网络系统管理与维护

Web 代理客户端支持身份验证。√

WSUS 服务的部署方案主要有：单服务器方案和链式方案。√

（ 基于网络流量 ）的计费是根据用户在一段时间内所使用的全部网络流量（发送和接收）统计数据来收取用户费用的一种计费方式。

（ 密码散列 ）函数被设计用来验证和确保数据完整性。

（ 主动测量 ）会向网络中发送特定的探测数据包，网络系统管理员通过对探测数据包所受网络影响而发生特性变化的分析，得到网络状态和性能参数。

（ 重复数据删除 ）可以通过软件或硬件来实现，它把存储的文件切成小块，再比较每个小块的区别，然后对重复的数据块只保留一个副本。

（ tracert ）命令用来跟踪源与目标节点之间的所有路由器。

（ ipconfig ）是 Windows 操作系统中的一个系统命令，用于显示本机的 TCPIP 网络配置值。

（ 特洛伊木马 ）是把自己伪装成为善意应用程序（进程）的恶意软件程序。

（不依赖局域网（LAN-Free）结构 ）是建立在 SAN 基础上的解决方案，是指数据无须通过局域网而直接进行备份。

（ Kerberos ）是一种基于票据（Ticket）的认证方式，其设计目标是通过使用一台中央服务器提供“票据”，而网络中提供资源的服务器和访问资源的客户端之间使用这个“票据”相互识别。

（ NetFlow ）是一种网络监测功能，可以收集流入和流出网络接口的 IP 数据包。

（ 增量备份）是以最近一次备份为基准，对最近一次备份后到进行此种备份的这段时间内，发生变化的数据进行备份。

（差异备份）是以最近一次完全备份为基准，对最近一次完全备份后到进行此种备份的这段时间内，发生变化的数据进行备份。

（钓鱼式攻击）是指入侵者伪装成为某个受信任的网站，如把自己伪装成用户使用的网上银行页面，要求用户更新自己的财务信息，如登录用户名、信用卡号码、消费密码等，进而获得用户的私人数据。

（ 单点测量 ）通常采用便携式测量仪表，在网络中的某个节点上安置测量系统或测量仪表进行测量。

（ 代理服务器）通常设置在企业内部网络中客户端与外部网络中服务器之间，它会暂存客户端发来的请求，并由自己发出这些请求。

(组织单位) 是一种可以对域中的某一部分对象进行单独管理的容器。

（ 引导型）病毒是一种寄生在磁盘引导区的计算机病毒，它用病毒的全部或部分取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其它地方。

（ 管理站）负责向被管理对象发出管理操作指令，并接收来自代理的通告信息。

（ 管理信息库）是一个存储网络管理信息的数据库，由被管理对象组成。

（ SNMP）是一系列网络管理规范的集合，包括：协议、数据结构的定义和一些相关概念，目前已成为网络管理领域中事实上的工业标准。

（代理 ）位于被管理对象中，被管理对象可以是计算机、网络设备、应用程序等。

（ 任务管理器 ）是最简单实用的服务器监视工具。利用它，管理员可以迅速获得简要的系统信息，例如：应用程序、进程、性能、联网和用户等。

（ 软件补丁 ）是一种插入到软件中并能对运行中出现的软件错误进行修改的程序编码，往往是在漏洞被发现后由软件开发商开发和发布的。

（ 协议分析仪 ）允许用户在指定的时间段内以数据包为单位查看指定协议的数据，对这些数据包的原始数据位和字节解码，并能依据其对该数据包所用协议的理解提供综合信息。

（ 引导型 ）病毒是一种寄生在磁盘引导区的计算机病毒，它用病毒的全部或部分取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其它地方

（ 示波器 ）是一种电子设备，用来测量并连续显示信号的电压及信号的波形。

（ 电缆测试仪 ）是针对 OSI 模型的第 1 层设计的，它只能用来测试电缆而不能测试网络的其它设备。

（ 电缆测试仪 ）是针对 OSI 模型的第 1 层设计的，它只能用来测试电缆而不能测试网络的其它设备。

（ WSUS ）是微软公司推出的用于局域网内计算机有关操作系统、应用软件等补丁管理的一种服务器软件，它可以快速、方便地为网络中每台运行 Windows 操作系统的计算机分发操作系统和应用软件的补丁。

“黑客”一词是由英语单词“Cracker”音译而来的，是指专门研究、搜寻计算机漏洞和网络漏洞的计算机爱好者。（ ×）

AH 的 IP 协议号为（ 51 ），提供数据的完整性（MD5、SHA-1）和数据源身份验证，但是不能提供数据保密性功能，所有数据均以明文进行传输。

CHAP 不会在网络上直接传输用户的密码，因此比 PAP 更安全。（ √ ）

CIDF 体系结构中的事件产生器可以是来自网络的数据包，也可以是从系统日志等其他途径得到的信息。（　　）√
CIH 病毒是一种危害性很小的病毒。×
DES 算法比 RSA 算法至少慢 100 倍。（　　）×
ipconfig 命令是个使用频率极高的测试命令，其主要功能是使用 ICMP（Internet Control Message Protocol，网络控制报文协议）数据包来测试从源端到目的端网络的连通性，它可以快速准确地判断网络故障。（　　）×
IPsec 是开放标准的一个框架，包括两个主要协议：（ AH　ESP　）。
IPsec 有两种工作模式：（ 传输　）模式和隧道模式。
IPsec 有两种工作模式：传输模式和隧道模式。（　　）√
ISO 的网络安全体系结构定义了六类安全机制。（　　）×
MD5 和 SHA 属于数据完整性检测方法。（　　）　√
MIB 定义了如何识别被管理对象，以及如何组织被管理对象的信息结构。MIB 中的对象按层次进行分类和命名。（　√　）
NetFlow 通过将数据包中的多个关键字段相结合来定义一个“流”，最初定义了（　七　）个关键字段。
Netscape 公司推出了一个名为（　SSL　）的传输层安全协议，用以保障在 Internet 上数据传输的安全。
netstat 命令用于显示 TCP 连接、当前计算机正在监听的端口、以太网统计信息、IP 路由表、IPv4 统计信息、IPv6 统计信息等。（　　√）
ping 扫描，也称为 TCP 扫描，它可以确定网络中某些设备（如计算机、路由器）是否在线。ping 扫描通常在攻击初期使用。（　×　）
PPP 身份验证方法包括（ PAP　　CHAP　）。
PPP 协议使用 LCP 来建立和维护数据链路连接。借助（NCP　）在同一条点到点连接上使用多种网络层协议。
PPP 协议是一种传输层协议，被设计用于点对点连接中传递数据，使用用户名和密码进行验证，并协调两个设备使用的网络协议。（ ×　）
RC4 属于非对称加密算法。（×　　）
Rivest、Shamir 和 Adleman 对 Diffe-Hellman 的公钥加密算法进行了改进，于 1977 年发明了 RSA 算法。（ √　）
RSA 密钥的长度可以是：（　512 位　1024 位　2048 位　）。
SecureNAT 客户端支持身份验证。×
SNMP 报文主要包括：（GetRequest　）报文、GetNextRequest 报文、SetRequest 报文、GetResponse 报文和 Trap 报文。
SNMP 的 Trap 报文用于代理主动向管理站通告重要事件。（　　）√
SNMP 管理系统通常由 SNMP 管理站、SNMP 代理和（ 管理信息库（MIB）　）组成。
SNMP 协议提供了三类操作，包括：Get、Set 和（ Trap　）。
TCPIP 网络性能指标可以从物理层、数据链路层、（　网络层）、传输层和（　应用层）5 个层次来分析。
TCP 连接的建立与断开采用（ “三次握手+四次断开”　）的方式。
VPN 服务器可以作为 RADIUS 体系中的网络接入服务器。（　　）√
Web 代理客户端不支持 DNS 转发功能。×
Web 代理客户端支持 DNS 转发功能。√
Windows 备份工具支持的备份类型主要有：（正常　）备份、差别备份、增量备份、每日备份等。
Windows 备份工具支持的备份类型主要有：正常备份、（ 差别　）备份、增量备份、每日备份等。
Windows 操作系统内置的 Guest 用户帐户，主要针对临时使用计算机的用户，对操作系统拥有极为有限的访问权限和权利。（ √　）
Windows 操作系统内置的 Users 组帐户的成员属于（标准账户　）帐户。
Windows 操作系统内置了“本地安全策略”功能，可以针对本地主机配置安全策略，管理员使用 secpol.cpl 命令，来打开“本地安全策略”窗口。（　　）×
Windows 操作系统内置了“本地安全策略”功能，可以针对本地主机配置安全策略。（　　）　√
Windows 操作系统中的密码必须符合复杂性要求，定义的帐户密码至少有（　6　）个字符的长度。
Windows 系统内置的（ Administrator　）用户帐户属于管理员帐户。
Windows 自带的备份工具既可以备份本机的系统状态也可以备份远程计算机的系统状态。×
按照防火墙实现的技术不同，可以分为硬件防火墙和软件防火墙。（　　）×
按照网络测量点的位置，可以分为端系统测量和（ 中间系统测量　）。
包过滤防火墙，通常是在网络的入口对通过的数据包进行选择，只有满足条件的数据包才能通过（进入企业内部网络），否则被抛弃。（　　）√

