# 1.信息安全包含:（ **物理** ）安全、（ **信息系统** ）安全和（ **数据** ）安全。

# 2.数据安全包含（ **可用性** ）、（ **完整性** ）、（ **保密性** ）三个基本特性。

# 3.公司对电脑密码的强壮度要求是：（ **8位以上**）字母加数字组合

# 4.信息安全四大要素是：（ **技术** ）、（ **制度** ）、（ **流程** ） 、（ **人** ）。

# 5.员工离开自己的计算机时要立即设置（ **锁屏** ）。

# 6.未来信息安全的发展趋势是由（ **防外** ）转变为（ **防内** ）。

# 7.工作人员因工作需要必须使用Internet时，需由各部门信息化管理员提交（ **OA** ）申请。

# 8.密码系统包括以下4个方面：（ **明文空间** ）、（ **密文空间** ）、（ **密钥空间** ）和（ **密码算法** ）。

# 9.解密算法D是加密算法E的（ **逆运算** ）。

# 10.常规密钥密码体制又称为 （ **对称密钥密码体制** ），是在公开密钥密码体制以前使用的密码体制。

# 11.如果加密密钥和解密密钥（ **相同** ），这种密码体制称为对称密码体制。

# 12.RSA算法的安全是基于 （ **分解两个大素数的积** ） 的困难。

# 13.DES算法密钥是（ **64** ）位，其中密钥有效位是（ **56** ）位

# 14.公开密钥加密算法的用途主要包括两个方面：（ **密钥分配** ）、（ **数字签名** ）。

# 15.消息认证是验证信息的完整性，即（ **验证数据在传送和存储过程中是否被篡改、重放或延迟** ）。

# 16.MAC函数类似于加密，它于加密的区别是MAC函数（ **不可逆** ）。

# 17.国际标准化组织中，最重要的两个组织是 （ **IEC** ）和 （ **ISO** ） 。

# 18.信息安全保障的三个要素是（ **人** ）（ **技术** ）和 （ **管理** ）。

# 19.（ **网桥** ）是连接两个协议差别很大的计算机网络时使用的设备。

# 20.远程证明技术主要包括（ **语义** ）、（ **属性** ） 和（ **软件** ）三种。

# 21.可以将安全策略分为（ **管理性** ）安全策略和（ **技术性** ）安全策略。

# 22.认证体系的核心是（ **CA** ）。

# 23.（ **安全运营管理** ）是面向信息系统运行阶段的安全服务产品。

# 24.访问OCSP服务器查询用户证书状态时，OCSP会返回（ **有效** ） 、（ **无效** ）和（ **未知** ）三种状态。

# 25.P2DR的含义是：（ **策略** ） 、（ **保护** ）、（ **探测** ）、（ **反应** ）。

# 26.数据未经授权不能进行更改的特性叫（ **完整性** ） 。

# 27.对消息的所有可能含义进行编码时，所需要最少的比特数，称之为（ **熵** ）。

# 28.把敏感数据转换为不能理解的乱码的过程称为（ **加密** ）；将乱码还原为原文的过程称为（ **解密** ）。

# 29.使用DES对64比特的明文加密，生成（ **64** ）比特的密文。

# 30.将特制的标志隐藏在数字产品之中，用以证明原创作者对作品的所有权的技术，称之为（ **数字水印** ）。

# 31. 在云计算环境下，为避免多租户之间数据泄露风险，常采用(**虚拟化**)技术实现不同租户数据的隔离存储与访问控制。

# 32.（ **SSL** ）工作在传输层，独立于上层应用，为应用提供一个安全的点—点通信隧道

# 33. 常见的网络攻击手段中，通过伪造合法用户身份获取系统权限的攻击方式被称为（**身份假冒**）攻击。

# 34.攻击者对系统进行攻击，以便得到有针对性的信息，攻击主要分为主动攻击和（ **被动** ） 两种。

# 35.计算机病毒检测分为（ **内存** ）检测和（ **磁盘** ）检测。

# 36.Pakistani Brain属于（ **引导区病毒** ）。

# 37.入侵检测系统根据目标系统的类型可以分为基于主机的入侵检测系统和基于（ **网络的入侵检测系统** ）。

# 38.在IPSec中只能提供认证的安全协议是（ **AH** ）。

# 39.覆盖型病毒与前/后附加型病毒的最大区别是（ **是否增加文件长度** ）。

# 40.密码学发展过程中的两大里程碑是（ **DES** ）和（ **RSA** ）。

# 41.PKI的中文全称是（ **公钥基础设施** ）。

# 42.包过滤器工作在OSI的（ **网络** ）层。

# 43.IPSec有（ **隧道模式** ）和（ **传输模式** ）两种工作模式。

# 44.入侵检测系统根据目标系统的类型可以分为基于（ **主机** ）入侵检测系统和基于（ **网络** ）的入侵检测系统。

# 45.当用户收到伪装成银行官方的钓鱼邮件，诱导其点击链接输入账号密码时，这种利用人性弱点实施攻击的方式属于(**社会工程学**)攻击。

# 46.（ **访问控制** ）的目的是为了限制访问主体对访问客体的访问权限。

# 47.恶意代码的基本形式有后门（ **逻辑炸弹** ）、（ **特洛伊木马** ）蠕虫等。

# 48.