1. **密码学是一门古老又现代的学科。几千年前，它作为神秘性和艺术性的字谜呈现，而现代密码学，作为数学、计算机、电子、通信、网络等领域的一门交叉学科，广泛应用于军事、商业和现代社会人们生产、生活的方方面面。古代密码学的形成于发展在（）。**

A. 1949~1975

B. 1940 年以前

C. 1949 年以前

D. 1946 年以前

参考答案：C

难易程度：一级

解析：密码学的发展历史，古典密码学（1949 年之前）、近代密码学（1949~1975）、现代密码学（1976 年以后）。

知识子域：密码学基础

2. **随着密码学的不断发展，密码学逐步从艺术走向科学。以下那个不属于密码学的发展阶段（）。**

A. 古典密码阶段

B. 近代密码阶段

C. 现代密码阶段

D. 当代密码阶段

参考答案：D

难易程度：一级

解析：密码学的发展历史，古典密码学（1949 年之前）、近代密码学（1949~1975）、现代密码学（1976 年以后）。

知识子域：密码学基础

3. **古典密码阶段从古代到 19 世纪末，在这个阶段中，人类有众多的密码实践，典型的范例是著名的凯撒密码。已知凯撒密码的偏移量 k=3，若密文为 DWWDFN QRZ，则明文是（）。**

A. ATTACK NOW

B. BUUBDL OPX

C. AYYADL NOW

D. ZSSZBJ MNV

参考答案：A

难易程度：一级

解析：凯撒密码偏移量为 k=3，密文 DWWDFN QRZ 往前移动三位得到明文 ATTACK NOW。

知识子域：密码学基础

4. **随着计算机和通信系统的普及，带动了对数字信息的保护需求。密码学进入近代密码阶段，其标志是（）。**

A. 香农(Shannon)发表了划时代论文“保密系统的通信理论”

B. W.Diffie 和 M.E.Hellman 公布了一种密钥一致性算法

C. 转轮机的出现

D. 一些学者提出了公开密钥体制

参考答案：A

难易程度：一级

解析：1949 年香农(Shannon)发表了划时代论文“保密系统的通信理论”，奠定了密码学的理论基础。密码学由此进入了近代密码阶段，开始成为一门科学。

知识子域：密码学基础

5. 以下属于古典密码的局限性（）

A. 不适合大规模生产

B. 不适合较大的或者人员变动较大的组织

C. 用户无法了解算法的安全性

D. 以上都是

参考答案：D

难易程度：一级

解析：古典密码的安全性在于保持算法本身的保密性，因此不适合大规模生产、不适合较大的或者人员变动较大的组织、用户无法了解算法的安全性。

知识子域：密码学基础

6. 以下那个不是古典密码的主要分类（）

A. 代替密码

B. 置换密码

C. 代替密码和置换密码的组合

D. 分组密码

参考答案：D

难易程度：一级

解析：古典密码的主要分类：代替密码、置换密码、代替密码和置换密码的组合

知识子域：密码学基础

7. 密码学包括密码编码学和密码分析学两部分。以下不是密码编码学研究的是（）

A. 信息的编码

B. 构建各种安全有效的密码算法和协议

C. 研究破译密码获得消息

D. 用于消息的加密、认证等方面

参考答案：C

难易程度：一级

解析：密码编码学主要研究信息的编码，构建各种安全有效的密码算法和协议，用于消息的加密、认证等方面。密码分析学是研究破译密码获得消息，或对消息进行伪造。

知识子域：密码学基础

8. 影响密码系统安全性的基本因素不包括（）

A. 密码算法复杂度

B. 密钥随机性

C. 密码复杂度

D. 密钥长度

参考答案：C

难易程度：一级

解析：影响密码系统安全性的基本因素包括：密码算法复杂度、密钥机密性和密钥长度等。

知识子域：密码学基础

9. 对于实际使用的密码系统而言，由于至少存在一种破译方法，即暴力攻击法，因此都不能满足无条件安全性，只能达到计算安全性。下面那个密码系统没有达到实际安全（）

A. 破译该密码系统的实际计算量(包括计算时间或费用)巨大。

B. 破译该密码系统所需要的计算时间超过被加密信息的生命周期。

C. 破译该密码系统的费用超过被加密信息本身的价值。

D. 破译该密码系统实际计算量和开销不大。

参考答案：D

难易程度：一级

解析：密码系统要达到实际安全，就要满足以下准则：（1）破译该密码系统的实际计算量(包括计算时间或费用)巨大，以至于在实际中是无法实现的。（2）破译该密码系统所需要的计算时间超过被加密信息的生命周期。例如，战争中发起战斗攻击的作战命令只需要在战斗打响前保密。（3）破译该密码系统的费用超过被加密信息本身的价值。如果一个密码系统能够满足以上准则之一，就可以认为是实际安全的。

知识子域：密码学基础

10. 对称密码算法也称为传统密码算法、秘密密钥算法或单密钥算法，其加密密钥和解密密钥相同。以下不属于对称密码算法的是（）

A. DES

B. AES

C. RSA

D. RC5

参考答案：C

难易程度：一级

解析：RSA 属于非对称加密算法。

知识子域：密码学基础

11. 以下不属于对称加密的优点的是（）

A. 算法简单、计算量小

B. 加密速度快、加密效率高

C. 适合加密大量数据、明文长度与密文长度相等

D. 算法强度复杂、加密强度高

参考答案：D

难易程度：一级

解析：对称加密算法的优点是算法简单、计算量小、加密速度快、加密效率高，适合加密大量数据，明文长度与密文长度相等。

知识子域：密码学基础

12. 密码学技术在信息安全中应用很广，以下属于信息安全要素的是（）

（1）机密性 （2）完整性 （3）可鉴别性 （4）不可否认性 （5）授权与访问控制

A.（1）（2）（3）（4）

B.（1）（2）（3）（5）

C.（1）（3）（4）（5）

D.（1）（2）（3）（4）（5）

参考答案：D

难易程度：一级

解析：信息安全要素包括：机密性、完整性、可鉴别性、不可否认性、授权与控制访问。

知识子域：密码学基础

13. 柯克霍夫（kerckhoff）原则指出密码体制可以对外公开，对密钥必须保密。密码系统的安全性取决于（）

A. 密码复杂度

B. 密钥

C. 加密算法

D. 密文长度

参考答案：B

难易程度：一级

解析：密码系统的安全性取决于密钥，

知识子域：密码学基础

14. 密码学中运用（）算法，加密和解密使用不同秘钥。

A. 对称加密

B. 哈希

C. 公钥加密

D. 随机加密

参考答案：C

难易程度：一级

解析：公钥加密算法加密解密使用不同的密钥。

知识子域：密码学基础

15. 哈希函数可以将任意有限长度信息映射为固定长度的值。以下哪个不是安全的哈希函数所满足的性质（）

A. 单向性

B. 双向性

C. 弱抗碰撞性

D. 强抗碰撞性

参考答案：B

难易程度：一级

解析：哈希函数具有单向性，消息通过哈希函数计算出哈希值，但是不能由哈希值反向计算出消息的原始内容。

知识子域：密码学基础

16. 下列哪个算法不属于哈希算法（）

A. RC5

B. MD5

C. SHA-1

D. SHA-256

参考答案：A

难易程度：一级

解析：RC5 是对称加密算法。

知识子域：密码学基础

17. 数据加密是保障数据安全的重要手段，以下不属于密码体制的是（）

A. 明文空间

B. 密文空间

C. 通信协议

D. 密钥空间

参考答案：C

难易程度：一级

解析：密码体制不包括通信协议。

知识子域：密码学基础

18. 以下属于数字签名的基本特性的是（）

A. 不可伪造性

B. 不可否认性

C. 消息完整性

D. 以上都是

参考答案：D

难易程度：一级

解析：数字签名的基本特性：不可伪造性、不可否认性、消息完整性。

知识子域：密码学基础

19. 公钥基础设施(PKI)也称公开密钥基础设施。以下不属于 PKI 的组成的是（）

A. 证书使用者

B. 证书权威机构(CA)

C. 证书注册机构(RA)

D. 证书库和终端实体

参考答案：A

难易程度：一级

解析：PKI 的组成一般包括证书权威机构(CA)、证书注册机构(RA)、证书库和终端实体等部分

知识子域：密码学基础

20. （ ）用于确保数据的保密性，阻止对手的被动攻击，如截取，窃听等；（ ）用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等。

A. 认证 加密

B. 认证 认证

C. 加密 认证

D. 加密 加密

参考答案：C

难易程度：一级

解析：加密用于确保数据的保密性，阻止对手的被动攻击，如截取，窃听等；认证用以确保报文发送者和接收者的真实性以及报文的完整性,阻止对手的主动攻击,如冒充、篡改、重播等

知识子域：密码学基础

21. 公钥基础设施（PKI）的组成一般包括证书权威机构(CA)、证书注册机构(RA)、证书库和终端实体等部分。以下哪个属于证书权威机构(CA)的工作（）

A. 作为 PKI 管理实体和服务的提供者，管理用户数字证书的生成、发放、更新和撤销等工作。

B. 是数字证书的申请、审核和注册中心

C. 用来发布、存储数字证书和证书撤销列表(CRL)，供用户查询、获取其他用户的数字证书和系统中的证书撤销列表所用

D. 拥有公私密钥对和相应公钥证书的最终用户，可以是人、设备、进程等。

参考答案：A

难易程度：一级

解析：CA 是证书签发权威，也称数字证书管理中心，它作为 PKI 管理实体和服务的提供者，管理用户数字证书的生成、发放、更新和撤销等工作。

知识子域：密码学基础

22. 密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面：保密性、完整性和（　）

A. 可维护性

B. 灵活性

C. 可用性

D. 持久性

参考答案：C

难易程度：一级

解析：密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面：保密性、完整性和可用性。

知识子域：密码学基础

23. 密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面：保密性、完整性和可用性。（　）是确保信息仅被合法用户访问，二不被泄露给非授权的用户、实体或过程，或供其利用的特性。

A. 保密性

B. 完整性

C. 可用性

D. 以上都不是

参考答案：A

难易程度：一级

解析：保密性是确保信息仅被合法用户访问，二不被泄露给非授权的用户、实体或过程，或供其利用的特性

知识子域：密码学基础

24. （）是实体身份的一种计算机表达。信息系统在执行操作时，首先要求用户标识自己的身份，并提供证明自己身份的依据，不同的系统使用不同的方式表示实体的身份，同一个实体可以有多个不同的身份。（）是将标识和实体联系在一起的过程。（）是信息系统的第一道安全防线，也为其他安全服务提供支撑。

A. 标识　标识　鉴别

B. 标识　鉴别　鉴别

C. 鉴别　鉴别　标识

D. 鉴别　标识　标识

参考答案：B

难易程度：一级

解析：标识是实体身份的一种计算机表达。信息系统在执行操作时，首先要求用户标识自己的身份，并提供证明自己身份的依据，不同的系统使用不同的方式表示实体的身份，同一个实体可以有多个不同的身份。鉴别是将标识和实体联系在一起的过程。鉴别是信息系统的第一道安全防线，也为其他安全服务提供支撑。

知识子域：身份鉴别与访问控制。

25. 在一个给定的网络中，客户 C 需要访问服务器 S 的服务，客户 C 必须被服务器 S 鉴别，同时客户 C 也需要鉴别服务器 B，那么这种鉴别属于哪种类型的鉴别（）

A. 单项鉴别

B. 双向鉴别

C. 第三方鉴别

D. 以上都不是

参考答案：B

难易程度：一级

解析：在一个给定的网络中，客户 C 需要访问服务器 S 的服务，客户 C 必须被服务器 S 鉴别，客户 C 也需要鉴别服务器 S，则称为双向鉴别。

知识子域：身份鉴别与访问控制

26. 有一些情况要求由双方均信任的第三方来确认用户和服务器的身份。这个属于哪种鉴别类型（）

A. 单项鉴别

B. 双向鉴别

C. 第三方鉴别

D. 以上都不是

参考答案：C

难易程度：一级

解析：有一些情况要求由双方均信任的第三方进行鉴别，以确认用户和服务器的身份。属于第三方鉴别。

知识子域：身份鉴别与访问控制

27. 实体身份鉴别一般依据实体所知、实体所有和实体特征。给自己的电脑设置开机密码属于那种身份鉴别方式（）

A. 实体所知

B. 实体所有

C. 实体特征

D. 实体所感

参考答案：A

难易程度：一级

解析：电脑设置开机密码、口令属于实体所知。

知识子域：身份鉴别与访问控制

28. 用户使用的鉴别依据(口令)通常由系统默认生成或由用户生成，为了记忆的方便，用户通常不对系统生成的默认口令进行更改或选择与自己相关的信息来设置口令，这种类型的口令虽然便于记忆，但容易猜测，对攻击者而言，使用这样口令进行保护的系统是非常脆弱的。以下哪个口令比较安全（）

A. admin123

B. Password

C. Qq123W2!

D. 147poi

参考答案：C

难易程度：一级

解析：C 有大小写字母、数字以及特殊字符组成。

知识子域：身份鉴别与访问控制

29. 重放攻击又称重播攻击、回放攻击，是指攻击者发送一个目的主机（需要登录的服务器）已接收过的数据包，特别是在认证的过程中用于认证用户身份时所接收的数据包以达到欺骗系统的目的。以下不属于重放攻击的防御措施的是（）

A. 在会话中引入时间戳

B. 错误次数超过 5 次锁定账户

C. 使用一次性口令

D. 在会话中引入随机数

参考答案：B

难易程度：一级

解析：B 选项是用来防御暴力破解、枚举。

知识子域：身份鉴别与访问控制

30. 实体身份鉴别一般依据实体所知、实体所有和实体特征。随着技术的成熟及硬件成本的不断下降，使用实体生物特征作为鉴别方式越来越广泛，下面哪个不是实体特征具有的特点是（）

A. 普遍性

B. 即时性

C. 唯一性

D. 稳定性

参考答案：B

难易程度：一级

解析：实体特征鉴别方式具有以下特点：普遍性、唯一性、稳定性、可比性。

知识子域：身份鉴别与访问控制

31. 在信息系统中，访问控制是重要的安全功能之一。以下不属于访问控制模型的特点的是（）

A. 只涉及安全性质，不过多牵扯系统的功能或其实现细节

B. 复杂的，不易理解

C. 精确的、无歧义的

D. 简单的、抽象的，容易理解

参考答案：B

难易程度：一级

解析：访问控制模型具有以下三个特点：精确的、无歧义的；简单的、抽象的，容易理解；只涉及安全性质，不过多牵扯系统的功能或其实现细节。

知识子域：身份鉴别与访问控制

32. （）是使信息在客体间流动的一种实体。（）是一种信息实体，或者是从其它主体或客体接收信息的实体。通常（）是指人、进程或设备等。通常数据块、存储页、文件、目录、程序等都属于（）。

A. 主体 客体 主体 客体

B. 主体 主体 客体 客体

C. 主体 客体 客体 主体

D. 客体 主体 客体 主体

参考答案：A

难易程度：一级

解析：主体是使信息在客体间流动的一种实体。通常主体是指人、进程或设备等。客体是一种信息实体，或者是从其它主体或客体接收信息的实体。通常数据块、存储页、文件、目录、程序等都属于客体。

知识子域：身份鉴别与访问控制

33. 常见的访问控制模型有（）

A. 自主访问控制

B. 强制访问控制

C. 基于角色地访问控制模型

D. 以上都是

参考答案：D

难易程度：一级

解析：常见的访问控制模型有：自主访问控制、强制访问控制、基于角色地访问控制模型

知识子域：身份鉴别与访问控制

34. 关于自主访问模型，以下说法正确地是（）

A. DAC 资源的所有者，往往也是资源地创建者，可以规定谁有权访问它们地资源。

B. DAC 可为用户提供灵活调整地安全策略，具有较好地易用性和可扩展性。

C. DAC 具有某种访问能力地主体能够自主地将访问全地某个自己授予其他主体。

D. DAC 常用于多种商务系统中，安全性较高。

参考答案：D

难易程度：一级

解析：DAC 常用于多种商务系统中，安全性较低

知识子域：身份鉴别与访问控制

35. 自主访问模型（DAC）通常使用（）来实现访问控制功能

A. 访问控制矩阵

B. 访问控制能力表

C. 访问控制主体

D. 访问控制客体

参考答案：B

难易程度：一级

解析：DAC 通常使用访问控制表(ACL)或能力表(CL)来实现访问控制功能

知识子域：身份鉴别和访问控制

36. 以下不属于强制访问控制模型的是（）

A. BLP 模型

B. RBAC 模型

C. Biba 模型

D. Clark-Wilson 模型

参考答案：B

难易程度：一级

解析：典型的强制访问控制模型包括：BLP 模型、Biba 模型、Clark-Wilson 模型、Chinese Wall 模型等，RBAC 是基于角色的访问控制模型。

