# ISCC选择题

公开密钥机制的功能是\_\_\_\_\_\_。D

A.能实现通信中各实体的身份认证

B.能保证数据完整性

C.能抗否认性

D.以上都是

病毒的运行特征和过程是\_\_\_\_\_\_。C

A.入侵、运行、驻留、传播、激活、破坏

B.传播、运行、驻留、激活、破坏、自毁

C.入侵、运行、传播、扫描、窃取、破坏

D.复制、运行、撤退、检查、记录、破坏

对于一个组织，保障其信息安全并不能为其带来直接的经济效益，相反还会付出较大的成本，那么组织为什么需要信息安全？\_\_\_\_\_\_。D

A.有多余的经费

B.全社会都在重视信息安全，我们也应该关注

C.上级或领导的要求

D.组织自身业务需要和法律法规要求

在下面的调试工具中，常用于静态分析的是 C

A.Windbg

B.Softice

C.IDA

D.Ollydbg

IPSec协议工作在OSI模型\_\_\_\_\_\_层。B

A.数据链路层

B.网络层

C.应用层

D.传输层

TELNET协议主要应用于哪一层 A

A.应用层

B.传输层

C.Internet层

D.网络层

RIP是\_\_\_\_\_\_协议栈上一个重要的路由协议。D

A.IPX

B.NETBEUL

C.APPLETalk

D.TCP/IP

对日志数据进行审计检查，属于\_\_\_\_\_\_类控制措施。B

A.预防

B.检测

C.威慑

D.修正

根据美国联邦调查局的评估，80%的攻击和入侵来自\_\_\_\_\_\_。B

A.接入网

B.企业内部网

C.公用IP网

D.个人网

MD5的每个非线性轮函数由\_\_\_\_\_\_步操作来完成，每步对应一个子分组。C

A.4

B.8

C.16

D.32

ISO17799的内容结构按照\_\_\_\_\_\_进行组织。C

A.管理原则

B.管理框架

C.管理域—控制目标—控制措施

D.管理制度

计算机病毒是指：C

A.带细菌的磁盘

B.已损坏的磁盘

C.具有破坏性的特制程序

D.被破坏了的程序

下面哪一个情景属于审计（Audit）D

A.用户依照系统提示输入用户名和口令

B.用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C.用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D.某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

网上银行系统的一次转账操作过程中发生了转账金额被非法篡改的行为，这破坏了信息安全的\_\_\_\_\_\_属性。B

A.保密性

B.完整性

C.不可否认性

D.可用性

假设使用一和加密算法，它的加密方法很简单，将每一个字母加5，即a加密成f，b加密成g,这种算法的密钥就是5，那么它属于\_\_\_\_\_\_。A

A.对称密码技术

B.分组密码技术

C.公钥密码技术

D.单向函数技术

用户暂时离开时，锁定Windows系统以免其他人非法使用。锁定系统的快捷方式为同时按住 C

A.WIN键和Z键

B.F1键和L键

C.WIN键和L键

D.F1键和Z键

\_\_\_\_\_\_是最常用的公钥密码算法。A

A.RSA

B.DSA

C.椭圆曲线

D.量子密码

在下列网络威胁中，哪个不属于信息泄露？\_\_\_\_\_\_。C

A.数据窃听

B.流量分析

C.拒绝服务攻击

D.偷窃用户账号

CMIP的中文含义为\_\_\_\_\_\_。B

A.边界网关协议

B.公用管理信息协议

C.简单网络管理协议

D.分布式安全管理协议

系统备份与普通数据备份的不同在于，它不仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速\_\_\_\_\_\_。A

