1. 与计算机硬件关系最密切的软件是（ ）。

A、编译程序

B、数据库管理程序

C、游戏程序

D、OS

答案：D

1. 系统的主要功能有（ ）。

A、进程管理、存储器管理、设备管理、处理机管理

B、虚拟存储管理、处理机管理、进程调度、文件系统

C、处理机管理、存储器管理、设备管理、文件系统

D、进程管理、中断管理、设备管理、文件系统答案：C

1. 按照应用领域对操作系统进行划分，不包含以下哪一种（ ）。

A、桌面操作系统

B、批处理操作系统

C、服务器操作系统

D、嵌入式操作系统答案：B

4. 用户在设置口令时，以下原则哪个是错误的（ ）。

A、严禁使用与账号相同或相似的口令

B、不要使用与个人有关的信息作为口令内容

C、不要设置短于 6 个字符或仅包含字母或数字的口令

D、可以使用空口令

答案：D

1. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（ ）。

A、身份鉴别是授权控制的基础和

B、身份鉴别一般不提供双向的认证

C、目前一般采用基于对称秘钥加密或公开密钥加密的方法

D、数字签名机制是实现身份鉴别的重要机制答案：B

1. 下列关于 CA 的说法错误的是（ ）。

A、CA 是负责发布证书的一组机构

B、CA 负责为用户分配公共密钥和私人密钥

C、CA 可分为企业 CA 和独立 CA D、根 CA 可以没有证书

答案：D

1. 在 NTFS 文件系统中，如果一个共享文件夹的共享权限和 NTFS 权限发生了冲突，那么以下说法正确的是：（ ）。

A、共享权限优先 NTFS 权限

B、系统会认定最少的权限

C、系统会认定最多的权限

D、以上都不是

答案：B

8. 在 NTFS 的权限中,修改权限不包括以下下列哪个权限（ ）。

NTFS（New Technology File System）是Windows NT内核的系列操作系统支持的、一个特别为网络和磁盘配额、文件加密等管理安全特性设计的磁盘格式，提供长文件名、数据保护和恢复，能通过目录和文件许可实现安全性，并支持跨越分区。