知识子域：身份鉴别和访问控制

37. 开放系统互连模型(OSI)是国际标准化组织发布的通信模型，OSI 七层模型从低到高依次是（）

A. 物理层、数据链路层、网络层、传输层、会话层、表示层和应用层

B. 物理层、数据链路层、传输层、网络层、会话层、表示层和应用层

C. 物理层、数据链路层、传输层、网络层、表示层、会话层和应用层

D. 物理层、网络层、数据链路层、传输层、表示层、会话层和应用层

参考答案：A

难易程度：一级

解析：OSI 七层模型从低到高依次是物理层、数据链路层、网络层、传输层、会话层、

表示层和应用层。

知识子域：网络安全协议

38. 对于 OSI 七层模型中，传输层的作用是（）

A. 不同应用程序的数据隔离，同步服务

B. 逻辑寻址，路径选择

C. 提供端到端的数据传输服务，建立逻辑连接

D. 建立、维护和拆除物理链路层的连接

参考答案：C

难易程度：一级

解析：传输层的作用提供端到端的数据传输服务，建立逻辑连接

知识子域：网络安全协议

39. 在 OSI 七层模型中，提供用户程序“接口”，如文件传输，文件管理，电子邮件的信息处理等的是（）

A. 物理层

B. 网络层

C. 传输层

D. 应用层

参考答案：D

难易程度：一级

解析：应用层提供用户程序“接口”，如文件传输，文件管理，电子邮件的信息处理等。

知识子域：网络安全协议

40. TCP/IP 是目前互联网使用的最基本的协议，也是互联网构成的基础协议。TCP/IP 架构包括（）

A. 链路层、传输层、会话层、应用层

B. 网络层、传输层、表示层、应用层

C. 链路层、网络层、传输层、应用层

D. 物理层、链路层、网络层、应用层

参考答案：C

难易程度：一级

解析：TCP/IP 体系架构包括链路层、网络层、传输层、应用层四层。

知识子域：网络安全协议

41. TCP/IP 协议族设计的目的是为实现不同类型的计算机系统互连，从设计之初就考虑到不同类型的计算机设备的特性，具有较好的开放性，但是存在很多安全风险，著名的 ARP 欺骗就是利用 ARP 协议无状态、无需请求就可以应答和缓存机制的问题实现，攻击者通过伪造 ARP 应答报文修改计算机上的 ARP 缓存实现欺骗。ARP 欺骗属于（）

A. 链路层的安全风险

B. 网络层的安全风险

C. 传输层的安全风险

D. 应用层的安全风险

参考答案：A

难易程度：一级

解析：链路层主要的两个协议 ARP 和 RARP，由于缺乏认证机制，很容易被攻击者利用实施欺骗攻击

知识子域：网络安全协议

42. **TCP/IP 协议族设计的目的是为实现不同类型的计算机系统互连，具有较好的开放性，但同时也存在很多安全风险，以下属于网络层的安全风险的是（）**

A. ARP 欺骗攻击

B. IP 地址欺骗攻击

C. SYN Flood 拒绝服务攻击

D. UDP Flood 拒绝服务攻击

参考答案：B

难易程度：一级

解析：IP 是网络层的协议

知识子域：网络安全协议

43. **应用层是 TCP/IP 体系的最高层，同的应用层协议实现差异较大，根据各自特性都有自身的安全性问题。以下属于应用层的安全风险的是（）**

A. 身份认证简单，通常使用用户名和登录口令进行认证或匿名方式，面临口令破解、身份伪造等攻击威胁。

B. 使用明文传输数据，由于应用层协议在设计时对安全性缺乏考虑，通常使用明文传输数据，由此导致了数据泄露、数据伪造等一系列问题，例如攻击者可能通过嗅探等方式获取传输中的敏感信息。

C. 缺乏数据完整性保护，由此带来了数据破坏、篡改等问题，例如攻击者可更改用户提交的数据，从而实施欺诈。

D. 以上都对

参考答案：D

难易程度：一级

解析：参考应用层的安全风险问题。

知识子域：网络安全协议

44. **IPSec(互联网协议安全)是 IETF(互联网工程任务组)制定的一组开放的网络安全协议。IPSec 属于（）**

A. 链路层

B. 网络层

C. 传输层

D. 应用层

参考答案：B

难易程度：一级

解析：IPSec 属于网络层

知识子域：网络安全协议

45. **TCP/IP 协议族安全性问题随着互联网的发展日益突出，相关组织和专家也对协议进行不断的改善和发展，为不同层次设计了相应的安全通信协议，用于对不同层次的通信进行安全保护，从而形成了由各层次安全通信协议构成的 TCP/IP 协议族安全架构。以下哪个协议属于链路层（）**

A. SNMP

B. S/MIME

C. L2TP

D. SSL

参考答案：C

难易程度：一级

解析：L2TP 属于链路层、SNMP 属于应用层、S/MIME 属于应用层、SSL 属于传输层

知识子域：网络安全协议

46. 基于 TCP/IP 协议族的安全架构，以下哪些协议属于应用层（）

（1） HTTPS（2）PPP（3）IPSec（4）SNMP（5）SSH（6）PPTP（7）SFTP

A. （1）（2）（5）（6）

B. （1）（4）（5）（7）

C. （2）（3）（4）（7）

D. （1）（4）（5）（6）（7）

参考答案：B

难易程度：一级

解析：HTTPS、SNMP、SSH、SFTP 属于应用层协议，PPP、PPTP 属于链路层协议，IPSec 属于网络层协议

知识子域：网络安全协议

47. 下列哪个不是基于实体特征的鉴别（）

A. 指纹、掌纹

B. 手机门禁卡

C. 面部识别

D. 语音识别

参考答案：B

难易程度：一级

解析：钥匙属于实体所有

知识子域：身份鉴别与访问控制

48. 在 TCP/IP 协议中，发送邮件使用的是（）。

A. SMTP

B. SNMP

C. PPTP

D. POP3

参考答案：A

难易程度：一级

解析：在 TCP/IP 协议中，发送邮件使用的是 SMTP。

知识领域：网络安全协议

49. 在 TCP/IP 协议中，发送邮件使用的是 SMTP 协议，默认端口号为（）。

A. 22

B. 25

C. 21

D. 23

参考答案：B

难易程度：一级

解析：在 TCP/IP 协议中，发送邮件使用的是 SMTP，默认端口号为 25。

知识领域：网络安全协议

50. 在 TCP/IP 协议中，IGMP 协议指的是（），位于 TCP/IP 协议的（）。

A. Internet 组管理协议 传输层

B. Internet 组管理协议 网络层

C. Internet 控制报文协议 网络层

D. Internet 控制报文协议 传输层

参考答案：B

难易程度：一级

解析：在 TCP/IP 协议中，IGMP 协议指的是 Internet 组管理协议，位于 TCP/IP 协议的网络层。

知识领域：网络安全协议

51. 在 TCP/IP 协议中，接收邮件使用的是（）。

A. POP

B. POP3

C. PPP

D. PPTP

参考答案：B

难易程度：一级

解析：在 TCP/IP 协议中，接收邮件使用的是 POP3。

知识领域：网络安全协议

52. 在 TCP/IP 协议中，接收邮件使用的是 POP3，默认端口号为（）。

A. 138

B. 110

C. 112

D. 139

参考答案：B

难易程度：一级

解析：在 TCP/IP 协议中，接收邮件使用的是 POP3，默认端口号为 110。

知识领域：网络安全协议

53. 在 TCP/IP 协议中，HTTPS 协议指的是（）

A. HTTP+SSH

B. HTTP+SSL

C. HTTP+SET

D. HTTP+SNMP

参考答案：B

难易程度：一级

解析：HTTPS 协议是由 HTTP 协议和 SSL 协议组成。

知识子域：网络安全协议

54. HTTPS 协议提供服务的默认端口是（）

A. 445

B. 80

C. 443

D. 22

参考答案：C

难易程度：一级

知识子域：网络安全协议

55. 在 TCP/IP 协议中，SFTP 协议指（）。

A. SSL 文件传输协议

B. SSH 文件传输协议

C. 简单文件传输协议
D. 文件传输协议
参考答案：B
难易程度：一级
解析：SFTP 指的是 SSH 文件传输协议。
知识子域：网络安全协议

56. 在 TCP/IP 协议中，SFTP 协议指 SSH 文件传输协议，默认端口号是（）。
A. 21
B. 22
C. 25
D. 23
参考答案：B
难易程度：一级
解析：SFTP 指的是 SSH 文件传输协议，默认端口号 22
知识子域：网络安全协议

57. 云计算是一种计算资源的新型利用模式,客户以购买服务的方式,通过网络获得计算、存储、软件等不同类型的资源。以下哪个不是云计算的特征（）
A. 服务不可计量
B. 快速伸缩性
C. 泛在接入
D. 资源池化
参考答案：A
难易程度：一级
解析：云计算主要有以下特征：按需自助服务、泛在接入、资源池化、快速伸缩性、服务可计量
知识子域：新技术领域

58. 以下哪个属于大数据平台安全风险（）
A. 大数据基础设施的安全风险
B. 大数据承载平台自身的安全风险
C. 大数据平台软件的安全漏洞风险
D. 以上都是
参考答案：D
难易程度：一级
解析：大数据平台安全的风险首先是基础设施的安全风险，也就是大数据承载平台自身的安全风险，其次，大数据平台软件也会存在安全漏洞。
知识子域：新技术领域

59. 大数据的生命周期包括（）
A. 数据采集、数据存储、数据处理、数据分发、数据删除
B. 数据采集、数据存储、数据处理、数据加密、数据删除
C. 数据采集、数据加密、数据处理、数据分发、数据删除
D. 数据采集、数据存储、数据处理、数据分发、数据加密
参考答案：A
难易程度：一级
解析：大数据的生命周期包括数据采集、数据存储、数据处理、数据分发、数据删除等

知识子域：新技术领域

60. （）作为互联网新兴技术，以其高可伸缩性、成本低廉、运维便利等优点被越来越多的企业采纳使用；（）是指大小超出常规数据库软件工具收集、存储、管理和分析能力的数据集；（）是指通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式；（）是指传统数据架构无法有效处理的新数据集。

A. 云计算　大数据　云计算　大数据
B. 大数据　云计算　大数据　云计算
C. 云计算　云计算　大数据　大数据
D. 大数据　大数据　云计算　云计算

参考答案：A

难易程度：一级

解析：云计算作为互联网新兴技术，以其高可伸缩性、成本低廉、运维便利等优点被越来越多的企业采纳使用；大数据是指大小超出常规数据库软件工具收集、存储、管理和分析能力的数据集；云计算是指通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式；大数据是指传统数据架构无法有效处理的新数据集。

知识子域：新技术领域

61. 以下哪个不符合数据采集阶段的安全要求（）

A. 定义采集数据的目的和用途，明确数据采集源和采集数据范围
B. 遵循合规原则，确保数据采集的合法性，正当性和必要性
C. 遵循数据最大化原则，采集满足业务所需的所有数据
D. 遵循质量保障原则，制定数据质量保障的策略、规程和要求

参考答案：C

难易程度：一级

解析：在数据采集阶段，安全要求为：定义采集数据的目的和用途，明确数据采集源和采集数据范围；遵循合规原则，确保数据采集的合法性，正当性和必要性；遵循数据最小化原则，只采集满足业务所需的最少数据；遵循质量保障原则，制定数据质量保障的策略、规程和要求；遵循确保安全原则，对采集的数据进行分类分级标识，并对不同类和级别的数据实施相应的安全管理策略和保障措施，对数据采集环境、设施和技术采取必要的安全管控措施。

知识子域：新技术领域

62. 关于移动互联网安全风险，下列属于开放信道带来的安全风险的是（）

A. 通信内容可能被窃听，篡改、通信用户身份可能被假冒等安全风险。
B. 业务流程缺乏安全风险分析，使得用户的个人利益受到损害。
C. 智能终端功能不断的多样化，使得安全风险不断累积，为用户带来了越来越多的安全风险。
D. 对不良信息没有严格审核，产生了一些不良的影响，包括色情、虚假、夸大甚至非法言论。

参考答案：A

难易程度：一级

解析：开封信道会带来的安全风险有：通信内容可能被窃听，篡改、通信用户身份可能被假冒等安全风险。

知识子域：新技术领域

63. 以下关于移动互联网安全防护的说法不正确的是（）

A. 设备/环境安全：设备环境不重要，能运行就可以。

B. 业务应用安全：业务管理信息安全和控制信息安全。
C. 技术系统安全：信息完整性，保密性，不可否认性。
D. 个人隐私保护：不传播非法、违背社会公德、侵犯公民隐私的信息。
参考答案：A
难易程度：一级
解析：设备/环境安全：设备环境符合标准要求，防攻击防入侵。
知识子域：新技术领域

64. 关于物联网安全风险下列说法不正确的是（）

A. 物联网导致的隐私泄露问题
B. 物联网平台不存在安全漏洞带来的安全问题
C. 物联网终端的移动性对信息安全带来的管理困难问题
D. 物联网快速增长的设备数量使得对设备的更新和维护都较为困难，终端设备的漏洞很难得到有效的修复
参考答案：B
难易程度：一级
解析：物联网平台存在的安全漏洞带来的安全问题。
知识子域：新技术领域

65. 与传统的互联网不同，物联网涉及感知、控制、网络通信、微电子、计算机、软件、嵌入式系统、微机电等技术领域，涵盖的关键技术非常多。典型的物联网体系结构通常包括（）

A. 感知层、物理层、支撑层和应用层
B. 感知层、传输层、支撑层和设备层
C. 感知层、传输层、支撑层和应用层
D. 感知层、传输层、处理层和应用层
参考答案：C
难易程度：一级
解析：典型的物联网体系结构通常包括感知层、传输层、支撑层和应用层四个层级。
知识子域：新技术领域

66. （）作为“中国智造”和“互联网+先进制造业”的核心要求，是推进制造强国和网络强国的重要基础。（）是把任何物品与互联网连接起来进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络。（）是移动通信和互联网发展到一定阶段的必然发展方向和融合产物。

A. 互联网　移动互联网　工业互联网
B. 物联网　工业互联网　移动互联网
C. 工业互联网　物联网　移动互联网
D. 移动互联网　工业互联网　物联网
参考答案：C
难易程度：一级
解析：工业互联网作为“中国智造”和“互联网+先进制造业”的核心要求，是推进制造强国和网络强国的重要基础。物联网(IoT)是把任何物品与互联网连接起来进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络。移动互联网是移动通信和互联网发展到一定阶段的必然发展方向和融合产物。
知识子域：新技术领域

67. 以下哪个属于工业控制系统（）

A. 数据采集与监控系统（SCADA）
B. 分布式控制系统（DCS）
C. 可编辑逻辑控制器（PLC）
D. 以上都是
参考答案：D
难易程度：一级
解析：数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编辑逻辑控制器（PLC）都属于工业控制系统。
知识子域：新技术领域

68. 下列关于 TCP 和 UDP 的说法不正确的是（）
A. TCP 协议是面向连接的通信协议。
B. TCP 协议能为应用程序提供可靠的通信连接。
C. UDP 传输协议是一种不可靠的面向无连接、可以实现多对一、一对多和一对一连接的通信协议。
D. UDP 传输协议适用于一次传送大量数据、对可靠性要求高的应用环境。
参考答案：D
难易程度：一级
解析：UDP 传输协议适用于一次只传送少量数据、对可靠性要求不高的应用环境。
知识领域：网络安全协议

69. 基于实体所知的鉴别中，口令鉴别由于简单易行，并且实现成本低，被广泛的应用在各类商业系统中，口令安全也一直是人们关注的重点，一个好的口令应当具备（）。
A. 使用多种字符
B. 定期更换
C. 尽量随机
D. 以上都是
参考答案：D
难易程度：一级
解析：一个好的口令应当使用多种字符、尽量随机、定期更换。
知识子域：身份鉴别与访问控制

70. 以下基于实体所知的鉴别威胁的是（）。
A. 暴力破解攻击
B. 窃听攻击
C. 重放攻击
D. 以上都是
参考答案：D
难易程度：一级
解析：基于实体所知的鉴别威胁的有：暴力破解攻击、窃听攻击、重放攻击。
知识子域：身份鉴别和访问控制

71. 下列哪个不是关于实体所知的鉴别威胁中的暴力破解的防护（）。
A. 使用安全的密码（自己容易记，别人不好猜，高强度，高复杂度）
B. 在会话中引入随机数
C. 设置系统、应用的安全策略
D. 随机验证码（变形、干扰、滑块、图像识别等）
参考答案：B

难易程度：一级

解析：在会话中引入随机数是针对重放攻击的防御。

知识子域：身份鉴别和访问控制

72. 目前通用的网络模型有两种，OSI 模型分为（）层，TCP/IP 模型分为（）层。

A. 7　3

B. 7　4

C. 5　5

D. 5　4

参考答案：B

难易程度：一级

解析：目前通用的网络模型有两种，OSI 模型分为 7 层，TCP/IP 模型分为 4 层。

知识子域：网络安全协议

73. PPP 协议提供了中在点到点链路上封装网络层协议信息的标准方法，其英文是（）。

A. The Point-to-Point Protocol

B. Point-to-Point Protocol over Ethernet

C. Point- Point-Point Protocol

D. Ethernet Protocol

参考答案：A

难易程度：一级

解析:PPP 协议提供了中在点到点链路上封装网络层协议信息的标准方法,其英文是(The Point-to-Point Protocol)