A.恢复整个系统

B.恢复所有数据

C.恢复全部程序

D.恢复网络设置

下列命令中，\_\_\_\_\_\_不是用来在路由器身份鉴别是安全服务中设置口令。B

A.router(config)#enablesecret

B.router(config-line)#passwordtest

C.router(config)#serviceencryptionpassword

D.router(config)#enablepassword

关于密钥的描述中下列说法正确的是\_\_\_\_\_\_。B

A.密钥是保密的。

B.私钥是保密的，而公钥是公开的。

C.用一个密钥加密的数据必须用同一密钥才能正确解密。

D.密钥的长度不短于明文的长度。

iOS平台上常见的Hook框架有 D

A.Xposed

B. Intent Fuzz

C. Drozer

D. Substrate

下列选项中，不属于计算机病毒特征的是\_\_\_\_\_\_。D

A.破坏性

B.潜伏性

C.传染性

D.免疫性

不属于计算机病毒防治的策略的是 D

A.确认您手头常备一张真正“干净”的引导盘

B.及时可靠升级反病毒产品

C.新购置的计算机软件也要进行病毒检测

D.整理磁盘

当你感觉到你的PC运行速度明显减慢，当你打开任务管理器后发现CPU的使用率达到了百分之百，你最有可能认为你受到了哪一种攻击？B

A.特洛伊木马

B.拒绝服务

C.欺骗

D.中间人攻击

通过修改\_\_\_\_\_\_文件来设置WEB虚拟主机。A

A.httpconf

B.sendmail.cf

C.diphosts

D.Host.conf

以太网交换机的最大带宽为\_\_\_\_\_\_。C

A.等于端口带宽

B.大于端口带宽的总和

C.等于端口带宽的总和

D.小于端口带宽的总和

网络地址转换(NAT)的三种类型是\_\_\_\_\_\_。C

A.静态NAT、动态NAT和混合NAT

B.静态NAT、网络地址端口转换NAPT和混合NAT

C.静态NAT、动态NAT和网络地址端口转换NAPT

D.动态NAT、网络地址端口转换NAPT和混合NAT

从系统结构上来看，入侵检测系统可以不包括\_\_\_\_\_\_。C

A.数据源

B.分析引擎

C.审计

D.响应

Windows NT提供的分布式安全环境又被称为A

A.域（Domain）

B.工作组

C.对等网

D.安全网

Telnet指的是D

A.万维网

B.电子邮件

C.文件传输

D.远程登录

某公司申请到一个C类IP地址，但要连接6个子公司，最大的一个子公司有26台计算机，每个子公司在一个网段中，则子网掩码应设为\_\_\_\_\_\_。D

A.255.255.255.0

B.255.255.255.128

C.255.255.255.192

D.255.255.255.224

电子商务交易必须具备抗抵赖性，目的在于防止：\_\_\_\_\_\_。C

A.信息从被监视的通信过程中泄漏出去

B.他人对数据进行非授权的修改、破坏

C.参与此交易的一方否认曾经发生过此次交易

D.一个实体假装成另一个实体

下面对于个人防火墙未来的发展方向，描述不准确的是\_\_\_\_\_\_。D

A.与xDSLModem、无线AP等网络设备集成

B.与防病毒软件集成，并实现与防病毒软件之间的安全联动

C.将个人防火墙作为企业防火墙的有机组成部分

D.与集线器等物理层设备集成

GRE协议\_\_\_\_\_\_。B

A.既封装、又加密

B.只封装、不加密

C.不封装、只加密

D.不封装、不加密

VPN的加密手段是\_\_\_\_\_\_。C

A.具有加密功能的防火墙

B.带有加密功能的路由器

C.VPN内的各台主机对各自的信息进行相应的加密

D.单独的加密设备

你修改域控制器上的GPO要求密码最少8位，然而对于用户没有生效，如何做？\_\_\_\_\_\_。C

A.初始化复制确定GPC和GPT都被复制

B.配置每台客户机本地策略要求密码8位

C.修改域上GPO要求密码至少8位，并且GPO不能被覆盖

D.修改域上GPO满足复杂程度要求