备份管理系统，主要包含（　备份软件　）和备份管理服务器，负责备份策略管理和备份作业监控，以及读取备份客户端的数据并把数据写入备份介质。
备份介质是指备份数据存储的媒介，一般为磁盘阵列、物理磁带库或者虚拟带库、光盘塔、（ 云存储　）。
备份客户端是指需要备份数据的业务主机，它负责提供要备份的数据，一般需安装（ 备份软件客户端代理程序　）。
备份系统的组件包括：备份管理系统、备份客户端、（ 备份网络　）和备份介质。
备份系统的组件包括备份管理系统、备份客户端、备份软件和备份介质。（　　）×
标准帐户通常分配给最终用户使用，适用于日常工作，对操作系统拥有一些基本的权限和权利。（　　）√
病毒是通过磁盘、网络等媒介传播扩散并能够“传染”其他程序的程序。（　　）√
常见的备份工具有（Windows 备份工具 ）。
常见的备份工具有（Ghost ）。
常用的加密算法有对称加密算法和非对称加密算法。（　　）√
常用的数据备份方式有完全备份、差异备份以及（ 增量备份　）。
传输控制协议（Transmission Control Protocol，TCP）是面向数据报文的传输层协议。在基于 TCP 的主动测量过程中，测量主机需要向被测量主机发送探测数据包，但通信双方之间的传输没有明确的连接（类似于邮件传输），通信双方是对等的，单次传输的最大数据量取决于具体的网络。（　　）×
传统的加密系统是以密钥为基础的，这是一种对称加密方法，也就是说，用户使用同一个密钥加密和解密。（　　）√
从 Windows 7 开始，Windows 操作系统才内置了软件防火墙功能。（　　）×
从宏观角度来看，在使用 Kerberos 时，一个客户端需要经过（　3　）个步骤来获取服务。
从数据用途角度来说，一般可将需要备份的数据分为系统数据、基本数据、应用数据、（　临时　）数据。
从网络测量系统的功能角度，网络测量系统的体系结构从底层到高层分别为数据采集层、数据管理层、（ 数据分析层　）和数据表示层。
大部分的网络是基于 TCPIP 协议构建的，网络系统管理员在排除网络故障时，可以参考 TCPIP 协议的分层思想。（ √　）
代理服务器通常设置在企业内部网络中客户端与外部网络中服务器之间，它会暂存客户端发来的请求，并由自己发出这些请求。（ √）
带宽通常表示网络传输路径或链路的传输容量，即数据包的传输速度。（ √ ）
当用户访问计算机系统、应用程序、网络资源时，无需进行身份凭据的验证。（　×　）
电缆测试仪是针对 OSI 模型的第（ 一层　）层设计的。
丢包率是单位时间内传输中丢失的数据包与所有数据包的比值。数据包丢失一般是由网络拥塞引起的，当丢包率超过 15%时，可能会导致网络不可用。（ √）
防火墙不能防止被病毒感染过的程序和文件进出网络。（ √　）
防火墙不能完全消除来自内部网络的威胁，但防火墙能够防止被病毒感染过的程序和文件进出网络。（×　　）
防火墙的部署方案主要有：边缘防火墙 、 三向防火墙和背对背防火墙。
防火墙的处理方式主要包括：Accept、Drop 和（　Reject ）。
防火墙客户端不能安装在（UNIX ）操作系统上。
防火墙客户端不支持身份验证。×
防火墙客户端能够安装在（ Windows Server 2003 ）操作系统上。
防火墙客户端支持 DNS 转发 √
防火墙客户端支持身份验证。 √
访问控制服务，与（访问控制机制）相关。
根据检测对象分类，可以将入侵检测系统分为：基于主机的入侵检测系统 、（基于网络的入侵检测系统）和混合型入侵检测系统。
故障管理（Fault Management）的主要任务是当网络运行出现异常（故障）时，能够迅速找到故障的位置和原因，对故障进行检测、诊断、隔离和纠正，以恢复网络的正常运行。（　　）√
故障管理包括（故障检测）、隔离故障和纠正故障 3 个方面。
管理信息库（Management Information Base，MIB）是一个存储网络管理信息的数据库，由被管理对象组成。（ ）√
管理员审批补丁的方式有：手动审批和自动审批。 √
国际标准 Share78 对灾难恢复解决方案从低到高分为（　七　）种不同层次。
国际标准 Share78 对灾难恢复解决方案从低到高分为多个不同层次，针对每个层次都有相应的容灾方案。其中（ 0 ）级是成本最低的灾难恢复方案（无异地备份）。

国际标准化组织于 1989 年发布了《信息处理系统-开放系统互联-基本参考模型 第 2 部分：安全体系结构》来定义网络安全体系结构。在该体系结构中提出了以下（ 五 ）类安全服务。
缓冲区是指应用程序或操作系统用来保存数据的临时区域。（ ） √
恢复点目标（Recovery Point Object，RPO）是指故障后恢复数据和服务上线所需的时间量。（ ）×
活动目录的优点是：降低总体拥有成本和 单一用户登录 。
活动目录的主要特点有：动态的组织形式、集中管理与分散管理相结合 、资源访问的分级管理等。
基本的网络测试命令有：Ping 命令、Tracert 命令、Show 命令和 Debug 命令等。 √
基础数据分析包括三方面功能：基本统计功能、（ 性能趋势预测 ）和数据关联分析。
基于局域网（LAN-Base）结构是最简单的备份组网方式。在大多数情况下，这种备份是使用服务器主机上自带的备份介质，而备份操作往往也是通过手工操作的方式进行的。（ ）×
基于数据库的复制方式可将远程数据库复制分为实时复制、（ 定时复制）和存储转发复制。
基于主机的入侵检测系统是针对整个网络的入侵检测系统，包括对网络中的所有主机、网络设备进行入侵行为的监测和响应。（ ）×
计费管理的组件包括：计费数据的采集和存储；（ 数据的分析和统计 ）；与用户、管理员之间的人机交互界面。
计费管理可以用来确定网络中每一种服务的价值，包括（硬件）类服务、软件类服务和人工服务。
计费管理为网络资源成本计算和收费提供依据，它记录网络资源的使用情况、提出计费报告、为网络资源的使用核算成本和提供收费依据。（ √ ）
计算机病毒的特征有：可执行性、隐蔽性 和传染性 。
计算机病毒的危害主要表现为：破坏计算机的数据、占用磁盘空间和影响计算机运行速度等。
计算机病毒具有的特征包括：传染性、隐蔽性、潜伏性、（ 破坏性 ）和（针对性 ）。
计算机病毒是一种人为制造的程序，它不会自然产生，而是由精通编程的人精心编制的。（ ） √
计算机病毒危害的“宿主”通常是指正常工作的计算机和网络。（ ） √
加密技术的基本思想是伪装信息，使未授权者不能理解它的真实含义。（ ） √
经典的加密方法，主要包括：替换加密、换位加密和（ 一次性填充）。
经典的加密方法，主要使用了 3 种加密技术：替换加密、换位加密和一次性填充。（ ） √
抗抵赖性服务，主要涉及：数字签名机制、（数据完整性机制）和（ 公证机制 ）。
抗抵赖性服务可防止发送方与接收方在执行各自操作后，否认各自所做的操作。（ ） √
可以使用（Ctrl+Shift+Esc）组合键，打开 Windows 任务管理器。
类似于用户的增减、设备的维修或更新、新技术的应用等事件，属于（配置管理）范畴。
链路带宽是指源节点到目的节点之间性能最低的链路所能达到的最大传输速度，也就是该传输路径所能提供给一个业务流的最大传输速度。×
每年 99.9％的服务可用性意味着数据和服务每年的计划外停机时间不得超过 0.1％，以一年 365 天，每天 24 小时为例，一年的停机时间不得超过（ 8.76 小时 ）。
每年 99.95％的服务可用性意味着数据和服务每年的计划外停机时间不得超过 0.05％，以一年 365 天，每天 24 小时为例，一年的停机时间不得超过（ 4.38 小时 ）。
密码策略用来设置帐户密码的安全性要求，如用户名的使用期限、长度和复杂性。（ ）×
默认时，当父容器的组策略设置与子容器的组策略设置发生冲突时，父容器的组策略设置最终生效。×
目录服务恢复模式仅在域控制器上使用。 √
目录服务恢复模式可以在域中任何一台计算机上使用。×
目录服务恢复模式只能在域控制器上使用。 √
目前，EAP 主要应用在有线局域网方面。（ ）×
目前，最常用的备份介质有磁带、硬盘、光盘、云存储等。（ ） √
目前网络存在的威胁主要表现：非授权访问、信息泄漏、破坏数据完整性、（拒绝服务攻击）和（利用网络传播病毒）。
认证（Authentication）是对用户的身份进行验证，判断其是否为合法用户。授权（Authorization）是对通过认证的用户，授权其可以使用哪些服务。计账（Accounting）是记录用户使用网络服务的资源情况，这些信息将作为计费的依据。（ √ ）
认证服务，主要涉及：加密机制、（数字签名机制）和（ 认证机制）。
如果 KDC 出现故障，那么客户端将无法请求票据并访问网络资源。（ ） √
如果安装了错误的调制解调器驱动程序，Windows 操作系统无法正常启动，那么应该进入（ 安全模式）进行恢复。