知识子域：网络安全协议

74. 目前广泛应用于浏览器与服务器之间身份认证和加密数据传输的协议是（）。

A. SSH 协议

B. SMTP 协议

C. SSL 协议

D. HTTP 协议

参考答案：C

难易程度：一级

解析:目前广泛应用于浏览器与服务器之间身份认证和加密数据传输的协议是 SSL 协议。

知识子域：网络安全协议

75. 安全传输层协议 TLS 用于在两个通信应用程序之间提供保密性和数据完整性，它的英文全称是（）。

A. Transport Layer Secure Protocol

B. Transport Layer Security Protocol

C. Transfer Layer Secure Protocol

D. Transport Layer Secure Protocol

参考答案：B

难易程度：一级

解析：安全传输层协议 TLS 它的英文全称 Transport Layer Security Protocol

知识子域：网络安全协议

76. SSH 协议是在（）与（）之间的加密隧道应用协议。

A. 网络层　传输层

B. 传输层　应用层

C. 数据链路层　网络层

D. 网络层　应用层

参考答案：B

难易程度：一级

解析：SSH 协议是在传输层与应用层之间的加密隧道应用协议。

知识子域：网络安全协议

77. 在 TCP/IP 协议中，由于 TCP 协议提供可靠的连接服务，采用（）来创建一个 TCP 连接；采用（）来断开 TCP 连接。

A. 三次握手　三次挥手

B. 三次握手　四次挥手

C. 四次握手　三次挥手

D. 四次握手　四次挥手

参考答案：B

难易程度：一级

解析：TCP 协议提供可靠的连接服务，采用三次握手来创建一个 TCP 连接；采用四次挥手来断开 TCP 连接。

知识子域：网络安全协议

78. 应用层协议定义了运行在不同端系统上的应用程序进程如何相互传递报文。下列不属于应用层协议的是（）。

A. HTTP 协议

B. FTP 协议

C. Telnet

D. UDP 协议

参考答案：D

难易程度：一级

解析：UPD 协议属于传输层协议。

知识子域：网络安全协议

79. 以下不属于公钥密码的优点的是（）。

A. 加密速度快、计算简单

B. 解决了密钥传递问题

C. 大大减少了密钥持有量

D. 提供了对称密码技术无法或很难提供的服务（数字签名）

参考答案：A

难易程度：一级

解析：公钥密码计算复杂、消耗资源大。

知识子域：密码学基础

80. 公钥基础设施（PKI）的组成一般包括证书权威机构(CA)、证书注册机构(RA)、证书库和终端实体等部分。以下哪个属于证书注册机构(RA)的工作（）。

A. 作为 PKI 管理实体和服务的提供者，管理用户数字证书的生成、发放、更新和撤销等工作。

B. 是数字证书的申请、审核和注册中心

C. 用来发布、存储数字证书和证书撤销列表(CRL)，供用户查询、获取其他用户的数字证书和系统中的证书撤销列表所用

D. 拥有公私密钥对和相应公钥证书的最终用户，可以是人、设备、进程等。

参考答案：B

难易程度：一级

解析：证书注册机构(RA)负责数字证书的申请、审核和注册中心。

知识子域：密码学基础

81. 以下对数字证书的描述正确的是（）。

A. 一段电子数据

B. 经证书权威机构 CA 签名的数据体

C. 包含拥有者身份信息和公开密钥的数据体

D. 以上都是

参考答案：D

难易程度：一级

解析：数字证书是一段电子数据，是经证书权威机构 CA 签名的，包含拥有者身份信息和公开密钥的数据体。

知识子域：密码学基础

82. 以下关于数字证书的说法错误的是（）。

A. 数字证书可以做为终端实体的身份证明。

B. 数字证书常用来解决相互间的信任问题。

C. 数字证书一定是可靠的。

D. 数字证书可以保证信息和数据的完整性和安全性。

参考答案：C

难易程度：一级

解析：数字证书不一定是可靠的。

知识子域：密码学基础

83. 关于对称密码算法缺点，以下说法错误的是（）。

A. 安全信道难以实现

B. 算法复杂、计算量大

C. 安全交换密钥问题及密钥管理复杂

D. 无法解决对消息的篡改、否认等问题

参考答案：B

难易程度：一级

解析：对称密码算法的算法简单、计算量小。

知识子域：密码学基础

84. 下列不属于公钥密码的特点的是（）。

A. 公钥私钥成对出现

B. 加密密钥和解密密钥相同

C. 公钥加密私钥解密-机密性

D. 私钥加密公钥解密-数字签名

参考答案：B

难易程度：一级

解析：公钥密码的加密密钥和解密密钥不同。

知识子域：密码学基础

85. 以下不属于非对称密码算法的是（）。

A. RSA

B. ECC

C. Rabin

D. RC5

参考答案：D

难易程度：一级

解析：RC5 属于对称密码算法

86. 哈希函数也称为（），它可以将（）信息映射为（）的值。

A. 随机函数　固定长度　固定长度

B. 随机散列函数　任意有限长度　固定长度

C. 单项散列函数　任意有限长度　固定长度

D. 双向随机函数　固定长度　固定长度

参考答案：C

难易程度：一级

解析：哈希函数也称为单向散列函数，它可以将任意有限长度信息映射为固定长度的值。

知识子域：密码学基础

87. 公钥基础设施（PKI）也称公开密钥基础设施，它的英文名称是（）。

A. Pubilc Key Infrastructure

B. Pubilc Keys Infrastructural

C. Public Secret Key Infrastructure

D. Public Secret Keys Infrastructural

参考答案：A

难易程度：一级

解析：公钥基础设施（Pubilc Keys Infrastructure，PKI）也称公开密钥基础设施。

知识子域：密码学基础

88. 身份鉴别的相关实体包括（）。

A. 验证者　被验证者

B. 被验证者　验证者　可信赖者

C. 被验证者　可信赖者

D. 验证者　可信赖者

参考答案：B

难易程度：一级

解析：身份鉴别的相关实体包括被验证者、验证者、可信赖者。

知识子域：身份鉴别与访问控制

89. 以下基于实体所有的鉴别威胁的是（）。

A. 用于鉴别的物品可能被复制

B. 用于鉴别的物品可能被篡改

C. 用于鉴别的物品可能被损坏

D. 以上都是

参考答案：D

难易程度：一级

解析：基于实体所有的鉴别威胁有：用于鉴别的物品可能被复制、篡改、损坏。

知识子域：身份鉴别与访问控制

90. OSI 七层模型分为底层协议和高层协议，底层协议偏重于处理实际的信息传输，复制创建网络通信连接的链路，包括（）；高层协议处理用户服务和各种应用请求，包括（）。

A. 物理层、数据链路层　　网络层、传输层、会话层、表示层、应用层

B. 物理层、数据链路层、网络层　　传输层、会话层、表示层、应用层

C. 物理层、数据链路层、网络层、传输层　　会话层、表示层、应用层

D. 物理层、数据链路层、网络层、传输层、会话层　　表示层、应用层

参考答案：C

难易程度：一级

解析：OSI 七层模型分为底层协议和高层协议，底层协议偏重于处理实际的信息传输，复制创建网络通信连接的链路，包括物理层、数据链路层、网络层、传输层；高层协议处理用户服务和各种应用请求，包括会话层、表示层、应用层。

知识子域：网络安全协议

91. 在 TCP/IP 的体系架构中，ARP 协议位于（），它的作用是（）。

A. 网络层　将 MAC 地址解析为 IP 地址

B. 链路层　将 MAC 地址解析为 IP 地址

C. 网络层　将 IP 地址解析为 MAC 地址

D. 链路层　将 IP 地址解析为 MAC 地址

参考答案：D

难易程度：一级

解析：在 TCP/IP 的体系架构中，ARP 协议位于链路层，它的作用是将 IP 地址解析为 MAC 地址。

知识子域：网络安全协议

92. 链路层也称网络接口层或数据链路层，是 TCP/IP 的最底层，它负责（）。

A. 接收来自网络层的 IP 数据报，并把数据报发送到指定的网络上，或从网络上接收物理帧，抽出网络层数据报，交给网络层。

B. 用于实现数据包在网络中正确的传递。

C. 为两台主机上的应用程序提供端到端的通信服务。

D. 为用户提供不同的互联网服务。

参考答案：A

难易程度：一级

解析：链路层也称网络接口层或数据链路层，是 TCP/IP 的最底层，它负责接收来自网络层的 IP 数据报，并把数据报发送到指定的网络上，或从网络上接收物理帧，抽出网络层数据报，交给网络层。

知识子域：网络安全协议

93. 《加强工业互联网安全工作的指导意见》给出了工业互联网安全体系建设的指导思想，明确提出了达成目标的（）和（）。

A. 七个主要任务　四项保障措施

B. 四个主要任务　七项保障措施

C. 五个主要任务　四项保障措施

D. 七个主要任务　五项保障措施

参考答案：A

难易程度：一级

解析：《加强工业互联网安全工作的指导意见》给出了工业互联网安全体系建设的指导思想，明确提出了达成目标的七个主要任务和四项保障措施。

知识子域：新技术领域

94. 世界第一台计算机诞生于（）。

A. 1945

B. 1946
C. 1947
D. 1948
参考答案：B
难易程度：一级
解析：世界上第一台计算机，电子数字积分计算机(ENIAC)于 1946 年 2 月 14 日在宾夕法尼亚大学诞生。
知识子域：计算机网络与网络设备

95. 世界上第一台计算机，电子数字积分计算机(ENIAC)诞生于（）。
A. 中国
B. 法国
C. 美国
D. 德国
参考答案：C
难易程度：一级
解析：世界上第一台计算机，电子数字积分计算机(ENIAC)于 1946 年 2 月 14 日在宾夕法尼亚大学诞生。
知识子域：计算机网络与网络设备

96. 以下哪个不属于计算机网络按覆盖范围的划分（）。
A. 城域网
B. 局域网
C. 广域网
D. 专用网
参考答案：D
难易程度：一级
解析：计算机网络根据覆盖范围分为广域网、城域网和局域网。
知识子域：计算机网络与网络设备

97. 学校的校园网络根据覆盖范围，属于（）。
A. 局域网
B. 专用网
C. 城域网
D. 广域网
参考答案：A
难易程度：一级
解析：学校的校园网根据覆盖范围属于局域网。
知识子域：计算机网络与网络设备

98. 关于计算机网络分类，下列说法正确的是（）。
A. 广域网用来将多个局域网进行互联。
B. 公众网是某个组织为满足本组织内部的特殊业务工作需要而建立的网络
C. 局域网是将微型计算机或工作站通过通信线路连接，作用距离比较小，
D. 专用网指网络服务提供商建设，供公共用户使用的通信网络。
参考答案：C
难易程度：一级
解析：广域网是互联网的核心部分，其任务是通过长距离传输主机所发送的数据。公众

网指网络服务提供商建设，供公共用户使用的通信网络。专用网是某个组织为满足本组织内部的特殊业务工作需要而建立的网络。

知识子域：计算机网络与网络设备

99. 每一个计算机网络都由节点和（）构成,节点也称为（）。

A. 链路　数据单元

B. 链路　网络单元

C. 网络　网络单元

D. 网络　数据单元

参考答案：B

难易程度：一级

解析：每一个计算机网络都由节点和链路构成,节点也称为网络单元。

100. 计算机网络的节点分为（）。

A. 转换节点和访问节点

B. 交换节点和控制节点

C. 转换节点和控制节点

D. 访问节点和控制节点

参考答案：A

难易程度：一级

解析：计算机网络的节点包括：转换节点和访问节点。

知识子域：计算机网络与网络设备

101. （）是多个访问节点通过通信链路连接到一个中央节点进行相互通信组成的结构，中央节点根据集中的通信控制策略对不同的访问节点的访问进行管理和控制。

A. 星型拓扑

B. 网状拓扑

C. 环型拓扑

D. 树型拓扑

参考答案：A

难易程度：一级

解析：星型拓扑是多个访问节点通过通信链路连接到一个中央节点进行相互通信组成的结构，中央节点根据集中的通信控制策略对不同的访问节点的访问进行管理和控制。

知识子域：计算机网络与网络设备

102. 以下属于星型拓扑结构的优点的是（）。

A. 结构简单，连接方便

B. 管理和维护都较为容易

C. 扩展性强

D. 以上都是

参考答案：D

难易程度：一级

解析：星型拓扑结构简单，连接方便，管理和维护都较为容易，并且扩展性强，是目前应用最广泛的网络结构。

知识子域：计算机网络与网络设备

103. （）是无线通信技术与网络技术相结合的产物是通过无线信道来实现网络设备之间的通信，是目前应用最为广泛的一种短程无线传输技术。

A. 远程网（LHN）

B. 局域网（LAN）

C. 无线局域网（WLAN）

D. 广域网（WAN）

参考答案：C

难易程度：一级

解析：无线局域网(WLAN)是无线通信技术与网络技术相结合的产物，是通过无线信道来实现网络设备之间的通信，是目前应用最为广泛的一种短程无线传输技术。

知识子域：计算机网络与网络设备

104. 无线局域网目前广泛使用的协议是（）标准族。

A. IEEE802.11x

B. IEEE802.1

C. IEEE801.1x

D. IEEE802.11a

参考答案：A

难易程度：一级

解析：无线局域网目前广泛使用的协议是 IEEE802.11x 标准族。

知识子域：计算机网络与网络设备

105. 无线局域网的基本概念包括（）。

A. 无线接入点、服务集标识和信道

B. 无线工作站、标识和传输通道

C. 无线工作站、服务集和信道

D. 无线信号、服务集和信道

参考答案：A

难易程度：一级

解析：无线局域网的基本概念包括无线接入点、服务集标识和信道。

知识子域：计算机网络与网络设备

106. 在无线局域网的概念中，无线接入点（AP）是（）。

A. 用于标识无线网络，可与将一个无线局域网分为几个需要不同身份验证的子网络。

B. 用于将无线工作站与无线局域网进行有效连接。

C. 是以无线信号作为传输媒体的数据信号传送通道。

D. 以上说法都不对。

参考答案：B

难易程度：一级

解析：无线接入点(AP),用于将无线工作站与无线局域网进行有效连接。

知识子域：计算机网络与网络设备

107. 无线局域网由于使用上的灵活和便利，应用日渐普及，应用广泛也意味着面临越来越多的安全问题。以下属于安全管理防护的是（）。

A. 为访客设立独立的接入网段，并在无线局域网与业务网之间部署隔离设备。

B. 部署入侵检测系统以发现可能的攻击并定期对无线局域网安全性进行审查。

C. 限制无线局域网的使用范围，例如仅用于互联网资料查询和日常办公应用。

D. 对无线局域网接入使用安全可靠的认证和加密技术，如果有必要，可以使用其他增强认证机制。

参考答案：C

难易程度：一级

解析：A、B、D 属于安全技术防护。

知识子域：计算机网络与网络设备

108. **无线局域网由于使用上的灵活和便利，应用日渐普及，应用广泛也意味着面临越来越多的安全问题。以下属于安全技术防护的是（）。**

A. 结合组织机构业务需求对无线局域网的应用进行评估，制定使用和管理策略。

B. 部署入侵检测系统以发现可能的攻击并定期对无线局域网安全性进行审查。

C. 明确定义并限制无线局域网的使用范围，尽量不在无线网络中传输和处理机密和敏感数据。

D. 限制无线局域网的使用范围，例如仅用于互联网资料查询和日常办公应用。

参考答案：B

难易程度：一级

解析：A、C、D 属于安全管理防护。

知识子域：计算机网络与网络设备

109. **用于连接设备、网络及进行相互协商、转换的部件就是网络互联设备，以下不属于网络互联设备的是（）。**

A. 中继器

B. 网卡

C. 集线器

D. 防火墙

参考答案：D

难易程度：一级

解析：常见的互联设备有：网卡、中继器、集线器、网桥、交换机、路由器、网关。

知识子域：计算机网络与网络设备

110. **网卡是网络接口卡(NIC)的简称，它是计算机或其它网络设备所附带的适配器，用于与其他计算机或网络设备进行通信。工作在 OSI 七层模型中的（）**

A. 物理层

B. 数据链路层

C. 网络层

D. 传输层

参考答案：B

难易程度：一级

解析：在 OSI 七层模型中，网卡工作在第二层，即数据链路层。

知识子域：计算机网络与网络设备

111. **中继器是连接网络线路的一种装置，是工作在（）的设备。**

A. 物理层

B. 数据链路层

C. 网络层

D. 传输层

参考答案：A

难易程度：一级

解析：中继器是工作在物理层的设备。

知识子域：计算机网络与网络设备

112. **集线器也称为 HUB，它的工作原理是把一个端口上收到的数据广播发送到其他所有端口上。是一个工作在（）的设备。**

A. 传输层
B. 网络层
C. 数据链路层
D. 物理层
参考答案：D
难易程度：一级
解析：集线器也称为 HUB，它的工作原理是把一个端口上收到的数据广播发送到其他所有端口上。集线器是一个工作在物理层的设备。
知识子域：计算机网络与网络设备