Telnet中常使用ssh的原因是\_\_\_\_\_\_。A

A.SSH提供了一个可以防止被窃听的安全通信通道

B.Telnet许可证可能在今后几年内会到期

C.SSH源码是公开的Telnet不公开源码

D.SSH协议使用比Telnet使用的加密算法更加棒的加密算法

在加密技术的实际应用中，以下\_\_\_\_\_\_是保密的关键？B

A.算法

B.密钥

C.算法和密钥

D.以上都是

当入侵检测分析引擎判断到有入侵后，紧接着应该采取的行为是\_\_\_\_\_\_。A

A.记录证据

B.跟踪入侵者

C.数据过滤

D.拦截

针对缓冲区溢出攻击，最佳的解决方法有哪些？\_\_\_\_\_\_。C

A.安装入侵检测系统

B.安装防火墙

C.给系统打最新的补丁

D.安装防毒软件

内容过滤技术的含义不包括\_\_\_\_\_\_。D

A.过滤互联网请求从而阻止用户浏览不适当的内容或站点

B.过滤流入的内容从而阻止潜在的攻击进入用户的网络系统

C.过滤流出的内容从而阻止敏感数据的泄漏

D.过滤用户的输入从而阻止用户传播非法内容

网络信息探测中第一步要做的是什么工作？A

A.扫描

B.Ping

C.隐藏自己

D.溢出

关于双钥密码体制的正确描述是\_\_\_\_\_\_。A

A.双钥密码体制中加解密密钥不相同，从一个很难计算出另一个

B.双钥密码体制中加密密钥与解密密钥相同，或是实质上等同

C.双钥密码体制中加解密密钥虽不相同，但是可以从一个推导出另一个

D.双钥密码体制中加解密密钥是否相同可以根据用户要求决定

以下关于盗版软件的说法，错误的是\_\_\_\_\_\_。C

A.可能会包含不健康的内容

B.成为计算机病毒的重要来源和传播途径之一

C.若出现问题可以找开发商负责赔偿损失

D.使用盗版软件是违法的

下面关于响应的说法正确的是\_\_\_\_\_\_。D

A.主动响应和被动响应是相互对立的，不能同时采用

B.被动响应是入侵检测系统中的唯一响应方式

C.入侵检测系统提供的警报方式只能是显示在屏幕上的警告信息或窗口

D.主动响应的方式可以是自动发送邮件给入侵发起方的系统管理员请求协助以识别问题和处理问题

下列不属于系统安全的技术是B

A.E防火墙

B.加密狗

C.认证

D.防病毒

计算机病毒程序隐藏在计算机系统的\_\_\_\_\_\_。 C

A.内存中

B.软盘中

C.存储介质中

D.网络中

A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送数字签名M，对信息M加密为：M’=KB公开（KA秘密（M））。B方收到密文的解密方案是\_\_\_\_\_\_。C

A.KB公开（KA秘密（M’））

B.KA公开（KA公开（M’））

C.KA公开（KB秘密（M’））

D.KB秘密（KA秘密（M’））

与对称加密技术相比，非对称加密算法之所以称之为“非对称”，其含义是指\_\_\_\_\_\_。B

A.加密算法和解密算法不对称。

B.加密密钥和解密密钥不同。

C.加密算法和解密算法不同。

D.加密算法不可逆。

下面不属于容灾内容的是\_\_\_\_\_\_。A

A.灾难预测

B.灾难演习

C.风险分析

D.业务影响分析

保护电子邮件安全的唯一方法是：\_\_\_\_\_\_。A

A.加密邮件内容

B.依赖杀毒软件

C.在安全设置中禁止其执行

D.安装个人防火墙

国家对计算机信息系统安全专用产品的销售\_\_\_\_\_\_。B

A.由行业主管部门负责

B.实行许可证制度

C.与其他产品一样，可以任意进行

D.国家不作规定

会话侦听与劫持技术属于( )技术B

A.密码分析还原

B.协议漏洞渗透

C.应用漏洞分析与渗透

D.DOS攻击

不属于安全策略所涉及的方面是\_\_\_\_\_\_。D

A.物理安全策略

B.访问控制策略

C.信息加密策略

D.防火墙策略

防火墙是组织实施其网络安全策略的主要技术手段之一。防火墙的基本类型主要包括了4类，其中有包过滤防火墙，包过滤防火墙工作在网络协栈的哪个层？\_\_\_\_\_\_。A