如果安装了错误的调制解调器驱动程序，Windows 操作系统无法正常启动，那么应该进入（安全模式 ）进行恢复。
如果没有预先经过同意就擅自使用网络或计算机资源，则被看作非授权访问。（ ）√
如果由于安装了错误的显卡驱动程序或者设置了错误的分辨率而导致无法正常显示的话，则可以选择“启用 VGA 模式”进行修复。√
如果由于安装了错误的显卡驱动程序或者设置了错误的分辨率而导致无法正常显示的话，则可以选择“启用 VGA 模式”进行修复。√
入侵者可以拦截网络中正常的通信数据，并修改和控制通信双方的 TCP 会话，而通信的双方却毫不知情，入侵者就可以使用抓包软件查看双方的通信内容。此种入侵手段被称为（中间人攻击 ）。
入侵者试图通过将数据包的源 IP 伪装成为一个受信任计算机的 IP 地址，并借此访问企业内部网络中的资源。此种入侵手段被称为（ IP 欺骗 ）。
上网行为管理的主要功能包含：（网页访问过滤）、网络应用控制、带宽流量管理、信息收发审计、用户行为分析、上网人员管理。
上网行为管理是指控制和管理用户对网络的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析、上网人员管理等。（ ） √
审核技术能够记录用户使用计算机网络系统进行各种活动的过程，记录系统产生的各类事件。（ ）√
输入 netstat （-n ）命令，则显示活动的 TCP 连接、地址和端口号（以数字形式表示）。
数据包分析工具是一种可以捕获和记录网络数据包的工具，可以帮助网络系统管理员解决网络问题、检查网络安全隐患、显示数据包传输状态、学习网络传输协议。（ ）√
数据保密性服务与公证机制具有相关性。（ ）×
数据管理功能包括基于数据管理和（事件）管理。
数据链路层的故障主要表现在通信双方的（二层 ）封装协议是否一致。
数据链路层负责在网络层与传输层之间进行信息传输，数据帧的封装、解封装、差错校验等。（ ）×
数据完整性服务，主要涉及：数字签名机制、（加密机制）和（数据完整性机制 ）。
特洛伊木马是把自己伪装成为善意应用程序（进程）的恶意软件程序。（ ）√
提供认证、授权和计账功能的标准，包括（RADIUS TACACS ）。
通常可以把网络信息安全的问题划分为物理层、网络层、（数据层 ）和（内容层 ）4 个层面。
通常可以把网络信息安全的问题划分为物理层、网络层、数据层和内容层 4 个层面。（ ）√
通常可以将网络管理系统分为管理站（Manager）和服务器（Server）两部分。（ ） ×
通过上网行为管理产品，网络系统管理员可以实时掌握已连接到网络的设备、用户及位置，为网络资源的合规使用提供支持。具体包括：上网身份管理、上网终端管理、（移动终端管理）和上网地点管理。
通过上网行为管理产品，网络系统管理员可以制定精细的带宽管理策略，对不同岗位的员工、不同网络应用划分带宽通道，并设定优先级，合理利用有限的带宽资源，确保网页下载文件的合法性。（ ）×
通过上网行为管理产品，网络系统管理员可以制定全面的信息收发监控策略，有效控制关键信息的传播范围，避免可能引起的法律风险。具体包括：普通邮件管理、Web 邮件管理、网页发帖管理、（即时通信管理）和其他外发管理。
同步远程复制能够向异地提供最新的数据，但应用程序会因等待写入完成指示而被延迟一段时间。（ ）√
完全备份是在某一个时间点上对所有数据的一个完全复制。这种备份方式的优点是备份速度快，备份数据量较少，没有重复的备份数据。（ ）×
网络测量的功能按照测量对象，可分为三大类：（网络性能测量 业务性能测量 网络流量测量 ）。
网络测量技术的基本要求是有效性、高速测量、准确性和（实时性）。
网络测量是利用测量工具检测网络设备或网络系统运行状态、获取网络性能参数的过程。（ ） √
网络层提供用户服务，如网页服务、电子邮件服务、文件传输服务、域名查询服务等。（ ）×
网络服务故障主要包括 3 个方面：服务器硬件故障、网络操作系统故障和（网络服务故障 ）。
网络故障大致可以分为 4 类，即应用故障、协议故障、操作故障和服务故障。（ ）×
网络故障排查流程：描述网络故障现象、收集可能的网络故障原因信息、（ 建立诊断计划）、网络故障分析、事后记录和总结。
网络故障诊断是以网络原理、网络配置和网络运行的知识为基础，从故障现象入手，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找问题的根源并排除故障，恢复网络正常运行的过程。√
网络故障诊断是以网络原理、网络配置和网络运行的知识为基础，从故障现象入手，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找问题的根源并排除故障，恢复网络正常运行的过程。√

网络管理包括五大功能：故障管理、配置管理、计费管理、性能管理和服务管理，简写为 FCAPS。（　　）×
网络管理员不需要经常对网络系统的各方面性能进行监视。×
网络链路的问题通常是由网卡、跳线、信息插座、交换机、UPS 等设备和服务配置引起的。（　　）×
网络系统管理与维护的基本功能有： 故障管理、配置管理、 性能管理 。
为了支持《信息处理系统-开放系统互联-基本参考模型 第 2 部分：安全体系结构》定义的安全服务，ISO 的网络安全体系结构定义了（　八）类安全机制。
伪装前的原始数据称为密文，伪装后的数据称为密钥，伪装的过程称为加密，加密在加密密钥的控制下进行。（　　）×
系统数据主要是指操作系统、数据库系统安装的各类软件包和应用系统执行程序。（　　）√
性能管理的主要功能包括：性能测量、（性能分析）、性能管理控制和提供性能指标。
性能管理的主要内容是对网络系统资源的吞吐量、使用率、时延、拥塞等系统性能进行分析，实现网络性能的监控和优化。（　　）√
需要经过 4 个会话阶段，才能建立一条完整的 PPP 链路。（ ）×
一旦把内部网络中的计算机配置成为 Web 代理客户端，它们将只能够把本地用户访问 Internet 的（HTTP）对象的请求提交给 ISA Server，由 ISA Server 代为转发。
一个 GPO 可以同时被链接到多个组织单位上。√
异步远程复制对应用程序性能的影响最小，而且异地磁盘系统在数据的更新程度也不会有任何延迟。（　　）×
引导型计算机病毒会影响计算机系统中的可执行文件（.exe）和命令文件(.com)。（　　）×
应用数据主要是指保证业务系统正常运行所使用的系统目录、用户目录、系统配置文件、网络配置文件、应用配置文件、存取权限控制等。（　　）×
与 LAN-Base 结构相比，LAN-Free 结构让多台服务器共享备份介质，备份数据不再经过局域网，而直接从磁盘阵列传到备份介质内。（　　）√
与带宽相关的参数有：链路带宽、瓶颈带宽、（　可用带宽 ）等。
域管理员可以使用（组织单位 ）对域中的某一部分对象进行单独的管理。
灾难恢复体系规划设计包括灾难恢复需求分析、策略制定、技术体系规划、（资源规划）等方面。
灾难恢复需求分析能力包括对风险分析、（业务影响分析）和灾难恢复目标制定 3 个方面，对其分析结果进行评估，以确保企业灾难恢复需求分析的结论符合企业业务恢复要求。
在（分布式测量）体系中，测量节点是完整的测量系统，它们分布在网络中的多个位置，既可以独立地进行网络测量，也可以将测量数据发送到测量中央服务器。
在（ 不依赖服务器（Server-Free）结构 ）中，备份服务器仍参与备份过程，但负担大大减轻，因为它的作用只是指挥，而且不涉及数据的装载和运输，不是主要的备份数据通道。
在 Cisco 公司的交换机上，可以使用 show vlan 命令查看交换机配置的 VLAN 相关信息（　　）√
在 ISO 的网络安全体系结构中定义的安全服务有：（访问控制服务　数据机密性服务　数据完整性服务） 。
在 Windows Server 服务器上的命令提示符窗口中，输入（ wf.msc ），打开“高级安全 Windows 防火墙”窗口。
在 Windows 操作系统的计算机上运行的 ping 命令会发送 4 个 ICMP 回送请求数据包，每个数据包为（ 32 字节）。
在 Windows 操作系统的命令提示符窗口中输入“ping 127.0.0.1”，能够根据响应结果，判断本机的 TCPIP 协议设置是否正常。（ ）√
在 Windows 操作系统的命令提示符窗口中输入 arp-a 命令，会显示所有网卡接口的 ARP 缓存表。（　　）√
在 Windows 操作系统中，（P@s0rd ）能够满足密码的复杂性要求。
在 Windows 资源监视器中，可以查看到的选项卡包括：（概述 ）、（CPU ）、内存、磁盘、（网络 ）。
在安装防火墙时，需要安装（防火墙客户端 ）软件。
在测量单向时延时，首先应该使测量节点 A 和测量节点 B 的时间同步，然后在节点 A 形成一个 64 字节的 UDP 数据包，获取节点 A 的时间后在包头部加载一个时间戳（A）并立即发出，当节点 B 完整地接收到这个数据包后，立即获取接收时间（B），则“B 减 A”的值即为该链路的单向时延。（　　）√
在防火墙的处理方式中，Drop 是指丢弃数据包，并且不通告数据源。（　　）√
在工作组环境中的 Windows 操作系统，可以使用（本地安全策略）管理器来配置本地计算机的安全策略。
在活动目录中，所有被管理的资源信息，例如：用户账户、组账户、计算机账户、甚至是域、域树、域森林等，统称为（ 活动目录对象）。
在设置组策略时，当父容器的组策略设置与子容器的组策略设置没有冲突时，子容器会继承父容器的组策略设置。√
在事件查看器中，（应用程序 ）日志记录应用程序所产生的错误、警告或者提示。例如：如果应用程序执行非法操作，系统会停止运行该应用程序，并把相应的事件记录到相应的日志中。