A、读取

B、列出文件及目录

C、拒绝访问

D、写入

答案：C

1. （ ）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。

A、SET B、DDN C、VPN D、PKIX

答案：C

1. 下列关于操作系统的说法，不正确的是：（ ）。

A、操作系统为用户提供两种接口：命令接口和程序接口

B、常见的个人操作系统有 Windows 系列和 Linux 系列

C、Linux 系统是一款闭源操作系统

D、操作系统在计算机系统中位于硬件和应用软件之间，所以，操作系统既面向系统资

源又面向用户

答案：C

1. 下列关于漏洞的说法，不正确的是（ ）。

A、漏洞是指计算机系统在硬件、软件、协议的设计、具体实现以及系统安全策略上存在的缺陷和不足

B、安全漏洞是信息安全的核心问题

C、漏洞狭义的概念是指软件程序漏洞或缺陷

D、为了防止计算机的漏洞被黑客利用，我们可以关掉计算机的“自动更新”功能答案：D

1. 以下哪一项不属于恶意代码（ ）

A、病毒

B、蠕虫

C、宏

D、特洛伊木马答案：C

1. 下列关于计算机病毒说法错误的是（ ）

A、有些病毒仅能攻击某一种操作系统，如 winD. Ows B、病毒一般附着在其他应用程序之后

C、每种病毒都会给用户造成严重后果

D、有些病毒能损坏计算机硬件答案：C

1. 以下哪一项是伪装成有用程序的恶意软件？（ ）

A、计算机病毒

B、特洛伊木马

C、逻辑炸弹

D、蠕虫程序答案：B

1. 我国正式公布了电子签名法，数字签名机制用于实现（）需求。

A、抗否认

B、保密性

C、完整性

D、可用性答案：A

16. 在 Windows 系统中可以察看开放端口情况的是：（ ）

A、Nbtstat

B、Net

C、Net show

D、Netstat

答案：D

1. 下列安全防护配置措施不正确的是（）

A、关闭系统审核策略

B、开启操作系统口令策略

C、关闭系统不必要的端口

D、开启防火墙和杀毒软件答案：A

1. Windows 系统下的用于存储用户名的文件是( )

A、SECRET B、PASSWD C、USERNAMES D、SAM

答案：D

1. 下列不属于本地安全策略的是（）

A、账户策略

B、组策略

C、本地策略

D、高级安全 Windows 防火墙

答案：B

1. 打开命令行界面后，查看本机 IP 地址的命令是（）

A、ipconfig B、netstat C、tracert D、route

答案：A

1. 下列关于防火墙的说法正确的是（）

A、入栈规则即你的电脑连接其他主机的规则

B、出站规则即其他主机连入你的电脑的规则

C、默认情况下防火墙允许所有传出连接

D、默认情况下防火墙允许所有传入连接答案：C

1. 关于强密码的特征，说法错误的是（）

A、长度至少要有 6 个字符

B、不包含用户的生日、电话、用户名、真实姓名或公司名等

C、不包含完整的字典词汇

D、必须包含大写字母、小写字母、数字和非字母字符

答案：A

1. 下列措施不能防止账户口令暴力破解的是（）

A、修改默认的管理员账户名

B、限制口令输入次数

C、更换密码时新密码不能与之前密码相同或相似

D、设置多位由数字和字母组成的超长密码答案：D

1. SMTP 连接服务器使用端口（ ）

SMTP是一种提供可靠且有效的电子邮件传输的协议。SMTP是建立在FTP文件传输服务上的一种邮件服务，主要用于系统之间的邮件信息传递，并提供有关来信的通知。SMTP独立于特定的传输子系统，且只需要可靠有序的数据流信道支持，SMTP的重要特性之一是其能跨越网络传输邮件，即“SMTP邮件中继”。使用SMTP，可实现相同网络处理进程之间的邮件传输，也可通过中继器或网关实现某处理进程与其他网络之间的邮件传输。

A、21 B、25 C、80 D、110

答案：B

1. 下列关于端口说法错误的是（）

A、IP 地址的端口都是以端口号来标记的，端口号范围是 0~65535 B、端口按协议类型可以分为 TCP 端口、UDP 端口

C、使用 net show 命令可以查看那些计算机正在与本机连接

D、在网络环境中可以使用防火墙或者本地策略的方式关闭一些端口

答案：C

1. 下列关于用户口令说法错误的是（ ）。

A、口令不能设置为空

B、口令长度越长，安全性越高

C、复杂口令安全性足够高，不需要定期修改

D、口令认证是最常见的认证机制答案：C

1. 下列关于木马病毒的特性，不正确的是（ ）

A、隐蔽性

B、主动传播性

C、自动运行性

D、破坏性答案：B

1. 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。

A、身份认证

B、安全审计

C、访问控制

D、数字证书

答案：C

1. 关于 C/S 、B/S 架构说法错误的是（ ）

A、C/S 架构是指客户端/服务器架构

B、B/S 架构是指浏览器/服务器架构

C、C/S 架构是建立在广域网之上, 对安全的控制能力相对弱, 面向是不可知的用户群

D、B/S 架构中终端用户不需要安装专门的软件，只需要安装浏览器即可答案：C

1. 在计算机系统中，操作系统是（ ）

A、一般应用软件

B、核心系统软件

C、用户应用软件

D、系统支撑软件答案：B

1. 入侵者在张某的博客中搜寻到他在某网站的交易信息，利用信息中的内容获取张某的个人信息，并进一步获取了其它额外的信息，这种行为属于（）

A、社会工程

B、非法窃取

C、电子欺骗

D、电子窃听

答案：A

1. 信息安全的发展经过了四个历史发展阶段，从信息安全的发展过程中可以看出，随着信息技术本身的发展和信息技术应用的发展，信息安全的内涵和外延都在不断地加深和扩大，包含的内容已从初期的数据加密演化到后来的数据恢复、信息纵深防御等。历史发展阶段顺序正确的是（）