A.网络层

B.会话层

C.表示层

D.物理层

下列关于启发式病毒扫描技术的描述中错误的是\_\_\_\_\_\_。C

A.启发式病毒扫描技术是基于人工智能领域的启发式搜索技术

B.启发式病毒扫描技术不依赖于特征代码来识别计算机病毒

C.启发式病毒扫描技术不会产生误报，但可能会产生漏报

D.启发式病毒扫描技术能够发现一些应用了已有机制或行为方式的病毒

ISO定义的安全体系结构中包含\_\_\_\_\_\_。B

A.4种安全服务

B.5种安全服务

C.6种安全服务

D.7种安全服务

为了防止电子邮件中的恶意代码，应该用\_\_\_\_\_\_。B

A.网页

B.纯文本

C.Outlook

D.会话

下列关于加壳与脱壳说法正确的是A

A.对于执行加了壳的应用程序，首先运行的实际上是壳程序，然后才是用户所执行的应用程序本身。

B.由于加壳的原因，加壳后程序所占的存储空间将会比原程序大上好几倍。

C.加过壳的程序无法直接运行，必须要先进行脱壳才能运行。

D.对于加过壳的程序，可以对其进行反编译，得到其源代码进行分析，并进行脱壳。

以下关于数字签名说法正确的是：\_\_\_\_\_\_。A

A.数字签名能给解决篡改、伪造等安全性问题

B.数字签名一般采用对称加密机制

C.数字签名是在所传输的数据后附加一段和传输数据无关的数字信息

D.数字签名能解决数据的加密传输，即安全传输问题

局域网的拓扑结构主要包括\_\_\_\_\_\_。A

A.总线结构、环型结构和星型结构

B.环网结构、单环结构和双环结构

C.单环结构、双环结构和星型结构

D.网状结构、单总线结构和环型结构

监听的可能性比较低的是（ ）数据链路 B

A.Ethernet

B.电话线

C.有线电视频道

D.无线电

IpSec协议中负责对IP数据报加密的部分是\_\_\_\_\_\_。A

A.封装安全负载（ESP）

B.鉴别包头（AH）

C.Internet密钥交换（IKE）

D.以上都不是

互联网上网服务营业场所安全管理系统是以记录并留存\_\_\_\_\_\_并集过滤封堵非法网站和通知汇报等管理功能于一体的安全管理系统。D

A.上网者的业务信息

B.从业人员行为信息

C.上网者的注册信息

D.计算机信息系统运行日志记录信息

以下哪一种方法无法防范口令攻击\_\_\_\_\_\_。A

A.启用防火墙功能

B.设置复杂的系统认证口令

C.关闭不需要的网络服务

D.修改系统默认的认证名称

信息安全领域内最关键和最薄弱的环节是\_\_\_\_\_\_。D

A.技术

B.策略

C.管理制度

D.人

不属于WEB服务器的安全措施的是\_\_\_\_\_\_。D

A.保证注册帐户的时效性

B.删除死帐户

C.强制用户使用不易被破解的密码

D.所有用户使用一次性密码

TCP滑动窗口的功能是什么？\_\_\_\_\_\_。C

A.使得窗口尺寸更大，以便一次可以发送更多的数据，从而更加有效地利用带宽。

B.窗口的尺寸根据每个数据报进行滑动以接收数据，从而更有效地利用带宽。

C.在TCP会话过程中，允许动态协商窗口尺寸的大小，从而更加有效地利用带宽。

D.限制进入的数据，使得分段必须逐个发送，不是有效的带宽的利用方式。

非对称加密算法在加/解密时，分别使用了\_\_\_\_\_\_。B

A.两个相同的密钥

B.两个不同的密钥，一个是保密的，另一个是公开的

C.两个不同的保密密钥

D.两个不同的公开密钥

有关数据库加密，下面说法不正确的是\_\_\_\_\_\_。C

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

假设系统有1000个用户，每两个用户之间可以进行保密通信，如果采用公钥加密算法，用系统要拥有\_\_\_\_\_\_个密钥。A

A.1000

B.499500

C.2000

D.5000

一份好的计算机网络安全解决方案，不仅要考虑到技术，还要考虑的是\_\_\_\_\_\_。C

A.软件和硬件

B.机房和电源

C.策略和管理

D.加密和认证

IPSec协议是开放的VPN协议，下面描述有误的是：\_\_\_\_\_\_。C

A.适应于向IPV6迁移

B.提供在网络层上的数据加密保护

C.支持动态的IP地址分配