在事件查看器中，（安全性 ）日志用来记录与网络安全有关的事情。例如：用户登录成功或失败、用户访问 NTFS 资源成功或失败等。
在事件查看器中，（ 系统）日志记录 Windows 操作系统自身产生的错误、警告或者提示。例如：当驱动程序发生错误时，这些事件将被记录到上述日志中。
在一个 Windows 域中，成员服务器的数量为（可有可无 ）。
在一个 Windows 域中，更新组策略的命令为：（ Gpupdate.exe）。
在一个 Windows 域中，可以把链接在一个组织单位上的 GPO 链接到另一个组织单位上。 √
在一个 Windows 域中，域控制器的数量为（ 至少 1 台）。
在一个 Windows 域中，至少需要（ 1 台 ）台域控制器。
在一个域上可以同时链接多个 GPO。 √
在一个域中，计算机的角色有： （域控制器、成员服务器、工作站） 。
在一个域中不能包含组织单位。 ×
在一个组织单位上不可以同时链接多个 GPO。 ×
在一个组织单位上可以同时链接多个 GPO。 √
在一个组织单位中可以包含多个域。 ×
在一个组织单位中可以包含多个域。 ×
在一些大型的备份管理系统中，备份服务管理服务器通常由备份服务器和（介质服务器）组成。
在制定组策略时，可以把组策略对象链接到（域）上。
在制定组策略时，可以把组策略对象链接到（组织单位）上。
在组策略中，计算机策略仅对（计算机账户）生效
在组策略中，用户策略仅对（用户账户）生效。
帐户锁定策略用来设置锁定用户帐户的方式，如（帐户锁定阈值）、帐户锁定的持续时间以及解锁帐户的方法。
帐户锁定时间，用于指定已锁定的帐户在自动解锁之前保持锁定状态的时长。（ ） √
主动测量方法可以利用 TCPIP 协议中的（ICMP）、TCP、UDP 等协议来发送探测数据包进行测量。
住宅的宽带接入服务，当用户订购服务之后，可以按月或按年支付费用，并随意访问 Internet。这种计费方式属于（统一费用）的计费。
状态检测防火墙，又称自动包过滤防火墙。（ ） ×
换位加密能够按照一定的规律重排字母的顺序。例如，以 LUCKY 作为密钥（在字母表中的出现顺序为 34125），对明文 HELLOWORLD 进行加密，会得到密文 LRLLHWEOOD，如下表所示。
密钥 L U C K Y
字母表中的顺序 3 4 1 2 5
明文 H E L L O W O R L D
密文 LR（C 列）LL（K 列）HW（L 列）EO（U 列）OD（Y 列）
请参考上述加密方法，以 TONY 作为密钥，将明文 HAPPYNEWYEAR 转换为密文：PAHP
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【答案选项】A.YY。 B.WR。 C.WY。 D.EA。 E.EN。 F.NE。 DFAB
在一台安装了 Windows 操作系统的服务器 Server3 上，管理员需要创建一个帐户策略，以确保用户密码最长使用期限为 30 天。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】：步骤 1： 步骤 2：在左侧导航栏中，展开“帐户密码” ，然后单击 步骤 3：在右侧窗格中，右击，并单击“属性” 步骤 4：在弹出的对话框中，在文本框中输入，然后单击“确定”。 步骤 5：关闭“本地安全策略”窗口。
【答案选项】 A. 密码最长使用期限。 B.登录服务器 Server3，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。 C.密码策略。 D. 已启用。 E.密码长度最小值。 F.30。BCAF
①访问控制技术 a 对网络系统资源的吞吐量、使用率、时延、拥塞等系统性能进行分析，实现网络性能的监控和优化。②性能管理 b 把自己的程序加入或取代部分操作系统的功能，具有很强的破坏性，可以导致整个系统的瘫痪。③操作系统型病毒 c 采用防火墙等技术将内部网络与外部网络分开，对内部网络进行保护。④内外网隔离技术 d 通过为用户和用户组赋予一定的权限，控制用户和用户组对目录、子目录、文件和其它资源的访问，以及指定用户对这些文件、目录、设备所能够执行的操作。⑤入侵检测 e 对各种入侵行为的发现与报警，是一种通过观察通信行为、根据安全日志或审计数据来检测入侵的技术。 ①： ②： ③： ④： ⑤：

DABCE

①配置管理　a 定期对网络系统进行安全性分析，及时发现网络系统中的薄弱环节和漏洞，最大限度地保证网络系统的安全。②计算机策略 b 组策略的载体③组策略对象 c 在网络建立、扩充、改造和运行的过程中，对网络的拓扑结构、资源配备、使用状态等配置信息进行定义、检测和修改，使其能够提供正常的网络服务。④嵌入型病毒 d 应用于计算机账户的组策略⑤网络漏洞检测技术 e 将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以嵌入方式链接。　　①：　　②：　　③：　　④：　　⑤：

CDBEA

①网络管理　a 负责分析和统计历史数据，建立性能基线和性能分析的模型，预测网络性能的长期趋势。②性能分析 b 规划、监督、控制网络资源的使用和网络的各种活动，以使网络的性能达到最优。③组织单位 c 域中存储活动目录数据库的计算机。④域控制器 d 破坏计算机功能或者数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。⑤计算机病毒 e 一种容器类的活动目录对象。①：　　②：　　③：　　④：　　⑤：

BAECD

在一台安装了 Windows 操作系统的服务器 Server5 上，管理员需要创建一个帐户策略，以实现用户在 30 分钟内输错 5 次密码后，其帐户被自动锁定 30 分钟。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：

步骤 2：在左侧导航栏中，展开“帐户密码”，然后单击

步骤 3：在右侧窗格中，右击，并单击“属性”

步骤 4：在弹出的对话框中，在文本框中输入，然后单击“确定”。在“建议的数值改动”对话框中，单击“确定”。

步骤 5：关闭“本地安全策略”窗口。

【答案选项】　A.帐户锁定阈值。　B.30。　C.帐户锁定策略。　D.登录服务器 Server5，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。　E.5。　F.帐户锁定时间。　DCAE

在一台安装了 Windows 操作系统的域控制器服务器 Server11 上，管理员需要设置 Windows 防火墙属性：将防火墙状态设置为：关闭。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：　步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击。　步骤 3：在弹出的对话框中，在右侧的列表框中，选择，然后单击“确定”。　步骤 4：关闭“高级安全 Windows 防火墙”窗口。

【答案选项】A. 防火墙状态。　B. 阻止。　C. 关闭。　D. 登录服务器 Server11，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。　E. 登录服务器 Server11，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。F. 属性。　DFAC

①故障管理　a 记录用户使用计算机网络系统进行各种活动的过程，记录系统产生的各类事件。②用户策略 b 限制与被管理对象建立联系、限制对被管理对象的操作、控制管理信息的传输。③审计技术 c 应用于用户账户的组策略④源代码病毒 d 攻击高级语言编写的程序，在程序编译前插入到源程序中，经编译成为合法程序的一部分。⑤访问控制 e 当网络运行出现异常（故障）时，能够迅速找到故障的位置和原因，对故障进行检测、诊断、隔离和纠正，以恢复网络的正常运行　　①：　　②：　　③：　　④：　　⑤：

ECADB

备份计算机上 Cmovie 文件夹中的内容，备份类型为：正常备份，备份文件存储在：Cmovie_bk.bkf。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的步骤中，从而把步骤补充完整。【操作步骤】:步骤 1：单击“开始”→“程序”→“附件”→“系统工具”→“备份”。步骤 2：在图中，清除“总是以向导模式启动”复选框，然后单击“高级模式”。步骤 3：在弹出的对话框中，单击【备份向导（高级）】按钮，然后在弹出的“欢迎使用备份向导”窗口中单击【下一步】。步骤 4：　步骤 5：步骤 6：在弹出的窗口中，单击【浏览】按钮，设置备份文件的名称和存储地点。步骤 7：步骤 8：在弹出的窗口中，可以看到备份文件的名称和存储地点。如果没有问题，单击【下一步】。步骤 9：在弹出的窗口，单击【高级】按钮。步骤 10：步骤 11：为了保证备份数据的可靠性，可以选中“备份后验证数据”。然后，单击【下一步】。步骤 12：在这里，选择“替换现有备份”。然后，单击【下一步】。步骤 13：在这里，选择“现在”。然后，单击【下一步】。步骤 14：在“完成向导”画面中，如果确认没有问题，则单击【完成】按钮。【答案选项】:A. 在“选择要备份的类型”处，单击下拉式箭头，选择备份类型。在这里，选择“正常”备份。然后，单击【下一步】。B. 在弹出的窗口中，选择要备份的 Cmovie 文件夹，然后单击【下一步】。C. 在弹出的对话框中，选择存储地点，然后指定备份文件名称。在这里，把文件备份到 Cmovie_bk.bkf 文件中。然后，单击【保存】。D. 在弹出的对话框

中，选择“备份选定的文件、驱动器或网络数据”，然后单击【下一步】。DBCA

假设在域 abc.com 中有一个“研发部”OU，在该 OU 中有 5 个用户账户：user1、user2、user3、user4 和 user5。域管理员需要设置一条组策略，使得“研发部”OU 中的所有用户登录到域以后，在自己的“开始”菜单中找不到“运行”命令。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。【操作步骤】：步骤 1： 步骤 2： 步骤 3： 步骤 4：右击刚刚创建的 GPO，然后在快捷菜单中单击“编辑”。步骤 5： 步骤 6：在对话框中，选中“已启用”，然后单击【确定】。【答案选项】A. 右击“研发部”OU，然后在快捷菜单中单击“创建并链接 GPO”。B. 在组策略编辑窗口中，单击“用户配置”→“管理模板”→“任务栏和[开始]菜单”→双击“从[开始]菜单中删除‘运行’菜单”组策略。C. 在“新建 GPO”画面的“名称”处，为该 GPO 命名，例如：“研发部”OU 的 GPO，然后单击【确定】。D. 单击“开始”→“程序”→“管理工具”→“组策略管理”。

DACB

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中 ①数据保密性服务 a 可以防止对任何资源的非授权访问，确保只有经过授权的实体才能访问相应的资源。②数据完整性服务 b 采用加密手段，防止数据被破解后泄露。③访问控制服务 c 能够确保某个实体身份的可靠性。④认证服务 d 为数据发送方选择安全的网络通信路径，避免发送方使用不安全路径发送数据而受到攻击，以提高数据的安全性。⑤路由控制机制 e 可防止未授权的对数据的修改操作。 ①： ②： ③： ④： ⑤：

BEACD

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中 ①帐户锁定阈值 a 是针对整个网络的入侵检测系统，包括对网络中的所有主机、网络设备进行入侵行为的监测和响应。②泛洪 b 用于指定在用户帐户被锁定之前允许登录失败的次数。③流加密 c 主要是指保证业务系统正常运行所使用的系统目录、用户目录、系统配置文件、网络配置文件、应用配置文件、存取权限控制等。④基础数据 d 是将数据包与密钥生成二进制比特流进行异或运算的加密过程。⑤基于网络的入侵检测系统 e 是指入侵者可以向网络中发送大量的无用数据包，使网络设备（如交换机）满负荷或超负荷运行，导致网络性能下降，甚至瘫痪。 ①： ②： ③： ④： ⑤：

BEDCA

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中

①ICMP a 采用“三次握手+四次断开”的方式来建立与断开连接。②Frame-Realyb 是 TCPIP 协议族中的网络管理协议，定义了传送管理信息的协议消息格式、管理站和代理之间进行消息传送的规则，能对 IP 网络中不同类型的设备进行监控和管理。③TCPc 用于显示本机的 TCPIP 网络配置值。④SNMPd 是 TCPIP 协议族中 IP 层的一个重要协议，提供了差错报告和 IP 设备间重要信息交换的机制，被广泛应用于网络的管理和主动测量方法之中。⑤ipconfige 一种二层数据帧的封装格式。 ①： ②： ③： ④： ⑤：