113. 以下网络互联设备不是工作在链路层的是（）。

A. 网卡
B. 交换机
C. 中继器
D. 网桥
参考答案：C
难易程度：一级
解析：中继器工作在物理层。
知识子域：计算机网络与网络设备

114. 网桥也叫桥接器，是用于连接两个局域网的一种存储/转发设备，作用与中继器类似，网桥工作在（）。

A. 物理层
B. 数据链路层
C. 传输层
D. 网络层
参考答案：B
难易程度：一级
解析：网桥也叫桥接器，是用于连接两个局域网的一种存储/转发设备，作用与中继器类似，网桥工作在数据链路层。
知识子域：计算机网络与网络设备

115. 关于网络互联设备交换机的描述正确的是（）

A. 交换机是一种电(光)信号转发的网络设备。
B. 交换机作为多端口的网桥，工作在物理层。
C. 交换机把一个端口上收到的数据广播发送到其他所有端口上。
D. 交换机用于连接网络层之上执行不同协议的子网，组成异构型的因特网。
参考答案：A
难易程度：一级
解析：交换机是一种电(光)信号转发的网络设备，交换机作为多端口的网桥，工作在数据链路层。
知识子域：计算机网络与网络设备

116. 以下网络互联设备不是工作在网络层的是（）。

A. 路由器
B. 三层交换机
C. 网卡
D. 网关

参考答案：C

难易程度：一级

解析：网卡工作在数据链路层。

知识子域：计算机网络与网络设备

117. **（）是工作在 OSI 模型中第三层的网络设备，对不同的网络之间的数据包进行存储、分组转发处理。（）是复杂的网络互联网设备，它用于连接网络层之上执行不同协议的子网，组成异构型的因特网。**

A. 路由器　网卡

B. 交换机　网关

C. 网关　路由器

D. 路由器　网关

参考答案：D

难易程度：一级

解析：路由器是工作在 OSI 模型中第三层的网络设备，对不同的网络之间的数据包进行存储、分组转发处理。网关是复杂的网络互联网设备，它用于连接网络层之上执行不同协议的子网，组成异构型的因特网。

知识子域：计算机网络与网络设备

118. **同轴电缆显著的特征是频带较宽，其中高端的频带最大可达到（）。**

A. 3GHz

B. 5GHz

C. 10GHz

D. 15GHz

参考答案：C

难易程度：一级

解析：同轴电缆显著的特征是频带较宽，其中高端的频带最大可达到 10GHz。

知识子域：计算机网络与网络设备

119. **以下不属于交换机的物理分层方式的是（）。**

A. 接入层

B. 汇聚层

C. 核心层

D. 交换层

参考答案：D

难易程度：一级

解析：交换机的物理分层方式：接入层、汇聚层、核心层。

知识子域：计算机网络与网络设备

120. **传输线路是信息发送设备和接受设备之间的物理通路，不同传输介质具有不同的安全特性，以下属于网络传输介质的是（）。**

A. 同轴电缆

B. 双绞线

C. 光纤

D. 以上都是

参考答案：D

难易程度：一级

解析：常见的网络传输介质有：同轴电缆、双绞线、光纤、无线传输。

知识子域：计算网络与网络设备

121. **双绞线传输带宽也在逐步扩大，从最初的仅能用于语音传输的一类线发展到目前达到 10Gbps 带宽的七类线。最常用的以太网属于（）。**

A. 五类线

B. 超五类线

C. 六类线

D. 七类线

参考答案：A

难易程度：一级

解析：最常用的以太网电缆是五类线。

知识子域：计算机网络与网络设备

122. **以下不属于光纤的优点的是（）。**

A. 不易被窃听

B. 成本高、安装维护需要专业设备

C. 信号衰减小、无电磁干扰

D. 抗腐蚀材料、重量轻

参考答案：B

难易程度：一级

解析：光纤具有高带宽、信号衰减小、无电磁干扰、抗腐蚀材料、重量轻及不易被窃听等特点。

知识子域：计算机网络与网络设备

123. **以下不属于无线传输带来的不安全因素（）。**

A. 通信内容容易被窃听

B. 通信内容可以被更改

C. 通信线路被截断

D. 通信双方的身份肯被假冒

参考答案：C

难易程度：一级

解析：无线通信网络带来一些不安全因素，如通信内容容易被窃听、通信内容可以被更改和通信双方身份可能被假冒。

知识子域：计算机网络与网络设备

124. **以下属于网络安全设备的是（）。**

A. 防火墙

B. 交换机

C. 中继器

D. 路由器

参考答案：A

难易程度：一级

解析：防火墙属于网络安全设备。

知识子域：防火墙

125. **防火墙的部署位置可能在（）。**

A. 可信网络与不可信网络之间

B. 不同安全级别的网络之间

C. 两个需要隔离的区域之间

D. 以上都有可能

参考答案：D

难易程度：一级

解析：防火墙的部署位置：可信网络与不可信网络之间；不同安全级别的网络之间；两个需要隔离的区域之间。

知识子域：防火墙

126. 以下不属于防火墙的作用的是（）。

A. 隔离两个不同安全要求的网络。

B. 根据定义的控制策略，检查并控制这个两个安全域之间所有流量。

C. 进出网络边界的数据进行保护，防止恶意入侵、恶意代码的传播等。

D. 保障外部网络数据的安全。

参考答案：D

难易程度：一级

解析：防火墙保障的内部网络数据的安全。

知识子域：防火墙

127. 以下属于防火墙的典型技术的是（）。

A. 静态包过滤

B. 代理防火墙与 NAT

C. 状态检测技术

D. 以上都是

参考答案：D

难易程度：一级

解析：防火墙的典型技术有：静态包过滤、代理防火墙与 NAT、状态检测技术。

知识子域：防火墙

128. 包过滤技术是防火墙最常用的技术。以下不属于包过滤技术的优点的是（）。

A. 安全性较差，不提供用户认证功能。

B. 逻辑简单，功能容易实现，设备价格便宜。

C. 处理速度快，在处理速度上具有一定的优势，处理速度很快，对网络性能影响也较小。

D. 过滤规则与应用层无关，无须修改主机上的应用程序，易于安装和使用。

参考答案：A

难易程度：一级

解析：A 选项是静态包过滤的缺点。

知识子域：防火墙

129. 网络地址转换(NAT)作用是将内部的私有 IP 地址转换成可以在公网使用的公网 IP。NAT 的英文全称是（）。

A. Network Address Translation

B. Network Address Traversal

C. Network Address Port Translation

D. Network Address Port Traversal

参考答案：A

难易程度：一级

解析：网络地址转换协议（NAT，Network Address Translation）

知识子域：防火墙

130. 信息时代的海量数据，促进了大数据的形成和发展，其中大数据应用的核心资源是（）。

A. 人

B. 隐私

C. 数据

D. 互联网

参考答案：C

难易程度：一级

解析：大数据的核心是数据

知识子域：新技术领域

131. 物联网是把任何物品与互联网连接起来进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络，以下说法错误的是（）。

A. 物联网就是移动互联网

B. 智能家电属于物联网设备

C. 物联网的英文缩写是 IoT

D. 智能摄像头属于物联网终端

参考答案：A

难易程度：一级

解析：物联网(IoT)是把任何物品与互联网连接起来进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络，核心和基础仍然是互联网，是将互联网延伸和扩展到任意的物品之间。

知识子域：新技术领域

132. 以下哪个不是防火墙的基础作用（）。

A. 隔离

B. 控制

C. 杀毒

D. 记录

参考答案：C

难易程度：一级

解析：防火墙的基本作用：控制、隔离、记录。

知识子域：防火墙

133. 防火墙的策略有（）。

A. 接受：允许通过。

B. 拒绝：拒绝信息通过，通知发送信息的信息源。

C. 丢弃：直接丢弃信息，不通知信息源。

D. 以上都是。

参考答案：D

难易程度：一级

解析：防火墙的策略有：接受、拒绝、丢弃

知识子域：防火墙

134. 随着网络安全问题的日益凸显，安全设备也呈现多样化趋势，以下不属于网络安全设备的是（）。

A. 路由器

B. 防火墙

C. 入侵检测系统

D. 网闸

参考答案：A

难易程度：一级

解析：路由器不是网络安全设备。

知识子域：边界安全防护设备

135. 防火墙在网络安全防护中发挥着重要的作用，在选购防火墙时参考标准包括（）。

A. 总成本

B. 稳定性

C. 可升级性

D. 以上都是

参考答案：D

难易程度：一级

解析：选购防火墙时参考标准有总成本、稳定性、可升级性等。

知识子域：防火墙

136. 正确的选择防火墙能够更加有效的防护网络安全，在选择防火墙类型时基本原则包括（）。

A. 大企业根据部署位置选择防火墙

B. 中小企业根据网络规模选择防火墙

C. 考查厂商的服务

D. 以上都是

参考答案：D

难易程度：一级

解析：选择防火墙类型时基本原则有大企业根据部署位置选择防火墙；中小企业根据网络规模选择防火墙；考查厂商的服务。

知识子域：防火墙

137. 随着网络环境的日益复杂，防火墙也在不断发展，以下对防火墙发展趋势的描述不正确的是（）。

A. 安全需求降低

B. 模式转变

C. 功能扩展

D. 性能提高

参考答案：A

难易程度：一级

解析：防火墙发展趋势对安全需求越高。

知识子域：防火墙

138. 防火墙的种类较多，可以从多个角度对其进行分类，按照防火墙放置的位置不同可以分为（）和（）。

A. 软件防火墙　硬件防火墙

B. 个人防火墙　区域防火墙

C. 个人防火墙　企业防火墙

D. 区域防火墙　内部防火墙

参考答案：C

难易程度：一级

解析：防火墙的种类较多，可以从多个角度对其进行分类，按照防火墙放置的位置不同可以分为个人防火墙和企业防火墙。

知识子域：防火墙

139. 防火墙的种类较多，可以从多个角度对其进行分类，按照防火墙实现的载体不同可以分为（）和（）。

A. 软件防火墙 硬件防火墙

B. 软件防火墙 区域防火墙

C. 硬件防火墙 企业防火墙

D. 区域防火墙 内部防火墙

参考答案：A

难易程度：一级

解析：防火墙的种类较多，可以从多个角度对其进行分类，按照防火墙实现的载体不同可以分为软件防火墙和硬件防火墙。

知识子域：防火墙

140. 以下关于防火墙和网闸的说法错误的是（）。

A. 防火墙是实现物理隔离的。

B. 网闸是是实现物理隔离或协议隔离。

C. 通过防火墙进行数据交换，会话双方是实时连接的。

D. 通过网闸进行数据交换，会话双方是非实时连接的。

参考答案：A

难易程度：一级

解析：防火墙是实现逻辑隔离的。

知识子域：边界安全防护设备

141. 以下不属于网闸的局限性的是（）。

A. 非实时连接

B. 实时连接

C. 需要专有硬件

D. 对应用的支持有限

参考答案：B

难易程度：一级

解析：网闸是非实时连接的。

知识子域：边界安全防护设备

142. 下列哪个适合安装统一威胁管理系统（）。

A. 不计预算，需要较强防护能力的大型组织机构

B. 预算有限，且需要较全面防护能力的中小型组织机构

C. 不计预算，需要较强的防护能力的中小型组织机构

D. 预算有限，需要简单防护的个人设备

参考答案：B

难易程度：一级

解析：统一威胁管理系统（UTM）适合预算有限，但需要较全面防护能力的中小型组织机构。

知识子域：网络边界防护设备

143. 以下哪项属于入侵防御系统的入侵防护技术（）。

A. 恶意站点检测

B. Web 分类过滤

C. 专业抗 DDoS

D. 以上都是

参考答案：D

难易程度：一级

解析：入侵防御系统的入侵防护技术有：恶意站点检测、web 分类过滤、专业抗 DDoS 等。

知识子域：网络边界防护设备

144. 防火墙是一个位于内外网之间的网络安全系统，以下对防火墙作用的描述不正确的是（）。

A. 抵抗外部攻击

B. 阻止所有访问

C. 保护内部网络

D. 防止恶意访问

参考答案：B

难易程度：一级

解析：防火墙用来抵抗外部攻击、保护内部网络、防止恶意访问。

知识子域：防火墙

145. 防火墙是一种位于内部网络与外部网络之间的网络安全系统。以下不属于防火墙作用的是（）。

A. 限制内部用户访问特殊站点

B. 隔离不同信任级别网络

C. 保护内部网络

D. 数据备份

答案：D

难易程度：一级

解析：防火墙不能进行数据备份。

知识子域：防火墙

146. 对于主机入侵检测系统，下列说法正确的是（）。

A. 不能用于加密网络环境

B. 能够监视所有系统

C. 可移植性好

D. 开发、测试的压力都比较小

参考答案：B

难易程度：一级

解析：主机入侵检测系统能供用于加密网络环境，可移植性差，开发、测试的压力都比较大。

知识子域：网络安全管理设备

147. 虚拟专用网络(VPN)是在公用网络上建立虚拟的专用网络的技术。VPN 的优势有()。

A. 较低的成本

B. 具有较高的安全性

C. 服务保证

D. 以上都是

参考答案：D

难易程度：一级

解析：VPN 技术的主要优势是：较低的成本、具有较高的安全性、服务保证。

知识子域：网络安全管理设备

148. 安全管理平台(SOC)也被称为安全运营中心，为组织机构提供()的安全信息管理。

A. 集中

B. 统一

C. 可视化

D. 以上都是

参考答案：D

难易程度：一级

解析：安全管理平台(SOC)也被成为安全运营中心，为组织机构提供集中、统一、可视化的安全信息管理。

知识子域：网络安全管理设备

149. 开发较为完善的安全管理平台的功能包括（）。

A. 统一日志管理、统一配置管理

B. 安全状态的统一管控

C. 各安全产品和系统的统一协调和处理

D. 以上都是

参考答案：D

难易程度：一级

解析：开发较为完善的 SOC 平台应包含以下功能：1)统一日志管理(集中监控)、2)统一配置管理(集中管理)、3)各安全产品和系统的统一协调和处理(协同处理)、4)安全状态的统一管控(统一安服)、5)其他功能。