D.不支持除TCP/IP外的其他协议

下列对计算机网络的攻击方式中，属于被动攻击的是\_\_\_\_\_\_。A

A.口令嗅探

B.重放

C.拒绝服务

D.物理破坏

UNIX/Linux操作系统的文件系统是\_\_\_\_\_\_结构。B

A.星型

B.树型

C.网状

D.环型

在TCP/IP协议中，UDP协议是一种( )协议D

A.主机-网络层

B.互联网络层

C.应用层

D.传输层

十六进制数(AB)16变换为等值的八进制数是\_\_\_\_\_\_。A

A.253

B.35l

C.243

D.101

以下方法中，不适用于检测计算机病毒的是\_\_\_\_\_\_。C

A.特征代码法

B.校验和法

C.加密

D.软件模拟法

根据国际上对数据备份能力的定义，下面不属于容灾备份类型？\_\_\_\_\_\_。C

A.存储介质容灾备份

B.业务级容灾备份

C.系统级容灾备份

D.数据级容灾备份

用户A通过计算机网络向用户B发消息，表示自己同意签订某个合同，随后用户A反悔，不承认自己发过该条消息。为了防止这种情况发生，应采用\_\_\_\_\_\_。A

A.数字签名技术

B.消息认证技术

C.数据加密技术

D.身份认证技术

在安全评估过程中，采取\_\_\_\_\_\_手段，可以模拟黑客入侵过程，检测系统安全脆弱性。C

A.问卷调查

B.人员访谈

C.渗透性测试

D.手工检查

关于TCP/IP连接过程中的第二次握手中，描述最贴切的是：\_\_\_\_\_\_。B

A.源主机A发给目的的主机序号为1234567，那目的主机回复给源主机的确认序号为1234566。源主机收到目的主机的回复报文并记录下目的的主机序号

B.源主机A发给目的的主机序号为1234567，那目的主机回复给源主机的确认序号为1234568。源主机收到目的主机的回复报文并记录下目的的主机序号

C.源主机A发送给目的主机的序号为1234567，目的主机收到报文后记录该序号

D.源主机A发送给目的主机的序号为1234567，目的主机收到报文后开始建立通讯

计算机信息系统，是指由\_\_\_\_\_\_及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。B

A.计算机硬件

B.计算机

C.计算机软件

D.计算机网络

防火墙最主要被部署在\_\_\_\_\_\_位置。A

A.网络边界

B.骨干线路

C.重要服务器

D.桌面终端

下面有关主键的叙述正确的是\_\_\_\_\_\_。B

A.不同的记录可以具有重复的主键值或空值

B.一个表中的主键可以是一个或多个字段

C.在一个表中主键只可以是一个字段

D.表中的主键的数据类型必须定义为自动编号或文本

3DES在DES的基础上，使用两个56位的密钥K1和K2，发送方用K1加密，K2解密，再用K1加密。接收方用K1解密，K2加密，再用K1解密，这相当于使用\_\_\_\_\_\_倍于DES的密钥长度的加密结果。B

A.1

B.2

C.3

D.6

下面有关DNS安装，正确的是：\_\_\_\_\_\_。B

A.可以安装在Windows2000Professional上

B.DNS属于Windows2000的网络服务

C.安装好DNS后需要授权

D.DNS服务无法和WINS服务共存

在下列有关数字签名作用的叙述中，不正确的是C

A.接收方不能伪造发送方的签名

B.发送方不能否认自己发出的签名消息

C.接收方可以对收到的签名消息进行否认

D.第三者可以确认，但不能伪造这一消息传送过程

采用特征代码法检测计算机病毒的优点是\_\_\_\_\_\_。B

A.速度快

B.误报警率低

C.能检查多态性病毒

D.能对付隐蔽性病毒

下面关于分布式入侵检测系统特点的说法中，错误的是\_\_\_\_\_\_。B

A.检测范围大

B.检测准确度低

C.检测效率高

D.可以协调响应措施

在公钥加密系统中使用的密钥对是\_\_\_\_\_\_。B

A.明文和密文

B.公钥和私钥

C.个人密钥和公钥

D.发送方和接收方

电子商务应用系统主要包括支付网关系统、业务应用系统、用户及终端系统和\_\_\_\_\_\_。A

A.CA系统

B.KDC系统

C.加密系统

D.代理系统