息系统定级不涉及?

(A)网络 (B)业务信息安全 (C)系统服务安全 (D)访问安全 (E)数据安全

答案：ADE

163. 业务信息安全被破坏时所侵害的客体的侵害程度分为?

(A)轻微损害 (B)一般损害 (C)严重损害 (D)特别严重损害 (E)完全损害

答案：BCD

164. 业务信息安全被破坏时所侵害的客体的侵害程度不包含?

(A)轻微损害 (B)一般损害 (C)严重损害 (D)特别严重损害 (E)完全损害

答案：AC

165. 系统服务安全被破坏时所侵害的客体的侵害程度分为？

(A)轻微损害 (B)一般损害 (C)严重损害 (D)特别严重损害 (E)完全损害

答案：BCD

166. 系统服务安全被破坏时所侵害的客体的侵害程度不包含？

(A)轻微损害 (B)一般损害 (C)严重损害 (D)特别严重损害 (E)完全损害

答案：AE

167. 分级保护针对的是涉密信息系统，主要划分为（）这几种等级。

(A)秘密 (B)机密 (C)绝密 (D)公开 (E)局部涉密

答案：ABC

168. 分级保护针对的是涉密信息系统，不包括（）等级？

(A)秘密 (B)机密 (C)绝密 (D)公开 (E)局部涉密

答案：DE

169.《涉及国家秘密的信息系统分级保护管理规范》规定了涉密信息系统分级保护管理必须遵循以下原则——()。

(A)规范定密，准确定级 (B)依据标准，同步建设 (C)突出重点，确保核心 (D)明确责任，加强监督 (E)明确责任，定点追责

答案：ABCD

170. 在 CC 标准的技术安全措施文档规范中，密码支持类的密码功能主要包括？

(A)身份认证 (B)数据机密性 (C)完整性保护 (D)数字签名 (E)访问控制

答案：ABCD

171. 在产品和系统中使用密码模块(包含密码算法)来提供哪些安全服务

(A)机密性 (B)完整性 (C)鉴别 (D)访问控制 (E)不可否认性

答案：ABC

172. 在产品和系统中使用密码模块(包含密码算法)不能提供哪些安全服务

(A)机密性 (B)完整性 (C)鉴别 (D)访问控制 (E)不可否认性

答案：DE

173. 安全产品和信息安全系统测评的基础是（）

(A)密码算法正确性检测 (B)密码模块检测认证 (C)网络模块安全性检测 (D)设备模块安全性检测 (E)网络模块安全性认证

答案：AB

174. 下列选项中哪些不是安全产品和信息安全系统测评的基础？

(A)密码算法正确性检测 (B)密码模块检测认证 (C)网络模块安全性检测 (D)设备模块安全性检测 (E)网络模块安全性认证

答案：CDE

175. （）不是 CMVP(Cryptographic Module Validation Program)必要的先决条件

(A)通用准则评估和认证计划(CCEVS) (B)密码算法正确性检测(CAVP) (C)FIPS PUB 标准 (D)NVLAP (E)NIST/CSE

答案：ACDE

176. （）没有在 CMVP(Cryptographic Module Validation Program)评估中发挥核心作用

(A)通用准则评估和认证计划(CCEVS) (B)密码算法正确性检测(CAVP) (C)FIPS PUB 标准 (D)NVLAP (E)NIST/CSE

答案：ABCD

177. 信息系统管理的目标是为企业、单位和组织提供最终的决策支持，信息系统的管理可分为?

(A)信息系统开发管理 (B)运行管理 (C)维护管理 (D)安全管理 (E)风险管理

答案：ABCD

178. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估的基本要素主要包括?

(A)要保护的信息资产 (B)信息资产的脆弱性 (C)信息资产面临的威胁 (D)存在的可能风险 (E)安全防护措施

答案：ABCDE

179. 风险评估能够对信息安全事故防患于未然，为信息系统的安全保障提供最可靠的科学依据。风险评估的流程有？

(A)评估准备阶段 (B)要素识别阶段 (C)风险分析阶段 (D)分析报告提交阶段 (E) 风险控制建议提交阶段

答案：ABCDE