DEABC

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中

①MD5 a 用于封装多种网络层协议（如 IP、IPX、AppleTalk）报文并通过同一条 PPP 数据链路发送它们。②NCPb 以明文方式发送密码，也就是没有经过加密，因此如果在传输进程中被拦截，密码有可能外泄，比较不安全。③PAPc 默认使用 TCP49 端口，并且对不同的设备采用不同的授权、认证和计账方法。④TACACS+d 是一种单向函数，这使得从给定输入数据计算出散列值很容易，但要从散列值反向计算出输入数据则不可行。⑤SSL 记录协议 e 建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。 ①： ②： ③： ④： ⑤：

DABCE

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中

①TLS a 提供代理服务的计算机或其他网络设备。②IPsecb 是指故障后恢复数据和服务上线所需的时间量。③Proxy Serverc 对 SSL 进行了改进，用于保证 Web 通信以及其他流行协议的安全。④CIDFd 将入侵检测系统分为 4 个组件：事件产生器、事件分析器、事件数据库、响应单元。⑤RTOe 提供的安全功能包括：保密性、完整性、身份验证和安全密钥交换。 ①： ②： ③： ④： ⑤：

CEADB

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中

①蠕虫 a 入侵者可以拦截网络中正常的通信数据，并修改和控制通信双方的 TCP 会话，而通信的双方却毫不知情，入侵者就可以使用抓包软件查看双方的通信内容。②特洛伊木马 b 把自己伪装成为善意应用程序（进程）的恶意软件程序。③中间人攻击 c 是指入侵者可以向网络中发送大量的无用数据包，使网络设备（如交换机）满负荷或超负荷运行，导致网络性能下降，甚至瘫痪。④泛洪 d 入侵者利用或操控企业内部人员，获取他们所需要的信息，包括电话诈骗；试图套出公司员工的名字和口令；伪装成为合法人员。⑤社会工程攻击 e 可以占领计算机的内存空间，以自我复

制的方式从一台计算机通过网络蔓延到另一台计算机。 ①： ②： ③： ④： ⑤：

EBACD

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中

①数字电压表 a 可以在网络中的每一帧中提供应用层、传输层、网络层和数据链路层信息。②时域反射计 b 可用于进行链路连通性测试，可以测量诸如交直流电压、电流、电阻、电容以及电缆连续性等参数，利用这些参数可以检测物理连通性。③电缆测试仪 c 可以对所连接的网络进行网络监视，判断网络运行是否正常，还可以进行协议分析，能够对网络上的协议或者通信问题进行故障诊断。④协议分析仪 d 可用于确定电缆断开的具体位置。通过电缆定时发送脉冲，监听反射回来的信号。⑤网络管理软件 e 针对 OSI 模型的第一层设计的，它只能用来测试电缆而不能测试网络的其他设备。 ①： ②： ③： ④： ⑤：

DBEAC

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中

①替换加密 a 把明文变为一种编码（如 ASCII 编码），选择一个等长的随机字符串作为密钥，对二者进行逐位异或运算（两个值不相同，则异或结果为 1，否则异或结果为 0）得到密文。②换位加密 b 将明文分成 64 位的块，对每个块进行 19 次变换（替换和换位），其中 16 次变换由 56 位的密钥的不同排列形式控制，最后产生 64 位的密文块。③一次性填充 c 用一个字母替换另一个字母。④DESd 按照一定的规律重排字母的顺序。⑤RSAe 其密钥的长度通常是 512 位~2048 位，它的安全性基于大素数分解的困难性。 ①： ②： ③： ④： ⑤：

CDABE

请为选择器①-⑤选择右侧最合适的解释，将配对好的 a-e 填写到括号中

①网络管理 a 负责分析和统计历史数据，建立性能基线和性能分析的模型，预测网络性能的长期趋势。②性能分析 b 是指对网络的运行状态进行监测和控制，使其能够安全、可靠、高效、经济地为客户提供服务。③SNMPc 是一种将企业内部网络与外部网络分离的方法，是在企业内部网络和外部网络之间所施加的安全防范系统。④防火墙 d 是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用，并且能自我复制的一组计算机指令或者程序代码。⑤计算机病毒 e 定义了一系列网络管理规范标准，提供了一个用来监测网络状态、管理配置文件、收集网络数据和检测网络行为的工具。 ①： ②： ③： ④： ⑤：

BAECD

在 ISA Server 上，管理员需要创建发布规则，把内部的 Web 服务器发布出来，以允许外部用户访问。其中，内部的 Web 服务器安装在计算机 PC1（IP 地址：192.168.1.1）上；ISA Server 连接内部的网卡 IP 地址为：192.168.1.200，连接外部的网卡 IP 地址为：131.107.1.200。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。 【操作步骤】：步骤 1： 步骤 2：在“欢迎使用新建 Web 发布规则向导”画面中输入发布规则的名称，例如：发布内部 Web 服务器，然后单击【下一步】。步骤 3：步骤 4：由于只发布一个 Web 网站，所以选择“发布单个网站或负载平衡器”，然后单击【下一步】。步骤 5：在弹出的窗口中，选择 HTTP 方式，然后单击【下一步】。步骤 6：步骤 7：在弹出的窗口中，在“路径”一项保留为空白，即：发布整个网站。然后，单击【下一步】。步骤 8：步骤 9：在弹出的窗口中选择合适的 Web 侦听器，以便通过此侦听器来侦听 Internet 用户的访问请求。步骤 10：由于不需要身份验证，因此选择“无委派，客户端无法直接进行身份验证”，然后单击【下一步】。步骤 11：在弹出的窗口中，保留默认的“所有用户”，然后单击【下一步】。步骤 12：出现“正在完成新建 Web 发布规则向导”画面时，单击【完成】按钮。【答案选项】A. 在弹出的窗口中的“公用名称”中输入：131.107.1.200，以便让外部用户通过此 IP 地址来访问内部网站。然后，单击【下一步】。B. 在“规则操作”窗口中，选择“允许”，然后单击【下一步】。C. 在弹出的窗口中输入 PC1 的 IP 地址：192.168.1.1。然后，单击【下一步】。D. 在 ISA Server 的管理控制台中，单击左窗格中的“防火墙策略”，然后单击任务窗格的“任务”选项卡，接着单击“发布网站”。

DBCA

在 ISA Server 上，管理员需要创建发布规则，以允许外部用户访问内部的电子邮件服务器，执行收发邮件的工作。其中，内部的邮件服务器安装在计算机 PC1（IP 地址：192.168.1.1）；ISA Server 连接内部的网卡 IP 地址为：192.168.1.200，连接外部的网卡 IP 地址为：131.107.1.200。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。 【操作步骤】：步骤 1：步骤 2：在“欢迎使用新建邮件服务器发布规则向导”画面中输入发布规则的名称，例如：发布内部邮件服务器，然后单击【下一步】。步骤 3： 步骤 4：步骤 5：在弹出的窗口中指定内部邮件服务器的 IP 地址，这里应该输入 PC1 的 IP 地址：192.168.1.1，然后单击【下一步】。步骤 6： 步骤 7：出现“正在完成新建邮件服务器发布规则向导”画面时，单击【完成】。【答案选项】A. 由于希望外部的客户端通过 SMTP 和 POP3 的标准端口来访问内部邮件服务器，所以在弹出的窗口中选择“POP3（standard port）”和“SMTP（standard port）”，然后单击【下一步】。B. 在弹出的窗口中，选择“外部”网络，然后单击【地址】按钮。然后，在弹出的窗口中选择“在

此网络上选择的 IP 地址”，从“可用的 IP 地址”中选择一个 IP 地址（即：131.107.1.200），然后单击【添加】按钮，把该地址添加到右侧的“选择的 IP 地址”栏中，再按【确定】按钮即可。C. 由于希望外部的客户端（而并非外部的邮件服务器）来访问内部邮件服务器，所以在弹出的窗口中选择“客户端访问：RPC、IMAP、POP3、SMTP”，然后单击【下一步】。D. 在 ISA Server 的管理控制台中，单击左窗格中的“防火墙策略”，然后单击任务窗格的“任务”选项卡，接着单击“发布邮件服务器”。

DCAB

在 ISA Server 上创建“允许传出的 Ping 流量”的访问规则，从而允许内部网中的用户可以使用 Ping 命令去访问外部网中的计算机。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。【操作步骤】：步骤 1：步骤 2：在“欢迎使用新建访问规则向导”画面中输入访问规则的名称，例如：允许传出的 Ping 流量，然后单击【下一步】。步骤 3：步骤 4：在“协议”窗口中，单击下拉式箭头，选择“所选的协议”。步骤 5：步骤 6：步骤 7：步骤 8：在“用户集”的画面中，选择 “所有用户”。接着，单击【下一步】。步骤 9：在“正在完成新建访问规则向导”画面中，单击【完成】。步骤 10 ：在弹出的警告窗口中，单击【应用】按钮，使该访问规则生效。

【答案选项】A. 在“规则操作”窗口中，选择“允许”，然后单击【下一步】。B. 单击【添加】按钮来添加协议，单击“通用协议”，从中选择“PING”，然后单击【添加】按钮。接着，单击【下一步】。C. 在 ISA Server 的管理控制台中，单击左窗格中的“防火墙策略”，然后单击任务窗格的“任务”选项卡，接着单击“创建访问规则”。D. 在“访问规则目标”的画面中，单击“网络”，从中选择“外部”，然后单击【添加】按钮。接着，在左图中单击【下一步】。E. 在“访问规则源”的画面中，单击“网络”，从中选择“内部”，然后单击【添加】按钮。接着，单击【下一步】。

CABED

在一台安装了 Windows 操作系统的服务器 Server12 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server12）上的 iSCSI 服务。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：