A、通信安全阶段、信息安全阶段、计算机安全阶段、信息安全保障阶段

B、计算机安全阶段、信息安全阶段、通信安全阶段、信息安全保障阶段

C、通信安全阶段、计算机安全阶段、信息安全阶段、信息安全保障阶段

D、计算机安全阶段、通信安全阶段、信息安全阶段、信息安全保障阶段答案：C

1. 社会工程学攻击成功的主要原因是人们的信息安全意识淡薄，而产生认知偏差。下列选项都属于社会工程学攻击方式的是（）

A、假托、等价交换、敲诈者病毒

B、信息收集、网络钓鱼攻击、身份盗用

C、身份盗用威胁、信息收集、AV 终结者

D、信息收集、敲诈者病毒、暴力破解攻击答案：B

1. 完整的数字签名过程（包括从发送方发送消息到接收方安全的接收到消息）包括（）和

验证过程。

A、加密

B、解密

C、签名

D、保密传输

答案：C

1. 信息安全保障的目的不仅是保护信息和资产的安全，更重要的是通过保障信息系统安全来保障信息系统所支持的业务安全，从而实现业务的可持续性。信息安全保障不包括以下哪个方面（）

A、安全特征

B、安全要素

C、生命周期

D、保障要素答案：B

1. 下面选项中关于对称密码体制和非对称密码体质描述错误的是（C）

A、对称密码体制通信双方拥有同样的密钥，使用的密钥相对较短，密文的长度往往与明文长度相同。

B、非对称密码体制中使用的密钥有两个，一个是对外公开的公钥，可以象电话号码一样进行注册公布；另一个是必须保密的私钥，只有拥有者才知道。

C、与非对称密码体制相比，对称密码体制加解密速度较慢。同等安全强度下，非对称

密码体制要求的密钥位数要多一些。

D、非对称密码体制主要是为了解决对称密码体制的缺陷而提出的，即为了解决对称密

码体制中密钥分发和管理的问题，以及不可否认的问题。

答案：C

1. 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需要遍历查询所有客体的 ACL C、耗费资源少，是一种成熟且有效的访问控制方法。

D、判断对特定客体的授权访问，可访问的主体和访问权限等答案：C

1. 数字签名是在签名者和签名接收者之间进行的，这种数字签名方式主要依赖公钥密码体制来实现，以下对数字签名描述正确的是（）

A、签名值的长度与被签名消息的长度有关

B、数字签名是被签名消息的一部分

C、数字签名算法中，通常对消息的 Hash 值签名，而不对消息本身签名

D、同一人利用同一签名算法对同一消息进行多次签名所得的签名值应值相同的答案：C

1. VPN 它有两层含义：首先是“虚拟的”，即用户实际上并不存在一个独立专用的网络，既不需要建设或租用专线，也不需要装备专用的设备，而是将其建立在分布广泛的公共网

络上，就能组成一个属于自己专用的网络。其次是“专用的”，相对于“公用的”来说，它强

调私有性和安全可靠性。不属于 VPN 的核心技术是（）

A、隧道技术

B、身份认证

C、日志记录

D、访问控制

答案：C

1. 网络地址转换是在 IP 地址日益缺乏的情况下产生的一种网络技术，主要目的是重用 IP

地址，以下关于网络地址转换技术的说法，错误的是（）

A、只能进行一对一的网络地址翻译

B、解决 IP 地址空间不足问题

C、向外界隐藏内部网结构

D、有多种地址翻译模式答案：A

1. 信息安全的三个基本安全属性不包括（）

A、机密性

B、完整性

C、可用性

D、真实性答案：D

1. 虚拟专用网络（VPN）通常是指在公共网路中利用隧道技术，建立一个临时的，安全的网络。这里的字母 P 的正确解释是（）

A、Special-purpose. 特定、专用用途的

B、Proprietary 专有的、专卖的

C、Private 私有的、专有的

D、Specific 特种的、具体的答案：C

1. 与 PDR 模型相比， P2DR 模型多了哪一个环节?