知识子域：网络安全管理设备

150. 二十世纪二十年代，德国发明家亚瑟谢尔比乌斯 Enigma 密码机。按照密码学发展历史阶段划分，这个阶段属于（）。

A. 古典密码学阶段

B. 近代密码学发展阶段

C. 现代密码学发展阶段

D. 当代密码学发展阶段

参考答案：A

难易程度：一级

解析：Enigma 密码机，按照密码学发展历史阶段划分，这个阶段属于古典密码阶段。

知识子域：密码学基础

151. 在入侵检测系统（IDS）的运行中，最常见的问题是（）。

A. 误报检测

B. 拒绝服务攻击

C. 错误拒绝率高

D. 分布式拒绝服务攻击

参考答案：A

难易程度：一级

解析：在入侵检测系统（IDS）的运行中，最常见的问题是误报检测。

知识子域：计算机网络与网络设备

152. 服务对外开放时需要对应到端口，其中 21 端口号对应以下哪个服务（）。

A. SSH

B. POP3

C. FTP

D. 以上都不是

参考答案：C

难易程度：一级

解析：FTP 默认端口号 21。

知识子域：网络安全协议

153. 从信息系统安全角度处理信息安全问题，设备安全已然成为人们关注的重点，以下属于设备安全的要求的是（）。

A. 稳定性

B. 可靠性

C. 可用性

D. 以上都是

参考答案：D

难易程度：一级

解析：对设备安全的要求包括稳定性、可靠性、可用性等。

知识子域：计算机网络与网络设备

154. DNS 即网域名称系统，它将域名和 IP 地址一一映射。DNS 服务对应的网络端口号是（）。

A. 21

B. 53

C. 69

D. 52

参考答案：B

难易程度：一级

解析：DNS 服务对应的端口号为 53。

知识子域：网络安全协议

155. OSI 七层模型中位于最顶层并向应用程序提供服务的是（）。

A. 网络层

B. 应用层

C. 表示层

D. 会话层

参考答案：B

难易程度：一级

解析：OSI 七层模型中位于最顶层并向应用程序提供服务的是应用层。

知识子域：网络安全协议

156. 很多互联网应用重要操作时都需要给手机发一个带验证码的短信，关于短信验证，以下说法哪个是正确的（）。

A. 手机号具有唯一性，因此可被用于做身份验证依据。

B. 互联网应用必须通过手机短信才能进行验证。

C. 手机短信具有极高的安全性，所以被用于身份验证。

D. 以上都对

参考答案：A

难易程度：一级

解析：手机号具有唯一性，因此可被用于做身份验证依据。

知识子域：身份鉴别与访问控制

157. 按网络的作用范围可将计算机网络分为广域网、城域网、局域网，下列说法不正确的是（）。

A. Internet 是目前最大的广域网。

B. 城域网的一个重要用途是用作骨干网。

C. 城域网通常跨接很大的物理范围，能连接多个城市、国家。

D. 在计算机网络和工业业务发展初期，各企业管理信息系统和访问信息系统的用户基本都处在局域网内。

参考答案：C

难易程度：一级

解析：城域网的作用范围达不到国家。

知识子域：计算机网络与网络设备

158. 在 VPN 方面，目前企业采用的保障业务安全的解决方案不包括（）。

A. 统一安全接入平台

B. 系统支持多种认证方式

C. 不使用任何防火墙和杀毒引擎

D. 统一派发设备，强管控

参考答案：C

难易程度：一级

解析：应当开启防火墙和杀毒引擎

知识子域：网络安全管理设备

159. 消息认证码 MAC 是消息内容和秘密钥的公开函数，其英文全称是（）。

A. Message Authentication Code

B. Messag Authentication Code

C. Message Authentication Date

D. Messag Authentication Code

参考答案：A

难易程度：一级

解析：消息认证码 MAC 英文名称是 Message Authentication Code。

知识子域：密码学基础

160. 安全设备是指企业在生产经营活动中，将危险、有害因素控制在安全范围内，以及减少、预防和消除危害所配备的装置和采取的设备，以下哪个选项不属于安全设备()。

A. 防火墙

B. VPN

C. IDS

D. 集线器

参考答案：D

难易程度：一级

解析：集线器不属于安全设备

知识子域：网络边界防护设备

161. 计算机互联的主要目的是（）。

A. 集中计算

B. 资源共享

C. 制定网络协议

D. 将计算机技术与 ton 更新技术相结合

参考答案：B

难易程度：一级

解析：计算机互联的主要目的是资源共享。

知识子域：计算机网络与网络设备

162. INTERNET 最初创建的目的是用于（）。

A. 政治

B. 经济

C. 军事

D. 教育

参考答案：C

难易程度：一级

解析：INTERNET 最初创建的目的是用于军事。

知识子域：计算机网络与网络设备

163. 在局域网中，MAC 指的是（）。

A. 物理层

B. 数据链路层

C. 介质访问控制子层

D. 逻辑访问控制子层

参考答案：C

难易程度：一级

解析：在局域网中，MAC 指的是介质访问控制子层。

知识子域：计算机网络与网络设备

164. 在以下四种传输介质中，带宽最宽、抗干扰能力最强的是（）。

A. 无线信道

B. 同轴电缆

C. 双绞线

D. 光纤

参考答案：D

难易程度：一级

解析：在这个四种传输介质中，带宽最宽、抗干扰能力最强的是光纤。

知识子域：计算机网络与网络设备

165. IP 协议是无连接的，其信息传输方式是（）。

A. 广播

B. 虚电路

C. 数据报

D. 多播

参考答案：C

难易程度：一级

解析：IP 协议是无连接的，其信息传输方式是数据报。

知识子域：网络安全协议

166. 路由选择协议为路由器提供网络最佳路径所需要的相互共享的路由信息。路由选择协议位于（）。

A. 物理层
B. 数据链路层
C. 网络层
D. 传输层
参考答案：C
难易程度：一级
解析：路由选择协议为路由器提供网络最佳路径所需要的相互共享的路由信息。路由选择协议位于网络层。
知识子域：网络安全协议

167. 世界上第一个计算机网络是（）。

A. ARPANET
B. INTERNET
C. CHINANET
D. CERNET
参考答案：A
难易程度：一级
解析：世界上第一个计算机网络是 ARPANET。
知识子域：计算机网络与网络设备

168. 广域网也称远程网，通常跨接很大的物理范围，所覆盖的范围从几十公里到几千公里。以下选项中，属于广域网的是（）。

A. 宿舍网
B. 校园网
C. 公司网
D. 国家网
参考答案：D
难易程度：一级
解析：国家网属于广域网。
知识子域：计算机网络与网络设备

169. 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
参考答案：C
难易程度：一级
解析：柯克霍夫原则：密码系统的安全性依赖于密钥而不依赖于算法。
知识子域：密码学基础

170. PKI 的主要理论基础是（）。

A. 摘要算法
B. 对称密码算法
C. 量子算法
D. 公钥密码算法
参考答案：D
难易程度：一级

解析：PKI（公钥基础设施），也称公开密钥基础设施。

知识子域：密码学基础

171. **一个信息管理系统通常会对用户进行分组并实施访问控制。下列选项中，对访问控制的作用的理解错误的是（）。**

A. 对经过身份鉴别后的合法用户提供所有服务

B. 在用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理

C. 拒绝非法用户的非授权访问请求

D. 防止对信息的非授权篡改和滥用

参考答案：A

难易程度：一级

解析：访问控制的核心：允许合法用户的授权访问，防止非法用户的访问和合法用户的越权访问。

知识子域：身份鉴别与访问控制

172. **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. IPSec

B. PP2P

C. L2TP

D. SSL

参考答案：D

难易程度：一级

解析：IPSec 工作在网络层，PP2P 和 L2TP 工作在数据链路层，SSL 工作在传输层。

知识子域：网络安全协议

173. **在 ISO 的 OSI 安全体系结构中，以下哪一个安全机制可以提供抗抵赖安全服务()。**

A. 加密信息

B. 数字签名

C. 访问控制

D. 路由控制

参考答案：B

难易程度：一级

解析：数字签名可以提供抗抵赖、鉴别和完整性。

知识子域：身份鉴别与访问控制

174. **关于密钥管理，下列说法错误的是（）。**

A. 密钥管理需要考虑密钥生命周期过程的每一个环节。

B. 在网络通信中，通信双方可利用 Diffie-Hellman 协议协商出会话密钥。

C. 保密通信过程，通信使用之前用过的会话密钥建立会话，不影响通信安全。

D. 科克霍夫原则指出算法的安全性不应基于算法的保密，而应基于密钥的安全性。

参考答案：C

难易程度：一级

解析：会话密钥不应重复使用，如果使用用过的会影响通信安全。

知识子域：密码学基础

175. **数字签名不能实现的安全特性为（）。**

A. 保密通信

B. 防抵赖
C. 防伪造
D. 防冒充
参考答案：A
难易程度：一级
解析：数字签名的作用不在于保密通信。
知识子域：密码学基础

176. 甲公司打算制作网络连续时所需要的插件的规格尺寸、引脚数量和线序情况，甲公司将这个任务委托了乙公司，那么乙公司的设计员应该了解 OSI 参考模型中的哪一层（）。

A. 数据链路层
B. 物理层
C. 网络层
D. 传输层
参考答案：B
难易程度：一级
解析：物理层规定通信设备的机械的、电气的、功能的和过程的特性，用以建立、维护和拆除物理链路连接，这些特性包括网络连接时所需接插件的规格尺寸、引脚数量等。
知识子域：网络安全协议

177. 以下哪个场景属于身份鉴别过程（）。

A. 用户依照提示输入用户名、口令和短信验证码，成功登录该应用。
B. 用户在网络上共享了的一份加密的 pdf 文档，以阻止其他人下载查看文档中的内容。
C. 用户给自己编写的文档加上水印。
D. 用户在网上下载了一份带水印的文档，去掉了水印。
参考答案：A
难易程度：一级
解析：A 选项属于身份鉴别的过程。
知识子域：身份鉴别与访问控制

178. 一个密码系统至少由明文、密文、加密算法、解密算法和密钥 5 部分组成，而其安全性是由下列哪个选项决定的（）。

A. 加密算法
B. 解密算法
C. 密钥
D. 加密算法和解密算法
参考答案：C
难易程度：一级
解析：系统的保密性不依赖于加密体制和算法的保密，而依赖于密钥。
知识子域：密码学算法

179. 在某信息系统的设计中，用户登录过程是这样的：（1）用户通过 HTTP 协议访问信息系统；（2）用户在登录页面输入用户名和口令；（3）信息系统在服务器端检查用户名和密码的正确性，如果正确，则鉴别完成。可以看出，这个鉴别过程属于（）。

A. 单向鉴别
B. 双向鉴别
C. 第三方鉴别

D. 三向鉴别

参考答案：A

难易程度：一级

解析：根据题意属于单向鉴别

知识子域：身份鉴别与访问控制

180. 小刘是某公司新入职的员工，公司要求他注册一个公司网站的账号，小刘使用一个安全一点的密码，请问以下选项中哪个密码是最安全（）。

A. 与用户名相同的密码

B. 自己的姓名和出生日期

C. 一个单词

D. 数字、字母和特殊符号混合且自己容易记住

参考答案：D

难易程度：一级

解析：D 选项更安全。

知识子域：身份鉴别与访问控制

181. 强制访问控制模型有多种类型，如 BLP、Biba、Clark-willson 和 ChineseWall 等。小明学习了 BLP 模型，并对该模型的特点进行了总结。以下对 BLP 模型的描述中，正确的是（）。

A. BLP 模型用于保证系统信息的完整性

B. BLP 的自主安全策略中，系统通过比较主体与客体的访问类属性控制主体对客体的访问

C. BLP 模型的规则是“向下读，向上写”

D. BLP 的强制安全策略使用一个访问控制矩阵表示

参考答案：C

难易程度：一级

解析：BLP 模型是一种强制访问控制模型用以保障机密性，向上写，向下读，自主访问控制模型使用一个访问控制矩阵表示。

知识子域：身份鉴别与访问控制

182. 信息发送者使用（）进行数字签名。

A. 自己的私钥

B. 自己的公钥

C. 对方的私钥

D. 对方的公钥

参考答案：A

难易程度：一级

解析：信息发送者使用自己的私钥进行数字签名。

知识子域：密码学基础

183. 常见密码系统包含的元素有（）。

A. 明文、密文、信道、加密算法、解密算法

B. 明文、摘要、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

D. 消息、密文、信道、加密算法、解密算法

参考答案：C

难易程度：一级

解析：常见密码系统包含的元素有明文、密文、密钥、加密算法、解密算法。

知识子域：密码学基础

184. **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. 外网——内网主机——防火墙——交换机

B. 外网——交换机——内网主机——防火墙

C. 外网——内网主机——交换机——防火墙

D. 外网——防火墙——交换机——内网主机

参考答案：D

难易程度：一级

解析：防火墙一般部署在内网和外网边界。

知识子域：防火墙

185. **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，不能逻辑隔离

C. 不能物理隔离，能逻辑隔离

D. 不能物理隔离，也不能逻辑隔离

参考答案：C

难易程度：一级

解析：防火墙能实现逻辑隔离，不能物理隔离。

知识子域：防火墙

186. **“统一威胁管理”是将防病毒，入侵检测和防火墙等安全需求统一管理，目前市场上已经出现了多种此类安全设备，这里“统一威胁管理”常常被简称为（）。**

A. FW

B. UTM

C. IDS

D. SOC

参考答案：B

难易程度：一级

解析：统一威胁管理系统（UTM）

知识子域：网络边界防护设备

187. **为防范网络欺诈确保交易安全，网银系统首先要求用户安全登录，然后使用“智能卡+短信认证”模式进行网上转账等交易，在此场景中用到下列哪些鉴别方法（）。**

A. 实体所知和实体所有的鉴别方法

B. 实体所有和实体特征的鉴别方法

C. 实体所知和实体特征的鉴别方法

D. 实体所知和实体行为的鉴别方法

参考答案：A

难易程度：一级

解析：题目中安全登录会涉及到账号密码为实体所知，智能卡和短信是实体所有。

知识子域：身份鉴别与访问控制

188. **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。小红作为合法用户通过指纹验证，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. 实体所感的鉴别方法

D. 实体特征的鉴别方法

参考答案：D

难易程度：一级

解析：指纹属于实体特征

知识子域：身份鉴别与访问控制

189. **小蓝通过账号，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

B. 由可信第三方完成的用户身份鉴别

C. 个人网银系统对用户身份的单向鉴别

D. 用户对个人网银系统合法性的单向鉴别

参考答案：C

难易程度：一级

解析：小蓝通过账号，密码和验证码成功登陆某银行的个人网银系统，属于个人网银系统对用户身份的单向鉴别。

知识子域：身份鉴别与访问控制

190. **小蓝用的小绿的密钥加密明文，将密文发送给小绿。小绿再用自己的私钥解密，恢复出明文。以下说法正确的是（）。**

A. 采用了对称密码体制

B. 采用了公钥密码体制

C. 采用了复合密码体制

D. 采用了单钥密码体制

参考答案：B

难易程度：一级

解析：题干中采取了公钥加密私钥解密的公钥密码体制。

知识子域：密码学基础

191. **以下哪种方法属于实体所有的鉴别方法（）。**

A. 用户通过自己设置的口令登录系统，完成身份鉴别

B. 用户使用个人指纹，通过指纹识别系统的身份鉴别

C. 用户利用和系统协商的秘密函数，对系统发送挑战进行正确应答，通过身份鉴别

D. 用户使用智能卡完成身份鉴别

参考答案：D

难易程度：一级

解析：智能卡属于实体所有。

知识子域：身份鉴别与访问控制

192. **某公司已有漏洞扫描和入侵检测系统(Intrusion Detection System，IDS)产品，需要购买防火墙，以下做法应当优先考虑的是（）。**

A. 任选一款防火墙

B. 选购一款当前最先进的防火墙

C. 选购一款便宜的防火墙

D. 选购一款同已有的安全产品设备联动的防火墙

参考答案：D

难易程度：一级

解析：在技术条件允许情况下，可以实现 IDS 和 FW 的联动。

知识子域：防火墙

193. **在 OSI 参考模型中有 7 个层次，提供了相应的安全服务来加强信息系统的安全性，以下哪一层提供了保密性、身份鉴别、数据完整性服务（）。**

A. 物理层

B. 表示层

C. 网络层

D. 传输层

参考答案：C

难易程度：一级

解析：网络层和应用层可以提供保密性、身份鉴别、完整性、抗抵赖、访问控制服务。

知识子域：网络安全协议

194. **一份文件通过哈希函数得到消息摘要，不能通过消息摘要得到原文件，这体现了哈希函数的（）。**

A. 机密性

B. 单向性

C. 弱抗碰撞性

D. 强抗碰撞性

参考答案：B

难易程度：一级

解析：题干体现了哈希函数的单向性。

知识子域：密码学基础

195. **两份包含不同内容的文件通过哈希函数得到相同的散列值，这违背了哈希函数的（）。**

A. 单向性

B. 机密性

C. 弱抗碰撞性

D. 强抗碰撞性

参考答案：D

难易程度：一级

解析：本题违背了哈希函数的强抗碰撞性。

知识子域：密码学基础

196. **以下不属于评估密码系统安全性的方法是（）**

A. 实际安全性。对于实际应用中的密码系统而言，不存在破译方法。

B. 无条件安全性：这种评价方法考虑的是假定攻击者拥有无限的计算资源，但仍然无法破译该密码系统。

C. 计算安全性：这种方法是指如果使用目前最好的方法攻破它所需要的计算资源远远超出攻击者拥有的计算资源，则可以认为这个密码系统是安全的。

D. 可证明安全性：这种方法是将密码系统的安全性归结为某个经过深入研究的困难问题(如大整数素因子分解、计算离散对数等)。这种评估方法存在的问题是它只说明了这个密码方法的安全性与某个困难问题相关，没有完全证明问题本身的安全性，

并给出它们的等价性证明。

参考答案：A

难易程度：二级

解析：评估密码系统安全性主要有三种方法：无条件安全性、计算安全性、可证明安全性。

知识子域：密码学基础

197. 关于对称加密和非对称加密，下列说法正确的是（）

A. 非对称加密体系要求通信双方事先传递密钥才能完成保密通信，并且密钥管理方便，可实现防止假冒和抵赖

B. 非对称加密指加密和解密使用不同密钥的加密算法，也称为公私钥加密。

C. 对称加密算法比非对称加密算法快，在保护通信安全方面，对称加密算法具有非对称密码难以企及的优势。

D. 非对称加密算法的特点是计算量小、加密速度快、加密效率高。

参考答案：B

难易程度：二级

解析：A.非对称加密体系不要求通信双方事先传递密钥。C.在保护通信安全方面，非对称加密算法却具有对称密码难以企及的优势。D.对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。

知识子域：密码学基础

198. 小明刷脸进入小区大门，通过输入密码进入楼门，用钥匙打开家门回到自己的家里。在以上过程中使用了哪种或哪几种身份鉴别的方式（）

A. 实体所知　实体所有　实体所感

B. 实体所有　实体特征

C. 实体所知　实体特征

D. 实体所知　实体所有　实体特征

参考答案：D

难易程度：二级

解析：刷脸属于实体特征、输入密码属于实体所知、使用钥匙属于实体所有。

知识子域：身份鉴别与访问控制

199. 强制访问控制(MAC)是主体和客体都有一个固定的安全属性，系统通过比较客体和主体的安全属性，根据已经确定的访问控制规则限制来决定主体是否可访问客体。关于强制访问控制模型，下面说法错误的是（）