步骤 2：在左侧导航栏中，右击“入站规则”并单击“新建规则”。

步骤 3：在“规则类型”对话框中，选择选项，并在列表框中选择“iSCSI 服务”，单击“下一步”。

步骤 4：在“规则”对话框中，勾选选项，然后单击“下一步”。

步骤 5：

【答案选项】

A. 在“操作”对话框中，选中“阻止连接”选项，单击“完成”。

B. 在“名称”对话框中，输入规则名称后，单击“完成”。

C. 预定义。

D. 登录服务器 Server12，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。

E. 登录服务器 Server12，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。

F. iSCSI 服务。

ECFA

在一台安装了 Windows 操作系统的服务器 Server14 上，管理员需要创建一个防火墙规则：仅拒绝此服务器（Server14）访问任何远程计算机的 TCP53 端口。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：

步骤 2：在左侧导航栏中，右击“出站规则”并单击“新建规则”。

步骤 3：在“规则类型”对话框中，选择选项，单击“下一步”。

步骤 3：在“协议和端口”对话框中，选择“TCP”，在右侧的文本框中输入 53，然后单击“下一步”。

步骤 4：在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。

步骤 5：在“配置文件”对话框中，单击“下一步”。

步骤 6：

【答案选项】

A. 特定远程端口。
B. 在“名称”对话框中，输入规则名称后，单击“下一步”。
C.所有远程端口。
D. 登录服务器 Server14，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
E. 登录服务器 Server14，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 端口。
DFAB
在一台安装了 Windows 操作系统的服务器 Server1 上，管理员需要创建一个帐户策略，以确保用户必须使用复杂的密码。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：
步骤 2：在左侧导航栏中，展开“帐户密码”-
步骤 3：在右侧窗格中，右击，并单击“属性”
步骤 4：在弹出的对话框中，选中选项，然后单击“确定”。
步骤 5：关闭“本地安全策略”窗口。
【答案选项】
A.密码必须符合复杂性要求。
B.登录服务器 Server1，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。
C.密码策略。
D.已禁用。
E.密码长度最小值。
F.已启用。
BCAF
在一台安装了 Windows 操作系统的服务器 Server2 上，管理员需要创建一个帐户策略，以确保用户密码长度最小值为 8 字符。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：
步骤 2：在左侧导航栏中，展开“帐户密码”-
步骤 3：在右侧窗格中，右击，并单击“属性”
步骤 4：在弹出的对话框中，在文本框中输入，然后单击“确定”。
步骤 5：关闭“本地安全策略”窗口。
【答案选项】
A.密码长度最小值。
B.登录服务器 Server2，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。
C.密码策略。
D. 已启用。
E. 密码必须符合复杂性要求。
F.8。
BCAF
在一台安装了 Windows 操作系统的服务器 Server4 上，管理员需要创建一个帐户策略，以确保用户密码最短使用期限为 1 天。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:

步骤 1：　步骤 2：在左侧导航栏中，展开“帐户密码” ，然后单击
步骤 3：在右侧窗格中，右击，并单击“属性” 步骤 4：在弹出的对话框中，在文本框中输入，然后单击“确定”。
步骤 5：关闭“本地安全策略”窗口。
【答案选项】
A. 密码最短使用期限。
B.登录服务器 Server4，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。　C.密码策略。　D. 已启用。　E.密码长度最小值。 F.1。
BCAF
在一台安装了 Windows 操作系统的服务器 Server6 上，管理员需要创建一个帐户策略，以实现用户在 20 分钟内输错 7 次密码后，其帐户被自动锁定 20 分钟。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：登录服务器 Server6，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。
步骤 2：在左侧导航栏中，展开“帐户密码” ，然后单击“帐户锁定阈值”。
步骤 3：在右侧窗格中，右击，并单击“属性”
步骤 4：在弹出的对话框中，在文本框中输入，然后单击“确定”。在“建议的数值改动”对话框中，单击“确定”。
步骤 5：在右侧窗格中，右击，并单击“属性”。
步骤 6：在弹出的对话框中，在文本框中输入，然后单击“确定”。在“建议的数值改动”对话框中，单击“确定”。
步骤 7：关闭“本地安全策略”窗口。
【答案选项】
A.帐户锁定阈值。
B.20。
C.帐户锁定策略。
D.登录服务器 Server6，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。
E.7。
F.帐户锁定时间。
AEFB
在一台安装了 Windows 操作系统的服务器 Server7 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server7）的 80 端口。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：
步骤 2：在左侧导航栏中，右击“入站规则”并单击“新建规则”。在“规则类型”对话框中，选择“自定义”选项，单击“下一步”。
步骤 3：在“程序”对话框中，单击“下一步”。
步骤 4：
步骤 5：在“作用域”对话框中，在“此规则应用于哪些本地 IP 地址”选项下方，选中“下列 IP 地址”选项，在下方文本框中输入服务器 Server7 的 IP 地址，然后单击“添加”；在“此规则应用于哪些远程 IP 地址”选项下方，选中“任何 IP 地址”选项，然后单击“下一步”。
步骤 6：
步骤 7：在“配置文件”对话框中，单击“下一步”。
步骤 8：
【答案选项】
A. 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。
B. 在“名称”对话框中，输入规则名称后，单击“下一步”。
C. 在“协议和端口”对话框中，选择“协议类型：TCP”、“本地端口：特定端口、80”，单击“下一步”。
D. 登录服务器 Server7，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。

E. 登录服务器 Server7，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
F. 在“协议和端口”对话框中，选择“协议类型：TCP”、“远程端口：特定端口、80”，单击“下一步”。
ECAB
在一台安装了 Windows 操作系统的服务器 Server8 上，管理员需要创建一个防火墙规则：拒绝此服务器（Server8）访问任何远程计算机的 443 端口的访问。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：
步骤 2：在左侧导航栏中，右击“出站规则”并单击“新建规则”。在“规则类型”对话框中，选择“自定义”选项，单击“下一步”。
步骤 3：在“程序”对话框中，单击“下一步”。
步骤 4：
步骤 5：在“作用域”对话框中，单击“下一步”。
步骤 6：
步骤 7：在“配置文件”对话框中，单击“下一步”。
步骤 8：
【答案选项】
A. 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。
B. 在“名称”对话框中，输入规则名称后，单击“下一步”。
C. 在“协议和端口”对话框中，选择“协议类型：TCP”、“本地端口：特定端口、443”，单击“下一步”。
D. 登录服务器 Server8，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
E. 登录服务器 Server8，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 在“协议和端口”对话框中，选择“协议类型：TCP”、“远程端口：特定端口、443”，单击“下一步”。
DFAB
在一台安装了 Windows 操作系统的域控制器服务器 Server10 上，管理员需要设置 Windows 防火墙属性：将日志文件的保存路径设置为 Dfwfw.log。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击。
步骤 3：在弹出的对话框中，单击右侧的“自定义”。
步骤 4：在弹出的对话框中，在右侧的文本框中输入“Dfwfw.log”，然后单击“确定”。
步骤 5：返回上一级对话框，单击“确定”。
步骤 6：关闭“高级安全 Windows 防火墙”窗口。
【答案选项】
A. 日志。
B. 名称。
C. 设置。
D. 登录服务器 Server10，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。

E. 登录服务器 Server10，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 属性。
DFAB

第 1 章　概述

判断题：

1. 网络系统管理是指对网络的运行状态进行监测和控制，使其能够安全、可靠、高效、经济地为客户提供服务。（　　）T
2. 通常可以将网络管理系统分为管理站（Manager）和服务器（Server）两部分。（　　）F
3. MIB定义了如何识别被管理对象,以及如何组织被管理对象的信息结构。MIB中的对象按层次进行分类和命名。（　　）T
4. 网络管理包括五大功能：故障管理、配置管理、计费管理、性能管理和服务管理，简写为 FCAPS。（　　）F
5. 故障管理（Fault Management）的主要任务是当网络运行出现异常（故障）时，能够迅速找到故障的位置和原因，对故障进行检测、诊断、隔离和纠正，以恢复网络的正常运行。（　　）T
6. 配置管理主要负责创建、检测和控制网络的配置状态。（　　）T
7. 计费管理为网络资源成本计算和收费提供依据，它记录网络资源的使用情况、提出计费报告、为网络资源的使用核算成本和提供收费依据。（　　）T
8. 性能管理的主要内容是对网络系统资源的吞吐量、使用率、时延、拥塞等系统性能进行分析，实现网络性能的监控和优化。（　　）T
9. ISO 的网络安全体系结构定义了六类安全机制。（　　）F
10. 身份验证，属于配置管理的主要功能。（　　）F
11. SNMP 的 Trap 报文用于代理主动向管理站通告重要事件。（　　）T
12. 审核技术能够记录用户使用计算机网络系统进行各种活动的过程，记录系统产生的各类事件。（　　）T
13. SNMP 的 Trap 报文由代理主动发给管理站，并且需要管理站的响应。（　　）F
14. 管理信息库（Management Information Base，MIB）是一个存储网络管理信息的数据库，由被管理对象组成。（　　）F

单选题：

1. （　　）负责向被管理对象发出管理操作指令，并接收来自代理的通告信息。A
   A.管理站　　B.代理　　C.管理信息库　　D.SNMP
2. （　　）是一个存储网络管理信息的数据库，由被管理对象组成。C
   A.管理站　　B.代理　　C.管理信息库　　D.SNMP
3. 类似于用户的增减、设备的维修或更新、新技术的应用等事件，属于（　　）范畴。C
   A.故障管理　　B.计费管理　　C.配置管理　　D.安全管理
4. SNMP 管理系统通常由 SNMP 管理站、SNMP 代理和（　　）组成。C
   A.管理者　　B.托管对象　　C. 管理信息库（MIB）　　D.网络数据库

多选题：

1. 目前最常用的网络管理协议包括（　　）、（　　）和（　　），它们广泛地应用于网络管理解决方案中。ABD
   A.CMIP　　B.CMIS　　C.ICMP　　D.SNMP　　E.SSTP
2. 网络管理包括五大功能：故障管理、配置管理、计费管理、（　　）和（　　）。BD
   A.动态管理　　B.性能管理　　C.服务管理　　D.安全管理　　E.质量管理
3. SNMP 使用（　　）和（　　）端口。AC
   A.UDP161　　B.TCP161　　C.UDP162　　D.TCP162　　E.ICMP161
4. 在 ISO 的网络安全体系结构中定义了 5 类安全服务，包括：认证服务、访问控制服务、数据保密性服务、（　　）和（　　）。BD
   A.权限管理服务　　B. 数据完整性服务　　C.加密服务　　D. 抗抵赖性服务　　E.网络服务