[PDR（网络安全模型之一）\_百度百科 (baidu.com)](https://baike.baidu.com/item/PDR/17563449?fr=aladdin)

A．防护

B．检测

C．反应

D．策略

答案：D

1. 以下关于信息安全威胁描述错误的是（）

A、从受威胁对象的角度，可以将我国面临的信息安全威胁分为 3 类：国家威胁、组织威胁和个人威胁。

B、信息系统都是在一定的自然环境下运行，自然灾害对信息系统的威胁时多方面的，地震、火灾、水灾等各种自然灾害都可能对信息系统造成灾难性破坏。

C、信息安全问题的根源主要来源于信息系统自身存在的脆弱性。

D、信息安全问题的外因主要来源于人为和环境威胁。

答案：C

1. Alice 用 Bob 的密钥加密明文，将密文发送给 Bob。 Bob 再用自己的私钥解密，恢复出明文。以下说法正确的是（）

A、此密码体制为对称密码体制

B、此密码体制为私钥密码体制

C、此密码体制为单钥密码体制

D、此密码体制为公钥密码体制答案： D

1. 密码学是网络安全的基础，但网络安全不能单纯依靠安全的密码算法、密码协议也是网络安全的一个重要组成部分。下面描述中错误的是（）

A.在实际应用中，密码协议应按照灵活性好、可扩展性高的方式制定，不要限制和框住的执行步骤，有些复杂的步骤可以不明确处理方式。

B.密码协议定义了两方或多方之间为完成某项任务而指定的一系列步骤，协议中的每个参与方都必须了解协议，且按步骤执行。

C.根据密码协议应用目的的不同，参与该协议的双方可能是朋友和完全信息的人，也可能是敌人和互相完全不信任的人。

D.密码协议(cryptographic protocol) ,有时也称安全协议(security protocol), 是使用密码学完成某项特定的任务并满足安全需求的协议，其末的是提供安全服务。

答案： A

1. 在混合加密方式下，真正用来加解密通信过程中所传输数据的密钥是（）

[对称与非对称加密算法\_liudongdong\_jlu-CSDN博客\_对称加密算法有哪些](https://blog.csdn.net/liudongdong19/article/details/82217431)

A、非对称密码算法的公钥

B、对称密码算法的密钥

C、非对称密码算法的私钥

D、CA 中心的公钥答案：B

1. 若 Bob 给 Alice 发送一封邮件，并想让 Alice 确信邮件是由 Bob 发出的，则 Bob 应该选用哪种密钥对邮件加密？

A、Alice 的公钥

B、Alice 的私钥

C、Bob 的公钥

D、Bob 的私钥答案：D

1. 公钥密码学的思想最早是谁提出的？

A、欧拉（Euler）

B、迪菲（Diffie）和赫尔曼（Hellman）C、费马（Fermat）D、Rivest、Shamir、Adleman

答案：B

1. PKI 的主要理论基础是（）

[5分钟让你知道什么是PKI - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/30136885)

A、对称密码算法

B、公钥密码算法

C、量子密码

D、摘要算法答案：B

1. 数字签名为保证其不可更改性，双方约定使用

A、 HASH 算法

B、 RSA 算法

C、 CAP 算法

[CAP协议以及算法 - 简书 (jianshu.com)](https://www.jianshu.com/p/7a379076f0da)

D、 ACR 算法

[ARC算法 - 简书 (jianshu.com)](https://www.jianshu.com/p/53b97f3b7687)