A. 强制访问控制规则强制执行的，系统中的主体和客体均无权更改。

B. 强制访问控制比自主访问控制具有更高的安全性，不能有效防范特洛伊木马。

C. 强制访问控制可以防止在用户无意或不负责任的操作时泄露机密信息，适用于专用或安全性要求较高的系统。

D. 强制访问控制在用户共享数据方面不灵活。

参考答案：B

难易程度：二级

解析：强制访问控制比自主访问控制具有更高的安全性，能有效防范特洛伊木马。

知识子域：身份鉴别和访问控制

200. 关于 OSI 七层模型来说，下列哪个不是分层结构的优点（）

A. 各层之间相互独立

B. 增加复杂性

C. 促进标准化工作

D. 协议开发模块化

参考答案：B

难易程度：二级

解析：分层结构的特点：各层之间相互独立；降低复杂性；促进标准化工作；协议开发模块化。

知识子域：网络安全协议

201. 在实体特征的鉴别中，对于鉴别系统的有效性判断，下列说法正确的是（）

A. 错误拒绝率（FRR）越高，系统判断更准确。

B. 错误接受率（FAR）越高，系统判断更准确。

C. 交叉错判率（CER）越低，系统判断更准确。

D. 交叉错判率（CER）越高，系统判断更准确。

参考答案：C

难易程度：二级

解析交叉错误率越低，证明该鉴别系统更准确，也就是质量更高

知识子域：身份鉴别与访问控制

202. 访问控制为用户对系统资源提供最大限度共享的基础上，对用户的访问权限进行管理，防止对信息的非授权篡改和滥用，以下不属于访问控制的作用的是（）

A. 保证用户在系统的安全策略下正常工作

B. 拒绝非法用户的非授权访问

C. 拒绝合法用户的越权访问

D. 拒绝合法用户的正常访问

参考答案：D

难易程度：二级

解析：访问控制的作用：保证用户在系统的安全策略下正常工作；拒绝非法用户的非授权访问；拒绝合法用户的越权访问

知识子域：身份鉴别与访问控制

203. 关于强制访问控制模型中的 BLP 模型，以下说法正确的是（）

A. BLP 模型是最早的一种安全模型，也是最有名的多级安全策略模型

B. BLP 模型是一个严格形式化的模型，并给出了形式化的证明

C. 既有自主访问控制，又有强制访问控制

D. 以上都是

参考答案：D

难易程度：二级

解析：参考 BLP 模型概念和访问控制策略。

知识子域：身份鉴别和访问控制

204. 关于 BLP 模型和 Biba 模型，下列说法正确的是（）

A. BLP 模型的安全策略是向上读，向下写

B. BLP 模型的安全策略是向上写，向下读

C. Biba 模型的安全策略是向上写，向下读

D. Biba 模型的安全策略是向上读，向下读

参考答案：B

难易程度：二级

解析：BLP 模型的安全策略是向上写，向下读；Biba 模型的安全策略是向上读，向下写。

知识子域：身份鉴别与访问控制

205.　在 OSI 七层模型中，物理层的传输单位是（）

A.　段

B.　分组

C.　报文

D.　比特流

参考答案：D

难易程度：二级

解析：物理层的传输单位是比特流。

知识子域：网络安全协议

206.　在 OSI 七层模型中，数据链路层的传输单位是（）

A.　帧

B.　比特流

C.　分组

D.　段

参考答案：A

难易程度：二级

解析：数据链路层的传输单位是帧。

知识子域：网络安全协议

207.　使用两种鉴别方式的组合(双因素鉴别)是常用的多因素鉴别形式。用户在使用支付宝进行刷脸买东西的时候使用了那几种身份鉴别的方式（）

A.　实体所知　实体所有

B.　实体所有　实体特征

C.　实体所知　实体特征

D.　实体所知　实体所有　实体特征

参考答案：C

难易程度：二级

解析：登录支付宝账号（实体所知），刷脸识别（实体特征）。

知识子域：身份鉴别与访问控制

208.　多因素鉴别方法，使用多种鉴别机制检查用户身份的真实性。用户在登录微信是除了用户名/密码，还需要手机短信验证，使用了哪几种身份鉴别的方式（）

A.　实体所知　实体所有

B.　实体所知　实体特征

C.　实体所有　实体特征

D.　实体所知　实体所有　实体特征

参考答案：A

难易程度：二级

解析：用户名/密码（实体所知），手机短信验证（实体所有）

知识子域：身份鉴别与访问控制

209.　存在大量应用系统使用 MD5 对口令明文进行处理成密码散列，攻击者虽然无法从密码散列中还原出口令明文，但由于口令的明文和散列可以视同一一对应的，攻击者可以构造出一张对照表，因此只要获得密码散列，就能根据对照表知道对应的口令明文，这样的对照表通常称为（）

A.　彩虹表

B. 哈希表

C. 密码散列表

D. SHA-1 表

参考答案：A

难易程度：二级

解析：存在大量应用系统使用 MD5 对口令明文进行处理成密码散列，攻击者虽然无法从密码散列中还原出口令明文，但由于口令的明文和散列可以视同一一对应的，攻击者可以构造出一张对照表，因此只要获得密码散列，就能根据对照表知道对应的口令明文，这样的对照表通常称为彩虹表。

知识领域：身份鉴别与访问控制

210. 以下哪个是关于云计算主要的特征中“按需自助服务”的描述（）

A. 客户通过标准接入机制,利用计算机、移动电话、平板等各种终端通过网络随时随地使用服务。

B. 云服务商将资源(如:计算资源、存储资源、网络资源等)提供给多个客户使用,这些物理的、虚拟的资源根据客户的需求进行动态分配或重新分配

C. 云计算可按照多种计量方式(如按次付费或充值使用等)自动控制或量化资源,计量的对象可以是存储空间、计算能力、网络带宽或账户数等

D. 在不需或较少云服务商的人员参与情况下,客户能根据需要获得所需计算资源,如自主确定资源占用时间和数量等

参考答案：D

难易程度：二级

解析：按需自助服务：在不需或较少云服务商的人员参与情况下,客户能根据需要获得所需计算资源,如自主确定资源占用时间和数量等

知识子域：新技术领域

211. 关于大数据生命周期中的“数据处理阶段”存在哪些安全问题（）

A. 存储架构安全、逻辑存储安全、存储访问安全、数据副本安全、数据归档安全等

B. 数据分布式处理安全、数据分析安全、数据加密处理、数据脱敏处理以及数据溯源等

C. 数据传输安全、数据访问控制、数据脱敏处理等

D. 数据源鉴别及记录、数据合法收集、数据标准化管理、数据管理职责定义、数据分类分级以及数据留存合规性识别等问题

参考答案：B

难易程度：二级

解析：数据处理阶段：数据分布式处理安全、数据分析安全、数据加密处理、数据脱敏处理以及数据溯源等

知识子域：新技术领域

212. 感知层属于物联网的最底层，下列哪个不属于感知层的技术（）

A. 实时定位

B. 二维码

C. 分布式计算

D. 短距离无线通信

参考答案：C

难易程度：二级

解析：分布式计算属于支撑层

知识领域：新技术领域

213. 我们经常使用 Ping 命令检查网络通不通，Ping 命令属于（）协议，位于 TCP/IP 协议的（）。

A. ICMP 传输层

B. IGMP 网络层

C. ICMP 网络层

D. IGMP 应用层

参考答案：C

难易程度：二级

解析：Ping 命令属于 ICMP 协议，位于 TCP/IP 协议的网络层。

知识领域：网络安全协议

214. 以下关于大数据的特征说法不正确的是（）

A. 大量（Volume）：非结构化数据的超大规模和增长，总数据量的 80%～90%。

B. 多样（Variety）：大数据的异构和多样性，很多不同形式（文本、图像、视频、机器数据等）。

C. 价值（Value）：大量的不想关信息，对未来趋势与模式的可预测分析，深度复杂分析（机器学习、人工智能）。

D. 高速（Velocity）：批量式分析，数据输入、处理与丢弃，事后见效。

参考答案：D

难易程度：二级

解析：高速（Velocity）：实时分析而非批量式分析，数据输入、处理与丢弃，立竿见影而非事后见效。

知识子域：新技术领域

215. 以下哪个属于移动互联网安全威胁（）

A. 业务层面：非法业务访问、违法数据访问、拒绝服务攻击、垃圾信息的泛滥、不良信息的传播、个人隐私和敏感信息的泄露、内容版权盗用和不合理的使用。

B. 网络层面：接入网非法窃听、用户身份仿冒、服务器滥用占用带宽、破坏数据和信息完整性、非授权定位等。

C. 终端层面：病毒、木马、蠕虫、网络钓鱼、身份伪冒、DDOS 攻击、窃取隐私、非授权使用资源、远程控制等。

D. 以上都是

参考答案：D

难易程度：二级

解析：互联网安全威胁包括业务层面、网络层面、终端层面。

知识子域：新技术领域

216. 下列哪个不属于工控网络的特点（）

A. 网络通讯协议不同，大量的工控系统采用私有协议

B. 对系统稳定性要求高，网络安全造成误报等同于攻击

C. 系统运行环境不同，工控系统运行环境相对先进

D. 更新代价高，无法像办公网络或互联网那样通过补丁来解决安全问题

参考答案：C

难易程度：二级

解析：系统运行环境不同，工控系统运行环境相对落后。

知识子域：新技术领域

217.　　以下属于工业控制系统网络威胁来源的是（）

A.　工业网络病毒

B.　无线技术应用风险

C.　工控设备高危漏洞

D.　以上都是

参考答案：D

难易程度：二级

解析：工业控制系统网络威胁来源有：高级持续性威胁、工业网络病毒、无线技术应用风险、工控设备高危漏洞、国外设备预留后门。

知识领域：新技术领域

218.　　以下不属于大数据面临的安全威胁的是（）。

A.　虚拟化 VMWare 漏洞攻击

B.　信息泄露或丢失

C.　大数据滥用、误用风险

D.　非授权访问、拒绝服务攻击

参考答案：A

难易程度：二级

解析：虚拟化 VMWare 漏洞攻击属于云计算所面临的安全威胁。

知识子域：新技术领域

219.　　我国国家标准（）对云计算定义为：云计算是指通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

A.　《信息安全技术 云计算服务安全指南》(GB/T 31167-2014)

B.　《信息安全技术 云计算服务安全》(GB 31167-2014)

C.　《云计算安全服务》(GB/T 31167-2014)

D.　《云计算信息安全服务》(GB 31167-2014)

参考答案：A

难易程度：二级

解析：我国国家标准《信息安全技术 云计算服务安全指南》(GB/T 31167-2014)中对云计算定义为：云计算是指通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式

知识子域：新技术领域

220.　　我国国家标准（）对于工业控制系统的定义是：工业控制系统(ICS)是一个通用术语,它包括多种工业生产中使用的控制系统,包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)和其他较小的控制系统,如可编程逻辑控制器(PLC)。

A.　GB 32919—2016 《信息安全技术 工业控制系统安全控制应用指南》

B.　GB/T 32919—2016 《工业控制系统安全控制应用》

C.　GB 32919—2016 《工业控制系统安全控制应用》

D.　GB/T 32919—2016 《信息安全技术 工业控制系统安全控制应用指南》

参考答案：D

难易程度：二级

解析：我国国家标准 GB/T32919—2016 《信息安全技术 工业控制系统安全控制应用指南》对于工业控制系统的定义是：工业控制系统(ICS)是一个通用术语,它包括多种工业生产中使用的控制系统,包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)和其他较小的控制系统,如可编程逻辑控制器(PLC)。

知识子域：新技术领域

221. 在 BLP 模型中，现有两个安全级为 A＝＜机密，｛外交，商务｝＞、B＝＜秘密，｛外交｝＞，AB 之间的支配关系为（）。

A. A 支配 B

B. B 支配 A

C. 没有支配关系

D. 以上都不正确

参考答案：A

难易程度：二级

解析：安全级之间的支配关系（密级高于或等于、范畴包含）。

知识子域：身份鉴别与访问控制

222. 云计算的主要服务形式有（）。

A. 软件即服务　平台即服务

B. 平台即服务　基础设施即服务

C. 软件即服务　基础设施即服务

D. 软件即服务　平台即服务　基础设施即服务

参考答案：D

难易程度：二级

解析：云计算的主要服务形式有：软件即服务、平台即服务、基础设施即服务。

知识子域：新技术领域

223. 下列关于同轴电缆的说法，错误的是（）。

A. 同轴电缆频带较宽。

B. 同轴电缆使用的总线拓扑结构。

C. 同轴电缆在一根电缆上连接多个设备，但是当其中一个地方发生故障时，会串联影响到线缆上的所有设备，可靠性存在不足。

D. 同轴电缆的故障的诊断和修复难度都较小。

参考答案：D

难易程度：二级

解析：同轴电缆的故障的诊断和修复难度都较大。

知识子域：计算机网络与网络设备

224. 下列关于双绞线的说法，错误的是（）。

A. 双绞线是由四对不同颜色的传输线所组成，是目前局域网使用最广泛的互联技术。

B. 双绞线相比光纤速率偏低，抗干扰能力较强

C. 双绞线性能可靠，成本低廉在网络通信中应用广泛。

D. 双绞线外包裹一次金属屏蔽器是为了减少辐射并阻止外部电磁干扰进入，使得传输更稳定可靠。

参考答案：B

难易程度：二级

解析：双绞线相比光纤速率偏低，抗干扰能力较差。

知识子域：计算机网络与网络设备

225. 关于光纤下列说法不正确的是（）

A. 光纤全名叫做光导纤维。

B. 光纤是以光信号传输的一种通信线路。

C. 光纤的材质是纯石英的玻璃圆柱体，它的质地坚固。

D. 进入光纤的光波在两种材料的解密上形成全反射，从而不断向前传播。

参考答案：B

难易程度：二级

解析：光纤的材质是纯石英的玻璃圆柱体，它的质地易碎。

知识子域：计算机网络与网络设备

226. 关于状态检测防火墙，下列说法正确的是（）。

A. 状态检测防火墙又称动态包过滤防火墙，是对传统包过滤的功能扩展。

B. 状态检测防火墙实质上也是包过滤，但它不仅对 IP 包头信息进行检查过滤，而且还要检查包的 TCP 头部信息甚至包的内容。

C. 状态检查防火墙不允许规则的动态变化。

D. 状态防火墙通过采用状态监视器，对网络通信的各层(包括网络层、传输层以及应用层)实施监测，抽取其中部分数据，形成网络连接的动态状态信息。

参考答案：C

难易程度：二级

解析：状态检测防火墙引入了动态规则的概念，允许规则的动态变化。

知识子域：防火墙

227. 状态检测防火墙对数据包的抽取包括（）。

A. 源地址、源端口号、目的地址、目的端口号、使用协议

B. 当前的会话状态、顺序号、应答标记、防火墙的执行动作

C. 最新报文的寿命

D. 以上都是

参考答案：D

难易程度：二级

解析：状态检测防火墙对数据包的数据抽取不仅仅包括数据包的源地址、源端口号、目的地址、目的端口号、使用协议等五元组，还包括会话当前的状态属性、顺序号、应答标记、防火墙的执行动作及最新报文的寿命等信息。

知识子域：防火墙

228. 以下哪个不是关于防火墙的企业部署方式（）

A. 单防火墙(无 DMZ)部署方式

B. 防火墙 Route-路由模式

C. 单防火墙(DMZ)部署方式

D. 双(多)防火墙部署方式

参考答案：B

难易程度：二级

解析:防火墙的企业部署方式有:单防火墙(无 DMZ)部署方式、单防火墙(DMZ)部署方式、双(多)防火墙部署方式。

知识子域：防火墙

229. EIA/TIA 的布线标准中规定了两种双绞线的线序 568A 和 568B。568B 的线序为()。

A. 橙白-橙、绿白-蓝、蓝白-绿、棕白-棕

B. 橙白-橙、绿白-绿、蓝白-蓝、棕白-棕

C. 绿白-绿、橙白-蓝、蓝白-橙、棕白-棕

D. 绿白-蓝、橙白-绿、蓝白-橙、棕白-棕

参考答案：A

难易程度：二级

解析：568B 线序：橙白-橙、绿白-蓝、蓝白-绿、棕白-棕

知识子域：计算机网络与网络设备

230. 对于入侵防御系统（IPS），下列说法正确（）。

A. 入侵防御系统(IPS)是结合了入侵检测、防火墙等基础机制的安全产品。

B. 入侵防御系统(IPS)精确度很高，不可能产生误报。

C. 入侵防御系统(IPS)通过对网络流量进行分析，检测入侵行为并产生响应以中断入侵，从而保护组织机构信息系统的安全。

D. 入侵防御系统(IPS)作为集检测、防御与一体的安全产品，对明确判断为攻击的行为，会采取措施进行阻断，无需人员介入。

参考答案：B

难易程度：二级

解析：入侵防御系统作为集检测、防御与一体的安全产品，对明确判断为攻击的行为，会采取措施进行阻断，无需人员介入，因此也可能由于误报导致将正常的用户行为进行拦截。

知识子域：边界安全防护设备

231. 网闸又叫物理隔离系统，由（）组成。

A. 外部处理单元、内部处理单元、缓存区处理单元

B. 外部处理单元、中心处理单元、隔离安全交换单元

C. 外部处理单元、内部处理单元、仲裁处理单元

D. 内部处理单元、冲裁处理单元、隔离安全交换单元

参考答案：C

难易程度：二级

解析：网闸又叫物理隔离网络，由外部处理单元、内部处理单元和仲裁处理单元组成。

知识子域：边界安全防护设备

232. 网络环境日益复杂，人们对安全防护技术的要求也在不断提高，以下关于防火墙技术的发展要求说法错误的是（）

A. 信息过滤的深度越来越浅

B. 安全协议的优化是必要的

C. 与操作系统相耦合越来越紧密

D. 由被动防护转变为智能、动态地保护内部网络

参考答案：A

难易程度：二级

解析：防火墙技术发展对信息过滤的深度越来越深。

知识子域：防火墙

233. 网络代理技术即通过代理服务器代理网络用户取得网络信息，在代理服务器上可对信息进行合法性验证，从而保护用户的安全。以下关于网络代理技术的说法错误的是（）。