计算机病毒的工作机制有潜伏机制（ **传染机制** ）和表现机制。

# 49.IPS技术包括基于（ **主机** ）的IPS和基于网络的IPS两大类。51 仅对截获的密文进行分析而不对系统进行任何篡改，此种攻击称为（ **被动** ）攻击。

# 50.密钥管理的主要内容包括密钥的（ **生成** ）、（ **分配** ）、（ **使用** ）、（ **存储** ）、（ **备份** ）、（ **恢复** ）和（ **销毁** ）。

# 51.密钥生成形式有两种：一种是由（ **中心集中** ）生成，另一种是由（ **个人分散** ）生成。

# 52.密钥的分配是指产生并使使用者获得（ **密钥** ）的过程。

# 53.密钥分配中心的英文缩写是（ **KDC** ）。

# 54.防火墙系统的体系结构分为（ **双宿主机体系结构** ）、（ **屏蔽主机体系结构** ）、（ **屏蔽子网体系结构** ）。

# 55.防火墙是位于两个 （ **网络之间** ），一端是 （ **内部网络** ），另一端是 （ **外部网络** ）。

# 56.计算机病毒的5个特征是：（ **主动传染性** ）、（ **破坏性** ）、（ **寄生性（隐蔽性** ） 、（ **潜伏性** ）、（ **多态性** ）。

# 57. 为了防止数据在传输过程中被窃取或篡改，通常会采用（**加密**）技术对数据进行处理，使其变为乱码形式。

# 58.用户在通过ADSL拨号方式上网时，IP地址及相关参数是（ **DHCP服务器** ）分配的。

# 59.TCP SYN泛洪攻击属于一种典型的（ **DOS** ）攻击。

# 60.IP协议提供了（ **尽力而为** ）的传递服务。

# 61.TCP/IP链路层安全威胁有：（ **MAC** ）、ARP）以太网共享信道的侦听

# 62.DRDoS与DDoS的不同之处在于：（ **攻击端不需要占领大量傀儡机** ）

# 63.证书的作用是：（ **用来向系统和其他实体证明自己的身份和攻法功钥** ）

# 64.SSL协议中双方的主密钥是在其（ **握手** ）协议产生的。

# 65.VPN的两种实现形式：（ **LAN-LAN** ） 和（ **Client-LAN** ）

# 66.IPSec是为了在IP层提供通信安全而制定的一套（ **协议簇** ） ，是一个应用广泛、开放的（ **VPN** ） 。

# 67.病毒技术包括：（ **寄生** ）技术 、（ **驻留** ） 技术、（ **加密变形** ）技术 、（ **隐藏** ） 技术。

# 68.防火墙的两种姿态（ **拒绝没有特别与许的任何事情** ） 和（ **允许没有特别拒绝的任何事情** ）。

# 69.TCP/IP层次划分为（ **数据链路** ）层、（ **网络** ）层、（ **传输** ）层、（ **应用** ）层。

# 70.TCP协议的滑动窗口协议的一个重要用途是（ **流量控制** ）。

# 71.诱骗用户把请求发送到攻击者自己建立的服务器上的应用层攻击方法是（ **DNS欺骗** ）。

# 72.身份认证分为： （ **单向认证** ） 和（ **双向认证** ）。

# 73.X.509证书包括：（ **签名算法** ） 、（ **认证内容** ） 和（ **使用签名算法对证书所作的签名** ）三部分。

# 74.防火墙主要通过（ **服务控制** ） 和（ **方向控制** ）、（ **用户控制** ） 和（ **行为控制** ）四种手段来执行安全 策略和实现网络控制访问。

# 75.SOCKS只能用于（ **TCP** ） 服务，而不能用于（ **UDP** ） 服务。

# 76.IPSec定义的两种通信保护机制分别是：（ **ESP** ） 机制和（ **UDP** ）机制。

# 77.在下列括号中填入局域网或广域网（ **局域网** ）通常为一个单位所拥有，（ **广域网** ）限制条件是传输通道的速率，（ **广域网** ）跨越无限的距离，（ **局域网** ）通常使用广播技术来替代存储转发的路由选择。80 虚拟主机服务是指为用户提供（ **域名注册** ）、（ **服务器空间租用** ）和网页设计制作等服务。

# 78.衡量数据通信的主要参数有（ **数据通信速率** ）和（ **误码率** ）。

# 79.IP地址11011011，00001101，00000101，11101110用点分10进制表示可写为（ **4．219，13，5，238** ）。

# 80.综合布线系统可划分为工作区子系统、骨干线子系统、（ **水平布线子系统** ）、管理子系统、（ **设备间子系统** ）和户外子系统。

# 81.任何网络都有以下三个要素，即：共享服务、（ **传输介质** ）和（ **网络协议** ）。

# 82.IP地址分配有动态主机分配协议、（ **自动专用IP地址寻址** ）和（ **手工设置** ）三种IP寻址方式。

# 83.防火墙的组成可以表示成（ **过滤器** ）＋（ **安全策略** ）。

# 84.认证主要包括实体认证和（ **消息认证** ）两大类。

# 85.Intranet分层结构包括网络、（ **服务** ）、应用三个层次。

# 86.在TCP／IP网络中，测试连通性的常用命令是（ **PING** ）。