答案：B

1. HASH 函数可应用于() A、数字签名

[数字签名 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/29007210)

B、生成程序或文档的“数字指纹”

C、安全存储口令

D、数据的抗抵赖性答案：B

1. 下列哪一种方法属于基于实体“所有” 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，对系统发送的挑战进行正确应答，通过身份鉴别

D.用户使用集成电路卡(如智能卡)完成身份鉴别答案：D

1. 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”以及实体“所有”的鉴别方法

B、实体“所有”以及实体“特征”的鉴别方法

C、实体“所知”以及实体“特征”的鉴别方法

D、实体“所有”以及实体“行为”的鉴别方法答案：A

1. 鉴别的基本途径有三种：所知、所有和个人特征，以下哪一项不是基于你所知道的：

A、口令

B、令牌

C、知识

D、密码

答案：B

1. 账号锁定策略中对超过一定次数的错误登录账号进行锁定是为了对抗以下哪种攻击? A．分布式拒绝服务攻击(DDoS)

B．病毒传染

C. 口令暴力破解

D．缓冲区溢出攻击

答案：C

1. 下面不属于常用的浏览器的安全措施的是（）

A、删除和管理 Cookies B、不点击网站的广告

C、禁用 ActiveX 控件

D、删除浏览器历史纪录答案：B

1. 以下不能设置口令加密的文件是

A．ZIP B．PPT C．PDF D．TXT

答案：D

1. 以下对异地备份中心的理解最准确的是：

A、与生产中心不在同一城市

B、与生产中心距离 10 公里以上

C、与生产中心距离 100 公里以上

D、与生产中心面临相同区域性风险的机率很小

答案：D

1. 关于信息安全事件管理和应急响应，以下说法错误的是：

A． 应急响应是指组织为了应对突发／重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施

B. 应急响应方法，将应急响应管理过程分为遏制、根除、处置、恢复、报告和跟踪 6 个

阶段

C．对信息安全事件的分级主要参考信息系统的重要程度、系统损失和社会影响三方面

因素

D．根据信息安全事件的分级参考要素，可将信息安全事件划分为 4 个级别：特别重大

事件(Ⅰ级)、重大事件(Ⅱ级)、较大事件(Ⅲ级)和一般事件(Ⅳ级)