第 2 章　网络用户配置管理

判断题：

1. 当用户访问计算机系统、应用程序、网络资源时，无需进行身份凭据的验证。（　　）F
2. Windows 操作系统内置的 Guest 用户帐户，主要针对临时使用计算机的用户，对操作系统拥有极为有限的访问权限和权利。（　　）T
3. Windows 操作系统内置的 Administrator 用户帐户，可以执行本台计算机的所有管理工作，如创建/更改/删除用户帐户、设置用户帐户的权限和权利、更改计算机名称、设置安全策略、管理硬件设备、管理文件系统等。（　　）T
4. 标准帐户通常分配给最终用户使用，适用于日常工作，对操作系统拥有一些基本的权限和权利。（　　）T
5. 密码策略用来设置帐户密码的安全性要求，如用户名的使用期限、长度和复杂性。（　　）F
6. 帐户锁定时间，用于指定已锁定的帐户在自动解锁之前保持锁定状态的时长。（　　）T
7. 上网行为管理是指控制和管理用户对网络的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析、上网人员管理等。（　　）T
8. 通过上网行为管理产品，网络系统管理员可以制定精细的带宽管理策略，对不同岗位的员工、不同网络应用划分带宽通道，并设定优先级，合理利用有限的带宽资源，确保网页下载文件的合法性。（　　）F
9. Windows 操作系统内置了“本地安全策略”功能，可以针对本地主机配置安全策略，管理员使用 secpol.cpl 命令，来打开“本地安全策略”窗口。（　　）F
10. Windows 操作系统内置了“本地安全策略”功能，可以针对本地主机配置安全策略。（　　）T

单选题：

1. Windows 系统内置的（　）用户帐户属于管理员帐户。A
   A. Administrator　　B.Power User　　C.root　　D.su
2. Windows 操作系统内置的 Users 组帐户的成员属于（　　）帐户。B
   A.管理员帐户　　B.标准账户　　C.来宾帐户　　D.匿名帐户
3. Windows 操作系统中的密码必须符合复杂性要求，定义的帐户密码至少有（　　）个字符的长度。C
   A.4　　B.5　　C.6　　D.7
4. 在 Windows 操作系统中，（　　）能够满足的密码必须符合复杂性要求。B
   A.1234ASDF　　B.P@sOrd　　C.1@qF　　D.11223344qqaassdd
5. 帐户锁定策略用来设置锁定用户帐户的方式，如（　　）、帐户锁定的持续时间以及解锁帐户的方法。D
   A.帐户密码历史　　B.帐户禁用期限　　C.帐户激活次数　　D.帐户锁定阈值
6. 在工作组环境中的 Windows 操作系统，可以使用（　　）管理器来配置本地计算机的安全策略。A
   A.本地安全策略　　B.安全策略　　C.系统安全策略　　D.本地策略
7. 上网行为管理的主要功能包含：（　　）、网络应用控制、带宽流量管理、信息收发审计、用户行为分析、上网人员管理。B
   A.网络线缆使用审核　　B. 网页访问过滤　　C.操作系统登录管理　　D.应用程序卸载控制
8. 通过上网行为管理产品，网络系统管理员可以实时掌握已连接到网络的设备、用户及位置，为网络资源的合规使用提供支持。具体包括：上网身份管理、上网终端管理、（　　）和上网地点管理。D
   A.搜索引擎管理　　B. 文件下载管理　　C. 上网带宽管理　　D. 移动终端管理
9. 通过上网行为管理产品，网络系统管理员可以制定全面的信息收发监控策略，有效控制关键信息的传播范围，避免可能引起的法律风险。具体包括：普通邮件管理、Web 邮件管理、网页发帖管理、（　　）和其他外发管理。C
   A.网页正文管理　　B.操作系统登录管理　　C. 即时通信管理　　D.上网应用阻断管理

多选题：

1. 在基于 Windows 操作系统的计算机上，可以将帐户大体划分为哪三种类型？（　　）ABC
   A.管理员帐户　　B.标准账户　　C.来宾帐户　　D.匿名帐户　　E.测试帐户
2. 通过上网行为管理产品，网络系统管理员可以实时了解、统计、分析 Internet 使用状况，并根据分析结果对管理策略做出调整和优化。具体包括（　　）。ACE
   A.上网行为实时监控　　B.上网带宽控制　　C.上网行为日志查询
   D.上网行为统计分析　　E.上网应用累计时长限额

第 3 章　网络安全

判断题：

1. 通常可以把网络信息安全的问题划分为物理层、网络层、数据层和内容层 4 个层面。（　）T
2. 物理层安全是指对网络与信息系统的运行状态的保护，主要关注的是信息系统的安全。（　）F
3. 如果没有预先经过同意就擅自使用网络或计算机资源，则被看作非授权访问。（　）T
4. 拒绝服务攻击会不断对网络服务系统进行干扰，改变其正常的运行流程，执行无关应用程序，大量消耗硬件资源，使系统响应减慢，甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能得到已经授权的服务。（　）T
5. 数据保密性服务可防止未授权的对数据的修改操作。（　）F
6. 抗抵赖性服务可防止发送方与接收方在执行各自操作后，否认各自所做的操作。（　）T
7. 常用的加密算法有对称加密算法和非对称加密算法。（　）T
8. 数字签名是保证数据完整性和抗抵赖性的一种重要手段。（　）T
9. 数据保密性服务与公证机制具有相关性。（　）F
10. 病毒是通过磁盘、网络等媒介传播扩散并能够“传染”其他程序的程序。（　）T
11. 计算机病毒是一种人为制造的程序，它不会自然产生，而是由精通编程的人精心编制的。（　）T
12. “黑客”一词是由英语单词“Cracker”音译而来的，是指专门研究、搜寻计算机漏洞和网络漏洞的计算机爱好者。（　）F
13. 计算机病毒的整个生命周期一般由四个阶段组成，即：潜伏阶段、传播阶段、发作阶段和破坏阶段。（　）F
14. 基于计算机病毒的感染途径，可以将计算机病毒分为文件型计算机病毒、引导型计算机病毒和宏病毒。（　）T
15. 引导型计算机病毒会影响计算机系统中的可执行文件（.exe）和命令文件(.com)。（　）F
16. 宏病毒，是一种寄存于文档或模板的宏中的计算机病毒。（　）T
17. 在防火墙的处理方式中，Drop是指丢弃数据包，并且不通告数据源。（　）T
18. 在防火墙的处理方式中，Receive是指允许数据包通过。（　）F
19. 根据防火墙的功能，网络系统管理员可以基于数据包的源地址、目标地址，来阻止或允许进出企业内部网络的数据包。（　）T
20. 根据防火墙的功能，网络系统管理员不可以基于数据包的源端口、目标端口，来阻止或允许进出企业内部网络的数据包。（　）F
21. 软件防火墙（也称为基于主机的防火墙）一般是安装在计算机上的软件，执行与硬件防火墙相同或类似的功能。（　）T
22. 按照防火墙实现的技术不同，可以分为硬件防火墙和软件防火墙。（　）F
23. 包过滤防火墙，通常是在网络的入口对通过的数据包进行选择，只有满足条件的数据包才能通过（进入企业内部网络），否则被抛弃。（　）T
24. 应用层防火墙，也称为代理。它接受来自内部网络用户的通信，然后与外部网络服务器建立单独连接，而不允许内部网络与外部网络直接通信，它在应用层的通信中扮演着一个消息传递者的角色。（　）T
25. 状态检测防火墙，又称自动包过滤防火墙。（　）F
26. 从 Windows 7 开始，Windows 操作系统才内置了软件防火墙功能。（　）F
27. 防火墙不能防止被病毒感染过的程序和文件进出网络。（　）T
28. 可以在 Windows 操作系统内置的“高级安全 Windows 防火墙”窗口中配置防火墙的入站规则和出站规则。（　）T
29. 防火墙不能完全消除来自内部网络的威胁，但防火墙能够防止被病毒感染过的程序和文件进出网络。（　）F
30. 入侵检测就是对各种入侵行为的发现与报警，是一种通过观察通信行为，根据安全日志或审计数据来检测入侵的技术。（　）T
31. 特洛伊木马是把自己伪装成为善意应用程序（进程）的恶意软件程序。（　）T
32. 缓冲区是指应用程序或操作系统用来保存数据的临时区域。（　）T
33. ping 扫描，也称为 TCP 扫描，它可以确定网络中某些设备（如计算机、路由器）是否在线。ping 扫描通常在攻击初期使用。（　）F
34. CIDF 体系结构中的事件产生器可以是来自网络的数据包，也可以是从系统日志等其他途径得到的信息。（　）T
35. 基于主机的入侵检测系统是针对整个网络的入侵检测系统，包括对网络中的所有主机、网络设备进行入侵行为的监测和响应。（　）F
36. 基于主机的入侵检测系统只关注主机上发生的入侵事件，而不会监测网络上的情况。（　）T
37. 加密技术的基本思想是伪装信息，使未授权者不能理解它的真实含义。（　）T
38. 伪装前的原始数据称为密文，伪装后的数据称为密钥，伪装的过程称为加密，加密在加密密钥的控制下进行。（　）F