A. 代理技术又称为应用层网关技术

B. 代理技术能完全代替防火墙功能

C. 代理技术具备一定的安全防御机制

D. 代理服务器能够管理网络信息

参考答案：B

难易程度：二级

解析：代理技术不能完全代替防火墙

知识子域：防火墙

234.　　上网行为管理的功能包括（）。

A.　对网页的访问控制、网络应用控制

B.　宽带及流量管理

C.　互联网传输数据审计、用户行为分析

D.　以上都是

参考答案：D

难易程度：二级

解析：上网行为管理的功能包括对网页的访问过滤、网络应用控制、带宽及流量管理、互联网传输数据审计、用户行为分析等。

知识子域：网络边界防护设备

235.　　以下不是上网行为管理产品的功能的是（）。

A.　能有效的防止内部人员接触非法信息、恶意信息，避免国家、企业秘密或敏感信息泄露。

B.　可对内部人员的互联网访问行为进行实时监控。

C.　提供了在数据流通过时的病毒检测能力。

D.　对网络流量资源进行管理。

参考答案：C

难易程度：二级

解析：在组织机构的互联网出口处部署上网行为管理产品，能有效的防止内部人员接触非法信息、恶意信息，避免国家、企业秘密或敏感信息泄露，并可对内部人员的互联网访问行为进行实时监控，对网络流量资源进行管理，对提高工作效率有极大的帮助。

知识子域：网络边界防护设备

236.　　防病毒网关是（）。

A.　一种对恶意代码进行过滤的边界网络安全防护设备。

B.　对内部网络用户的互联网行为进行控制和管理的边界网络安全产品。

C.　为了满足我国涉及国家秘密的计算机系统必须与互联网物理隔离的要求的前提下，提供数据交换服务的一类安全产品。

D.　对入侵行为进行检测并进行响应的网络安全设备。

参考答案：A

难易程度：二级

解析：防病毒网关是一种对恶意代码进行过滤的边界网络安全防护设备。

知识子域：网络边界防护设备

237.　　统一威胁管理系统是集防火墙、防病毒、入侵检测、上网行为管理等多种网络安全功能于一体的网络安全设备。下列哪个是它的优势（）。

A.　模块化管理，比较容易使用

B.　功能集成带来的风险集中

C.　资源整合带来的高成本

D.　以上都是

参考答案：A

难易程度：二级

解析：统一威胁管理系统（UTM）的优势：资源整合带来的低成本、模块化管理，比较容易使用、配置工作量小，能够提高安全管理人员的工作效率。

知识资源：网络边界防护设备

238. **以下不属于主机检测系统的优点的是（）。**

A. 分析网络报文

B. 监视所有网络

C. 仅能保护安装了产品的主机

D. 能够检测到攻击行为的后果

参考答案：C

难易程度：二级

解析：C 选项是主机检测系统的缺点

知识子域：网络安全管理设备

239. **对于网络入侵检测系统，下列说法不正确的是（）。**

A. 网络入侵检测系统一般旁路安装，对设备性能要求不高，不容易成为瓶颈。

B. 网络入侵检测系统无法对加密的数据进行分析检测。

C. 网络入侵检测系统高速交换网络中处理负荷较重，存在性能不足。

D. 网络入侵检测系统能检测到攻击行为，能对攻击行为后果进行判断。

参考答案：D

难易程度：二级

解析：网络入侵检测系统仅能检测到攻击行为，无法对攻击行为后果进行判断。

知识子域：网络安全管理设备

240. **入侵检测系统通常分为（）两种类型。**

A. 网络入侵检测和设备入侵检测

B. 网络入侵检测和主机入侵检测

C. 软件入侵检测和硬件入侵检测

D. 软件入侵检测和主机入侵检测

参考答案：B

难易程度：二级

解析：入侵检测系统通常分为网络入侵检测(NIDS)和主机入侵检测(HIDS)两种类型。

知识子域：网络安全管理设备

241. **入侵检测系统对入侵行为的识别分为（）。**

A. 基于误用检测和基于异常检测

B. 基于系统检测和基于异常检测

C. 基于误用检测和基于正常检测

D. 基于误用检测和基于用户检测

参考答案：A

难易程度：二级

解析：入侵检测系统对入侵行为的识别分为基于误用检测和基于异常检测。

知识子域：网络安全管理设备

242. **网络安全审计系统是（）。**

A. 一种对网络数据报文进行采集、识别、记录、分析的网络安全设备。

B. 对各类网络设备、操作系统、数据库、支撑软件、应用软件进行安全性检查的一类安全产品。

C. 对入侵行为进行检测并进行响应的网络安全设备。

D. 对内部网络用户的互联网行为进行控制和管理的边界网络安全产品。

参考答案：A

难易程度：二级

解析：网络安全审计系统是一种对网络数据报文进行采集、识别、记录、分析的网络安全设备。

知识子域：网络安全管理设备

243. 堡垒主机是运维管理中广泛使用的一个安全设备，用于（）。

A. 对入侵行为进行检测并进行响应

B. 在公用网络上建立虚拟的专用网络

C. 解决远程维护操作安全问题

D. 对恶意代码进行过滤

参考答案：C

难易程度：二级

解析：堡垒主机是运维管理中广泛使用的一个安全设备，用于解决远程维护操作安全问题。

知识子域：网络安全管理设备

244. 由于密码技术都依赖于密钥，因此密钥的安全管理是密码技术应用中非常重要的环节，下列关于密钥管理说法错误的是（）。

A. 在保密通信过程中，通信双方也可利用 Diffie-Hellman 协议协商出会话密钥进行保密通信。

B. 密钥管理需要在安全策略的指导下处理密钥生命周期的整个过程，包括产生、存储、备份、分配、更新、撤销等。

C. 在保密通信过程中，通信双方可以一直使用之前用过的会话密钥，不影响安全性。

D. 科克霍夫在《军事密码学》中指出系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥。

参考答案：C

难易程度：二级

解析：通信双方一直使用之前用过的会话密钥，会影响安全性。

知识子域：密码学基础

245. 哈希函数的碰撞是指（）。

A. 两个不同的消息，得到相同的消息摘要。

B. 两个相同的消息，得到不同的消息摘要。

C. 消息摘要长度和消息长度不一样。

D. 消息摘要长度和消息长度一样。

参考答案：A

难易程度：二级

解析：哈希函数的碰撞是指两个不同的消息，得到相同的消息摘要。

知识子域：密码学基础

246. 公钥密码的应用不包括（）

A. 数字签名

B. 身份认证

C. 消息认证码

D. 非安全信道的密钥交换

参考答案：C

难易程度：二级

解析：消息认证码不属于公钥密码应用的范畴。

知识子域：密码学基础

247. VPN 用于在公用网络上建立专用网络，从而进行加密通讯。通常 VPN 无需在以下哪项使用数字证书和 PKI（）。

A. 安装部署

B. 身份验证

C. 访问控制

D. 密钥管理

参考答案：A

难易程度：二级

解析：安装部署不需要数字证书和 PKI。

知识子域：网络安全管理设备

248. 门禁卡的作用不包括以下哪项（）。

A. 身份鉴别

B. 访问控制

C. 定位追踪

D. 出入凭证

参考答案：C

难易程度：二级

解析：门禁卡的作用不包括定位追踪。

知识子域：身份鉴别与访问控制

249. https 是很多网站采用的网页访问协议，以下关于 https 的优势说法哪个是正确的（）。

A. 性能要比 http 好

B. 访问速度要比 http 快

C. 安全性要比 http 高

D. 可用性要比 http 强

参考答案：C

难易程度：二级

解析：https 协议的安全性比 http 高。

知识子域：网络安全协议

250. 移动终端对于信息安全的重要意义在于（）。

A. 移动终端中存储着大量的用户个人信息。

B. 移动终端已经成为用户身份验证的一种物品。

C. 移动终端已经成为大量的义务办理渠道，例如手机银行。

D. 以上都对

参考答案：D

难易程度：二级

解析：移动终端中存储着大量的用户个人信息;移动终端已经成为用户身份验证的一种物品;移动终端已经成为大量的义务办理渠道。

知识子域：新技术领域

251. 近年来，随着云计算、大数据技术逐渐应用到安全领域，基于软件即服务（Software-as-a-service，SaaS）模式的 Web 应用安全监测十分具有市场潜力，通常情况下的 SaaS 软件主要应用于哪些企业管理软件（）。

A. 人力资源管理

B. 客户资源管理

C. 供应链管理

D. 以上都是

参考答案：D

难易程度：二级

解析：SaaS 软件主要应用于：人力资源管理、客户资源管理、供应链管理等。

知识子域：新技术领域

252. **现在局域网已非常广泛地使用，下列关于局域网的选项中，不正确的是（）。**

A. 局域网可以实现文件管理、应用软件共享等功能。

B. 局域网是将各种计算机、外部设备、数据库等互相连接起来组成的计算机通信网。

C. 局域网的全称为 Local Area Network，LAN。

D. 局域网是覆盖全世界的。

参考答案：D

难易程度：二级

解析：局域网覆盖范围很小。

知识子域：计算机网络与网络设备

253. **VPN 适用于大中型企业的总公司和各地分公司或分支机构的网络互联和企业同商业合作伙伴之间的网络互联。下列关于 VPN 业务发展趋势的描述中，不正确的是（）。**

A. VPN 厂商的服务质量将会有实质性的提高

B. 运营商取消建设专有 VPN 网络

C. 大型企业 VPN 网络需求增高

D. VPN 厂商竞争更加激烈

参考答案：B

难易程度：二级

解析：运营商不会取消建设专有网络。

知识子域：网络安全管理设备

254. **主机入侵防御系统（HIPS）是一种能监控你电脑中文件的运行和文件运用了其他的文件以及文件对注册表的修改，并向你报告请求允许的软件。下列属于基于主机的入侵防御系统优点的是（）。**

A. 软件直接安装在系统上，可以保护系统免受攻击

B. 当移动系统接入受保护网络时，保护特定主机免受攻击

C. 保护系统免受本地攻击

D. 以上都是

参考答案：D

难易程度：二级

解析：基于主机的入侵防御系统优点有：软件直接安装在系统上，可以保护系统免受攻击、当移动系统接入受保护网络时，保护特定主机免受攻击、保护系统免受本地攻击等。

知识子域：网络安全管理设备

255. **访问控制理论是网络空间安全学科所特有的理论基础。以下属于访问控制的有（）。**

A. 信息隐藏

B. 身份认证

C. 密码技术

D. 以上都是

参考答案：D

难易程度：二级

解析：信息隐藏、身份认证、密码技术都属于访问控制。

知识子域：身份鉴别与访问控制

256. **以下关于序列密码说法不正确的是（）。**

A. 序列密码是单独地加密每个明文位

B. 序列密码的加密和解密使用相同的函数

C. 由于序列密码小而快，所以它们非常合适计算资源有限的应用

D. 现实生活中序列密码的使用比分组密码更为广泛，例如 Internet 安全领域

参考答案：D

难易程度：二级

解析：分组密码比序列密码更广泛。

知识子域：密码学基础

257. **帧中继是在用户--网络接口之间提供用户信息流的双向传送， 并保持信息顺序不变的一种承载业务，帧中继网是什么类型的网络（）。**

A. 局域网

B. 城域网

C. 以太网

D. 广域网

参考答案：D

难易程度：二级

解析：帧中继属于广域网。

知识子域：计算机网络与网络设备

258. **无线广域网是把物理距离极为分散的局域网连接起来的通信方式。无线广域网进行数据通信需要使用（）。**

A. 通信卫星

B. 光纤

C. 公共数据网

D. 电话线

参考答案：A

难易程度：二级

解析：无线广域网进行数据通信使用通信卫星。

知识子域：计算机网络与网络设备

259. **无线局域网是相当便利的数据传输系统，硬件设备包含无线网卡，无线 AP 和无线天线，其中 AP 的作用是（）。**

A. 无线接入

B. 路由选择

C. 业务管理

D. 用户认证

参考答案：A

难易程度：二级

解析：AP 的作用是无线接入。

知识子域：计算机网络与网络设备

260. **漏洞扫描技术是一类重要的网络安全技术。它和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。对于漏洞扫描的原理：1、返回响应；2、发送探测数据包；3、读取漏洞信息；4、特征匹配分析。正确的顺序为（）。**

A. 1->3->2->4

B. 3->4->2->1

C. 1->2->3->4

D. 3->2->1->4

参考答案：D

难易程度：二级

解析：漏洞扫描的原理：1、读取漏洞信息；2、发送探测数据包；3、返回响应；4、特征匹配分析。

知识子域：网络安全管理设备

261. 路由器、防火墙、交换机等网络设备是整个互联网世界的联系纽带，占据着非常重要的地位，是计算机网络的节点。网络设备的安全性尤为重要。下列漏洞中不属于网络设备漏洞的是（）。

A. 网络摄像头漏洞

B. 交换机设备漏洞

C. Windows 系统漏洞

D. 防火墙漏洞

参考答案：C

难易程度：二级

解析：Windows 系统漏洞不属于网络设备漏洞。

知识子域：计算机网络与网络设备

262. 某移动智能终端支持通过指纹识别解锁系统的功能，与传统的基于口令的鉴别技术相比，关于此种鉴别技术说法不正确的是（）。

A. 此类系统一般由用户指纹信息采集和指纹信息识别两部分组成

B. 指纹信息是每个人独有的，指纹识别系统不存在安全威胁问题

C. 所选择的特征（指纹）便于收集、测量和比较

D. 每个人所拥有的指纹都是独一无二的

参考答案：B

难易程度：二级

解析：指纹识别系统也会存在安全问题。

知识子域：身份鉴别与访问控制

263. 以下哪个不是产生 ARP 欺骗的原因（）。

A. ARP 协议是一个无状态的协议

B. ARP 协议是将 IP 地址转化为 MAC 地址的重要协议

C. ARP 信息在系统中会缓存

D. ARP 缓存是动态的，可以被改写

参考答案：B

难易程度：二级

解析：B 不是导致欺骗的原因。

知识子域：网络安全协议

264. 以下关于网络安全设备说法正确的是（）。

A. 入侵检测系统的主要作用是发现并报告系统中未授权或违反安全策略的行为。

B. 虚拟专用网是在公共网络中，利用隧道技术，建立一个永久、安全的通信网络。

C. 防火墙既能实现内外网物理隔离，又能实现内外网逻辑隔离。

D. 安全隔离与信息交换系统也称为网闸，需要信息交换时，同一时间可以和两个不同

安全级别的网络连接。

参考答案：A

难易程度：二级

解析： B 虚拟专用网是在公共网络中，利用隧道技术，建立一个临时的、安全的网络；C 防火墙不能实现内外网物理隔离；D 在需要信息交换时，安全隔离与信息交换系统内部隔离安全交换单元模拟形成开关，同一时间只和一个网络进行连接，不会同时连接两个网络。