答案：B

1. 以下对于信息安全事件理解错误的是：

A、信息安全事件，是指由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件

B、对信息安全事件进行有效管理和响应，最小化事件所造成的损失和负面影响，是组织信息安全战略的一部分

C、应急响应是信息安全事件管理的重要内容

D.、通过部署信息安全策略并配合部署防护措施，能够对信息及信息系统提供保护， 杜

绝信息安全事件的发生

答案： D

1. 有关危害国家秘密安全的行为的法律责任，正确的是：

A、严重违反保密规定行为只要发生，无论产生泄密实际后果，都要依法追究责任

B、非法获取国家秘密，不会构成刑事犯罪，不需承担刑事责任

C．、过失泄露国家秘密，不会构成刑事犯罪，不需承担刑事责任

D、承担了刑事责任，无需再承担行政责任和／或其他处分答案： A

1. 金女士经常通过计算机在互联网上购物，从安全角度看，下面哪项是不好的操作习惯（）

A、使用专用上网购物用计算机，安装好软件后不要对该计算机上的系统软件，应用软件进行升级

B、为计算机安装具有良好声誉的安全防护软件，包括病毒查杀，安全检查和安全加固方面的软件

C、在 IE 的配置中，设置只能下载和安装经过签名的，安全的 ActiveX 控件

D、在使用网络浏览器时，设置不在计算机中保留网络历史纪录和表单数据答案： A

1. 在设计信息系统安全保障方案时，以下哪个做法是错误的：

A、要充分切合信息安全需求并且实际可行

B、要充分考虑成本效益，在满足合规性要求和风险处置要求的前提下，尽量控制成本

C、要充分采取新技术，在使用过程中不断完善成熟，精益求精，实现技术投入保值要

求

D、要充分考虑用户管理和文化的可接受性，减少系统方案障碍答案： C

1. 由于发生了一起针对服务器的口令暴力破解攻击，管理员决定对设置帐户锁定策略以对抗口令暴力破解。他设置了以下账户锁定策略如下：

复位账户锁定计数器 5 分钟-----保证一定时间的拒绝验证服务提交

账户锁定时间 10 分钟

-----提供账号保护，如果比较急切，那么用户本身需要提供解锁服务，否则就需要等待

账户锁定阀值 3 次无效登陆

以下关于以上策略设置后的说法哪个是正确的

A、设置账户锁定策略后，攻击者无法再进行口令暴力破解，所有输错的密码的拥护就会被锁住

B、如果正常用户部小心输错了 3 次密码，那么该账户就会被锁定 10 分钟， 10 分钟内即使输入正确的密码，也无法登录系统

C、如果正常用户不小心连续输入错误密码 3 次，那么该拥护帐号被锁定 5 分钟， 5

分钟内即使交了正确的密码，也无法登录系统

D、攻击者在进行口令破解时，只要连续输错 3 次密码，该账户就被锁定 10 分钟，而正常拥护登陆不受影响

答案： B

1. 为了防御网络监听，最常用的方法是（）

A、采用物理传输（非网络）

B、信息加密

C、无线网

D、使用专线传输答案：B

1. 在网络安全中，在未经许可的情况下，对信息进行删除或修改，这是对（）的攻击。

A、可用性

B、保密性

C、完整性

D、真实性答案：C

1. 使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于（）漏洞。

A、拒绝服务

B、文件共享

C、BIND 漏洞

D、远程过程调用

答案：A

1. 针对窃听攻击采取的安全服务是( ) A、鉴别服务

B、数据机密性服务

C、数据完整性服务

D、抗抵赖服务答案：B

1. 通过截取以前的合法记录稍后重新加入一个连接，叫做重放攻击，为防止这种情况，可以采用的方法是（）

[重放攻击-实例解析\_weixin\_30512785的博客-CSDN博客](https://blog.csdn.net/weixin_30512785/article/details/96952696)

A、加密

B、加入时间戳

C、认证

D、使用密钥

答案：B

1. 能完成不同的 VLAN 之间数据传递的设备是（）

A.中继器

B.二层交换器

C.网桥

D.路由器

答案：D

1. 一个 VLAN 可以看作是一个（）

A.冲突域

B.广播域

C.管理域

D.阻塞域答案：B

1. 以下网络地址中属于 B 类的可用 IP 地址的是（）

A. 192.12.31.2

B.191.12.255.255

1. 55.32.255.0

D.128.34.255.9

答案：D

1. 在运行 Windows 的计算机中配置网关，类似于在路由器中配置（）

A.直接路由

B.默认路由

C.静态路由

D.动态路由答案：C

1. 100BASE-T 规定，Hub 通过 RJ45 接口与计算机连线距离不超过（）米

A.50 米

B.100 米

C.150 米

D.185 米

答案 B

1. 在网络互连中，在网络层实现互连的设备是（）

A.中继器

B.路由器

C.网桥

D.网关

答案：B

1. 如果一个单位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.网关

B.中继器

C.交换机

D.路由器答案：C

1. TCP/IP 协议是 Internet 中计算机之间通信所必须共同遵循的一种（）

A.信息资源

B.通信规定

C.软件

D.硬件

答案：B

1. IP 地址能惟一地确定 Internet 上每台计算机与每个用户的（）

A.距离

B.费用

C.位置

D.时间

答案：C

1. “www.itsec.gov.cn”是 Internet 中主机的（）

A.硬件编码

B.密码

C.软件编码

D.域名

答案：D