知识子域：网络安全管理设备

265. 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（）。

A. 自主访问控制

B. 强制访问控制

C. 基于角色的访问控制

D. 基于任务的访问控制

参考答案：A

难易程度：二级

解析：“针对每个用户指明能够访问的资源”属于自主访问控制。

知识子域：身份鉴别与访问控制

266. 如果一个企业注重于数据的保密性，则建议其使用哪种访问控制模型（）

A. DAC 模型

B. BLP 模型

C. Biba 模型

D. RBAC 模型

参考答案：B

难易程度：二级

解析：BLP 模型侧重于数据的保密性。

知识子域：身份鉴别和访问控制

267. 如果一个企业注重于数据的完整性，则建议其使用哪种访问控制模型（）

A. DAC 模型

B. BLP 模型

C. Biba 模型

D. RBAC 模型

参考答案：C

难易程度：二级

解析：Biba 模型解决了系统内数据的完整性问题。

知识子域：身份鉴别和访问控制

268. 关于物联网体系结构通常，下列说法正确的是（）

A. 支撑层的任务是全面感知外界信息，这一层的主要设备是各种信息收集器。

B. 传输层主要用于把感知层收集到的信息安全可靠地传输到信息支撑层，然后根据不同的应用需求进行信息处理。

C. 应用层主要工作是对节点采集的信息的处理，对信息进行分析和过滤，需要判断接收到的信息是否真正有用，过滤掉垃圾甚至恶意信息。

D. 感知层是具体的应用业务，所涉及的安全问题与业务特性相关，例如隐私保护、知识产权保护、取证、数据销毁等方面。

参考答案：B

难易程度：三级

解析：感知层的任务是全面感知外界信息，这一层的主要设备是各种信息收集器。传输层主要用于把感知层收集到的信息安全可靠地传输到信息支撑层，然后根据不同的应用需求进行信息处理。支撑层主要工作是对节点采集的信息的处理，对信息进行分析和过滤，需要判断接收到的信息是否真正有用，过滤掉垃圾甚至恶意信息。应用层是具体的应用业务，所涉及的安全问题与业务特性相关，例如隐私保护、知识产权保护、取证、数据销毁等方面。

知识子域：新技术领域

269. 以下关于包过滤技术的缺点说法错误的是（）。

A. 过滤规则集合复杂，配置困难。

B. 能防止地址欺骗，不能防止外部客户与内部主机直接连接。

C. 对于网络服务较多、结构较为复杂的网络，包过滤的规则可能很多，配置起来复杂，而且对于配置结果不易检查验证配置的正确性。

D. 由于过滤判别的只有网络层和传输层的有限信息，所以无法满足对应用层信息进行过滤的安全要求。

参考答案：B

难易程度：三级

解析：包过滤技术不能防止地址欺骗。

知识子域：防火墙

270. 以下不属于状态检测防火墙的优点的是（）。

A. 状态检测能够与跟踪网络会话有效地结合起来，并应用会话信息决定过滤规则。能够提供基于无连接协议的应用(如 DNS 等)及基于端口动态分配协议(如 RPC)的应用的安全支持。

B. 具有记录有关通过的每个包的详细信息的能力，各数据包状态的所有信息都可以被记录，包括应用程序对包的请求、连接持续时间、内部和外部系统所做的连接请求等。

C. 处理速度快，在处理速度上具有一定的优势，由于所有的包过滤防火墙的操作都是在网络层上进行的，且在一般情况下仅仅检查数据包头，即处理速度很快，对网络性能影响也较小。

D. 安全性较高，状态防火墙结合网络配置和安全规定做出接纳、拒绝、身份认证、报警或给该通信加密等处理动作。一旦某个访问违反安全规定，就会拒绝该访问，并报告有关状态作日志记录。

参考答案：C

难易程度：三级

解析：C 选项属于静态包过滤的优点。

知识子域：防火墙

271. 以下哪个是状态检测机制的缺点（）

A. 检查内容比包过滤检测技术多，所以对防火墙的性能提出了更高的要求。

B. 需要针对不同的应用进行开发、设置，可能导致对部分应用不支持。

C. 安全性较差，不提供用户认证功能。

D. 由于需要对数据包进行处理后转发，处理速度比包过滤防火墙慢。

参考答案：A

难易程度：三级

解析：状态检测机制的缺点有：检查内容比包过滤检测技术多，所以对防火墙的性能提出了更高的要求；状态检测防火墙的配置非常复杂，对于用户的能力要求较高，使用起来不太方便。

知识子域：防火墙

272. DMZ 区是非军事区或隔离区是（）。

A. 一种网络区域，就是在不信任的外部网络和可信任的内部网络之间建立一个面向外部网络的物理或逻辑子网。

B. 为内部网络和外部网络进行数据通信的转接者。

C. 通过采用状态监视器，对网络通信的各层(包括网络层、传输层以及应用层)实施监测，抽取其中部分数据，形成网络连接的动态状态信息。

D. 以上都不正确

参考答案：A

难易程度：三级

解析：DMZ 是英文 demilitarized zone 的缩写，即非军事区或隔离区，是一种网络区域，就是在不信任的外部网络和可信任的内部网络之间建立一个面向外部网络的物理或逻辑子网。

知识子域：防火墙

273. 以下属于双绞线的两两缠绕的目的是（）。

A. 在接收信号的差分电路中可以将共模信号消除，从而提取出有用信号。

B. 抵御一部分外界电磁波干扰。

C. 降低自身信号的对外干扰。

D. 以上都是

参考答案：D

难易程度：三级

解析：把两根绝缘的导线互相绞在一起，干扰信号作用在这两根相互绞缠在一起的导线上是一致的（共模信号），在接收信号的差分电路中可以将共模信号消除，从而提取出有用信号（差模信号）。双绞线就是采用了这样一对互相绝缘的金属导线互相绞合的方式来抵御一部分外界电磁波干扰，更主要的是降低自身信号的对外干扰，每一根导线在传输中辐射的电波会被另一根线上发出的电波抵消。

知识子域：计算机网络与网络设备

274. 经过多年的技术发展，现在的上网行为管理可实现的功能有很多，其中不包括()。

A. 实时检测入侵并告警

B. 上网身份管控

C. 邮件外发的管控

D. 上网应用的管控

参考答案：A

难易程度：三级

解析：上网行为管理可实现的功能有：上网身份管控、互联网浏览管控、邮件外发管控、用户行为管控、上网应用管控。

知识子域：网络边界防护设备

275. 统一威胁管理系统是集防火墙、防病毒、入侵检测、上网行为管理等多种网络安全功能于一体的网络安全设备。它的局限性有（）。

A. 功能集成带来了风险集中，不符合“纵深防御”的安全管理思想

B. 功能集成带来的系统复杂性、不同模块的协作问题

C. 功能集成带来的性能瓶颈

D. 以上都是

参考答案：D

难易程度：三级

解析：统一威胁管理系统（UTM）的局限性有：功能集成带来了风险集中，不符合“纵深防御”的安全管理思想；功能集成带来的系统复杂性、不同模块的协作问题；功能集成带来的性能瓶颈。

知识子域：网络边界防护设备

276. 关于入侵检测系统中的误用检测系统，下列说法正确的是（）。

A. 建立入侵行为模型（攻击特征）。

B. 假设可以识别和表示所有可能的特征。

C. 基于系统和基于用户的误用。

D. 以上都对

参考答案：D

难易程度：三级

解析：误用检测技术建立入侵行为模型（攻击特征）、假设可以识别和表示所有可能的特征、基于系统和基于用户的误用。

知识子域：网络安全管理设备

277. 关于入侵检测系统中的异常检测系统，下列说法正确的是（）。

A. 设定异常的行为模式

B. 假设所有的入侵行为都是异常的

C. 基于系统和基于设备的异常

D. 以上都对

参考答案：B

难易程度：三级

解析：异常检测技术设定“正常”的行为模式、假设所有的入侵都是异常的、基于系统和基于用户的异常。

知识子域：网络安全管理设备

278. 关于入侵检测系统的部署下列说法不正确的是（）

A. 入侵检测系统的部署前首先需要明确部署目标，也就是检测攻击的需求是什么，然后根据网络拓扑结构，选择适合的入侵检测类型及部署位置。

B. 如果值需要分析针对服务器的攻击，则可以将网络入侵检测系统部署在服务器区的交换机上。

C. 基于主机的入侵检测系统一般更多是用于保护关键主机或服务器，只需要将检测代理部署到这些关键主机或服务器中即可。

D. 需要对全网的数据报文进行分析，不需要在核心交换机上设置镜像端口，也能使网络入侵检测系统能对全网的数据流量进行分析。

参考答案：D

难易程度：三级

解析：需要对全网的数据报文进行分析，就需要在核心交换机上设置镜像端口，将其他端口的数据镜像到入侵检测系统连接的交换机端口，从而使网络入侵检测系统能对全网的数据流量进行分析。

知识子域：网络安全管理设备

279. 关于入侵检测系统的局限性下列说法正确的是（）。

A. 入侵检测虽然能检测到攻击，但由于攻击方式、类型众多，对用户的要求不高。

B. 由于网络传输能力快速增长，对入侵检测系统的性能要求也越来越高，这使得入侵检测难以满足实际业务需要。

C. 入侵检测系统不需要用户具备一定的网络安全知识，系统的配置、管理也较为复杂。

D. 入侵检测系统采取了各类不同的检测技术，入侵检测系统高虚警率问题得以解决。

参考答案：B

难易程度：三级

解析：入侵检测也存在一些问题，这些问题包括：入侵检测虽然能检测到攻击，但由于攻击方式、类型众多，对用户有较高的要求，需要用户具备一定的网络安全知识，系统的配置、管理也较为复杂；由于网络传输能力快速增长，对入侵检测系统的性能要求也越来越高，这使得入侵检测难以满足实际业务需要；尽管采取了各类不同的检测技术，但入侵检测系统高虚警率问题仍然难以解决。

知识子域：网络安全管理设备

280. 以下关于 WAF 产品功能的描述中，不正确的是（）。

A. WAF 产品应该具备针对应用层 DOS 攻击的防护能力。

B. WAF 的应用交付能力可以完全保障用户的敏感信息的安全。

C. WAF 可以阻止非授权访问的攻击者窃取客户端或者网站上含有敏感信息的文件。

D. 基于 URL 的应用层访问控制和 HTTP 请求的合规性检查，都属于 WAF 的应用合规功能。

参考答案：B

难易程度：三级

解析：WAF 的应用交付能力可以完全保障用户的敏感信息的安全，太绝对。

知识子域：防火墙

281. 集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。下面关于集线器的描述正确的是（）。

A. 集线器不能延伸网络可操作的距离

B. 集线器不能过滤网络流量

C. 集线器不能成为中心节点

D. 集线器不能放大变弱的信号

参考答案：B

难易程度：三级

解析：集线器不能过滤网络流量。

知识子域：计算机网络与网络设备

282. 分组密码算法是十分重要的密码算法，以下描述错误的是（）。

A. 分组密码算法要求输入明文按组分成固定长度的块

B. 分组密码算法也称为序列密码算法

C. 分组密码算法每次计算得到固定长度的密文输出块

D. 常见的 DES、IDEA 算法都属于分组密码算法

参考答案：B

难易程度：三级

解析：分组密码是在加密过程中将明文进行分组后在进行加密，序列密码又叫流密码对每一个字节进行加密。

知识子域：密码学基础

283. 以下关于可信计算说法错误的是（）。

A. 可信的主要目的是要建立起主动防御的信息安全保障体系
B. 可信计算机安全评价标准(TCSEC)中第一次提出了可信计算机和可信计算基的概念
C. 可信的整体框架包含终端可信、终端应用可信、操作系统可信、网络互联可信、互联网交易等应用系统可信
D. 可信计算平台出现后会取代传统的安全防护体系和方法

参考答案：D

难易程度：三级

解析：可信计算平台出现后不会取代传统的安全防护体系和方法。

知识子域：新技术领域

284. （）是在公用网络上建立虚拟的专用网络的技术。

A. SET
B. DDN
C. VPN
D. PKI

参考答案：C

难易程度：二级

解析：VPN 是一种架构在公用通信基础设施上的专用数据通信网络，利用 IPSec 等网络层安全协议和建立在 PKI 的加密与签名技术来获得私有性。

知识子域：网络安全管理设备

285. 在信息系统中，（）是在为系统资源提供最大限度共享的基础上对用户的访问权进行管理，防止对信息的非授权篡改和滥用。

A. 身份认证
B. 访问控制
C. 安全审计
D. 数字签名

参考答案：B

难易程度：一级

解析：在信息系统中，访问控制是在为系统资源提供最大限度共享的基础上对用户的访问权进行管理，防止对信息的非授权篡改和滥用。

知识子域：身份鉴别与访问控制

286. 能完成不同的 VLAN 之间数据传递的设备是（）

A. 交换机
B. 中继器
C. 路由器
D. 防火墙

参考答案：C

难易程度：一级

解析：能完成不同的 VLAN 之间数据传递的设备是路由器。

知识子域：计算机网络与网络设备

287. 在一家公司的两个部门各有一个局域网，那么将它们互连的最简单的方法是使用（）。

A. 交换机
B. 路由器
C. 中继器

D. 网桥

参考答案：A

难易程度：一级

解析：交换机可以为接入交换机的任意两个网络节点提供独享的电信号通路。

知识子域：计算机网络与网络设备

288. 域名系统 DNS 的作用是（）。

A. 存储 IP

B. 存储域名

C. 将域名转换成 IP

D. 以上都不对

参考答案：C

难易程度：一级

解析：域名系统 DNS 的作用是将域名转换成 IP。

知识子域：网络安全协议

289. 在同一个信道上的同一时刻，能够同时进行双向数据传送的通信方式是（）。

A. 单工

B. 三工

C. 半双工

D. 全双工

参考答案：D

难易程度：一级

解析：在同一个信道上的同一时刻，能够同时进行双向数据传送的通信方式是全双工。

知识子域：计算机网络与网络设备

290. 关于访问控制列表，不正确的说法是（）。

A. 是以文件为中心建立访问权限表

B. 查询特定主体访问客体时不需要遍历查询所有客体的 ACL

C. 判断对特定客体的授权访问，可访问的主体和访问权限等

D. 访问控制列表(ACL)是一种基于包过滤的访问控制技术

参考答案：B

难易程度：一级

解析：查询特定主体访问客体时需要遍历查询所有客体的 ACL

知识子域：身份鉴别与访问控制

291. 数据传输可分为有线传输和无线传输，以下不属于有线传输的是（）。

A. 光纤

B. 双绞线

C. 无线电波

D. 同轴电缆

参考答案：C

难易程度：一级

解析：无线电波属于无线传输。

知识子域：计算机网络与网络设备

292. 网络安全设备是保护网络安全的设施，以下不属于安全设备的是（）。

A. 防火墙

B. WAF

C. CPU

D. VPN Network

参考答案：C

难易程度：一级

解析：CPU 不属于安全设备。

知识子域：防火墙

293. 以下属于防火墙技术原理的是（）。

A. 挡住未经授权的访问控制。

B. 禁止具有脆弱性的服务带来危害。

C. 实施保护，以避免各种 IP 欺骗和路由攻击。

D. 以上都是

参考答案：D

难易程度：一级

解析：防火墙技术原理：挡住未经授权的访问控制；禁止具有脆弱性的服务带来危害；实施保护，以避免各种 IP 欺骗和路由攻击。

知识子域：防火墙

294. 在 OSI 七层模型中，应用层的传输单位是（）

A. 帧

B. 段

C. 报文

D. 分段

参考答案：C

难易程度：二级

解析：应用层的传输单位是报文。

知识子域：网络安全协议

295. 入侵防御系统（IPS）一般布于防火墙和外来网络的设备之间，依靠对数据包的检测进行防御，以下选项中属于 IPS 的主要功能的是（）。

A. 实时监视和拦截攻击

B. 保护客户端

C. 虚拟补丁

D. 以上都是

参考答案：D

难易程度：一级

解析：IPS 的主要功能：实时监视和拦截攻击；保护客户端；虚拟补丁。

知识子域：边界安全防护设备

296. 以下属于代理防火墙的优点的是（）。

A. 可避免内外网主机的直接连接，从可以隐藏内部 IP 地址，而更好的保护内部计算机。

B. 以与认证、授权等安全手段方便地集成，面向用户授权。

C. 为用户提供透明的加密机制。

D. 以上都是

参考答案：D

难易程度：二级

解析： 代理防火墙的优点：可避免内外网主机的直接连接，从可以隐藏内部 IP 地址，而更好的保护内部计算机；以与认证、授权等安全手段方便地集成，面向用户授权；为

用户提供透明的加密机制。

知识子域：防火墙

297. **以下属于防病毒网关设备的优势（）。**

A. 病毒库只需要更新一套

B. 很难被恶意代码停止

C. 通过和终端保护使用不同厂商的产品，能够形成异构保护

D. 以上都是

参考答案：D

难易程度：三级

解析：防病毒网关设备的优势有：病毒库只需要更新一套；很难被恶意代码停止；通过和终端保护使用不同厂商的产品，能够形成异构保护。

知识子域：网络边界防护设备

298. **IPV6 将 32 位地址空间扩展到（）**

A. 64 位

B. 128 位

C. 256 位

D. 1024 位

参考答案：B

难易程度：三级

解析：128 位的,ipv4 是 32 位的

知识子域：网络边界防护设备

299. **Internet 中应用行为控制不包括哪些功能？（）**

A. Post 操作

B. 代理上网

C. 数据存储

D. 文件上传

参考答案：C

难易程度：三级

解析：

知识子域：网络边界防护设备

300. **下面关于 IPv6 协议优点的描述中，准确的是（）**

A. IPv6 协议允许全局 IP 地址出现重复

B. IPv6 协议解决了 IP 地址短缺的问题

C. IPv6 协议支持通过卫星链路的 Intemet 连接

D. IPv6 协议支持光纤通信

参考答案：B

难易程度：三级

解析：

知识子域：网络边界防护设备