39. 传统的加密系统是以密钥为基础的，这是一种对称加密方法，也就是说，用户使用同一个密钥加密和解密。（　　）T
40. 经典的加密方法，主要使用了 3 种加密技术：替换加密、换位加密和一次性填充。（　　）T
41. DES（Data Encryption Standard，数据加密标准）制定于 1977 年，它将明文分成 64 位的块，对每个块进行变换（替换和换位）。（　　）T
42. RC4 属于非对称加密算法。（　　）F
43. Rivest、Shamir 和 Adleman 对 Diffe-Hellman 的公钥加密算法进行了改进，于 1977 年发明了 RSA 算法。（　　）T
44. DES 算法比 RSA 算法至少慢 100 倍。（　　）F
45. 数据完整性的检测方法是基于一种单向的数学函数（散列函数），这种函数相对来说易于计算，而且也容易作逆运算。（　　）F
46. 散列值只被用于提供数据完整性。（　　）T
47. MD5 和 SHA 属于数据完整性检测方法。（　　）T
48. PPP 协议是一种传输层协议，被设计用于点对点连接中传递数据，使用用户名和密码进行验证，并协调两个设备使用的网络协议。（　　）F
49. 发起 PPP 连接后，链路将经过 4 个会话建立阶段。（　　）F
50. CHAP 不会在网络上直接传输用户的密码，因此比 PAP 更安全。（　　）T
51. 认证（Authentication）是对用户的身份进行验证，判断其是否为合法用户。授权（Authorization）是对通过认证的用户，授权其可以使用哪些服务。计账（Accounting）是记录用户使用网络服务的资源情况，这些信息将作为计费的依据。（　　）T
52. 认证服务器和票据授予服务器构成了密钥分发中心。（　　）T
53. 代理服务器通常设置在企业内部网络中客户端与外部网络中服务器之间，它会暂存客户端发来的请求，并由自己发出这些请求。（　　）T
54. 通常情况下，代理服务有利于保障网络终端的隐私或安全，防止源自内部的攻击。（　　）F
55. 计算机病毒危害的“宿主”通常是指正常工作的计算机和网络。（　　）T
56. VPN 服务器可以作为 RADIUS 体系中的网络接入服务器。（　　）T
57. 如果 KDC 出现故障，那么客户端将无法请求票据并访问网络资源。（　　）T
58. 目前，EAP 主要应用在有线局域网方面。（　　）F
59. IPsec 是一个建立在网络层之上的企业私有协议。（　　）F
60. IPsec 有两种工作模式：传输模式和隧道模式。（　　）T

单选题：

1. 通常可以把网络信息安全的问题划分为物理层、网络层、数据层和（　　）4 个层面。A
   A.内容层　　B.应用层　　C.数据层　　D.传输层
2. （　　）安全是指对信息在数据处理、存储、传输、显示等使用过程中的保护，主要关注的是数据信息本身的安全，保障数据依据授权使用，而不被窃取、篡改、冒充、抵赖。其主要涉及数据的保密性、完整性、真实性、不可抵赖性等。B
   A.内容层　　B.数据层　　C.会话层　　D.传输层
3. 国际标准化组织于 1989 年发布了《信息处理系统-开放系统互联-基本参考模型 第 2 部分：安全体系结构》来定义网络安全体系结构。在该体系结构中提出了以下（　　）类安全服务。C
   A.六　　B.三　　C.五　　D.七
4. 认证服务能够确保某个实体身份的可靠性，可分为两种类型。一种认证服务类型是认证实体本身的身份，确保其真实性，称为实体认证。另一种认证服务类型是证明某个信息是否来自某个特定的实体，这种认证称为（　　）。D
   A.数据认证　　B.元数据认证　　C.信息认证　　D. 数据源认证
5. 为了支持《信息处理系统-开放系统互联-基本参考模型 第 2 部分：安全体系结构》定义的安全服务，ISO 的网络安全体系结构定义了（　　）类安全机制。A
   A.八　　B.七　　C.五　　D.三
6. 计算机病毒的整个生命周期一般由四个阶段组成，包括：潜伏阶段、传播阶段、（　　）和发作阶段。C
   A.散发阶段　　B.隐藏阶段　　C.触发阶段　　D.破坏阶段
7. 如果继续使用厂商不再支持的操作系统，就会存在非常严重的安全风险。以微软的 Windows 生命周期为例，客户端操作系统的生命周期一般为（　　）年。B
   A.六　　B.十　　C.五　　D.八

8. 防火墙的处理方式主要包括：Accept、Drop 和（　　）。C
A.Allow　　B.Deny　　C.Reject　　D. Receive
9. 边缘网络也称为（　　），位于内部防火墙与外部防火墙之间，受保护强度较低，一般用于放置面向 Internet 的服务设备，这些设备需要接受来自互联网的用户访问。D
A.Internet　　B.External　　C.Internal　　D. DMZ
10. 按照防火墙实现的技术不同，可以分为包过滤防火墙、（　　）防火墙、电路层防火墙、状态检测防火墙。B
A.数据层　　B.应用层　　C.传出层　　D.无状态
11. （　　）是把自己伪装成为善意应用程序（进程）的恶意软件程序。D
A.骇客　　B.黑客　　C.蠕虫　　D.特洛伊木马
12. 入侵者试图通过将数据包的源 IP 伪装成为一个受信任计算机的 IP 地址，并借此访问企业内部网络中的资源。此种入侵手段被称为（　　）。A
A.IP 欺骗　　B.ARP 欺骗　　C.泛洪攻击　　D.拒绝服务攻击
13. 入侵者可以拦截网络中正常的通信数据，并修改和控制通信双方的 TCP 会话，而通信的双方却毫不知情，入侵者就可以使用抓包软件查看双方的通信内容。此种入侵手段被称为（　　）。C
A.IP 欺骗　　B.端口扫描　　C.中间人攻击　　D.缓冲器溢出
14. （　　）是指入侵者伪装成为某个受信任的网站，如把自己伪装成用户使用的网上银行页面，要求用户更新自己的财务信息，如登录用户名、信用卡号码、消费密码等，进而获得用户的私人数据。D
A.社会工程攻击　　B.泛洪攻击　　C.中间人攻击　　D. 钓鱼式攻击
15. 美国国防部高级研究计划局提出的通用入侵检测框架将入侵检测系统分为四个组件，包括：事件产生器、事件分析器、（　　）和响应单元。B
A.事件查看器　　B.事件数据库　　C.入侵检测器　　D. 网络收集器
16. 根据检测对象分类，可以将入侵检测系统分为：基于主机的入侵检测系统 、（　　）和混合型入侵检测系统。A
A.基于网络的入侵检测系统　　B.基于存储的入侵检测系统
C.基于用户的入侵检测系统　　D.基于应用程序的入侵检测系统
17. 在一般的保密通信模型中，在发送端将明文 P 用加密算法 E 和密钥 K 加密，变换成密文 C，即 C=E（K，P），在接收端利用解密算法 D 和密钥 K，对 C 进行解密，得到明文 P，即（　　）。D
A.P=E（K，C）　　B.P=E（C，D）　　C.P=K（C，D）　　D. P=D（K，C）
18. 经典的加密方法，主要包括：替换加密、换位加密和（　　）。A
A.一次性填充　　B.散列值　　C.奇偶校验　　D.报文摘要
19. （　　）函数被设计用来验证和确保数据完整性。C
A.对称加密　　B.流加密　　C.密码散列　　D.非对称加密
20. MD5 在本质上是简单的二进制操作（如异或运算）的一个复杂序列，被用于在输入数据上执行，生成一个（　　）位的报文摘要值。B
A.56　　B.128　　C.160　　D.256
21. PPP 协议使用 LCP 来建立和维护数据链路连接。借助（　　）在同一条点到点连接上使用多种网络层协议。C
A.UDP　　B.TCP　　C.NCP　　D.ICMP
22. （　　）是一种基于票据（Ticket）的认证方式，其设计目标是通过使用一台中央服务器提供“票据”，而网络中提供资源的服务器和访问资源的客户端之间使用这个“票据”相互识别。D
A.AAA　　B.PPP　　C.802.1X　　D.Kerberos
23. 从宏观角度来看，在使用 Kerberos 时，一个客户端需要经过（　　）个步骤来获取服务。B
A.2　　B.3　　C.4　　D.5
24. （　　）协议是一种广泛应用于无线网络的基于端口的网络访问控制协议。它具有完备的用户认证、管理功能，可以很好地支撑宽带网络的计费、安全访问、日常运营和管理要求。B
A.UDP　　B.802.1X　　C.802.3　　D.Kerberos
25. Netscape 公司推出了一个名为（　　）的传输层安全协议，用以保障在 Internet 上数据传输的安全。D
A.TLS　　B.SSH　　C.FTP　　D.SSL
26. POP3（Post Office Protocol - Version 3，邮局协议版本 3）在使用 TLS 保护后，被称为（　　）。A
A.POP3S　　B.SePOP3　　C.POP3-TLS　　D.TLS-POP3
27. IPsec 有两种工作模式：（　　）模式和隧道模式。C
A.汇聚　　B.分发　　C.传输　　D.接入

28. 在 Windows Server 服务器上的命令提示符窗口中，输入（　　），打开“高级安全 Windows 防火墙”窗口。D
A.wf.cpl　　B.firewall.msc　　C.firewall.cpl　　D.wf.msc

29. （　　）通常设置在企业内部网络中客户端与外部网络中服务器之间，它会暂存客户端发来的请求，并由自己发出这些请求。B
A.防火墙　　B.代理服务器　　C.入侵检测系统　　D.加密服务器

30. 访问控制服务，与（　　）相关。C
A.加密机制　　B.数据完整性机制　　C.访问控制机制　　D.公证机制

31. AH 的 IP 协议号为（　　），提供数据的完整性（MD5、SHA-1）和数据源身份验证，但是不能提供数据保密性功能，所有数据均以明文进行传输。A
A.51　　B.53　　C.21　　D.23

多选题：

1. 通常可以把网络信息安全的问题划分为物理层、网络层、（　　）和（　　）4 个层面。BC
A.传输层　　B.数据层　　C.内容层　　D.中间层　　E.支持层

2. 目前网络存在的威胁主要表现：非授权访问、信息泄漏、破坏数据完整性、（　　）和（　　）。AC
A.拒绝服务攻击　　B.下载软件不安全　　C.利用网络传播病毒
D.网络信息不对称　　E.网络带宽紧张

3. 抗抵赖性服务，主要涉及：数字签名机制、（　　）和（　　）。BD
A.加密机制　　B.数据完整性机制　　C.访问控制机制
D.公证机制　　E.业务流填充机制

4. 数据完整性服务，主要涉及：数字签名机制、（　　）和（　　）。AB
A.加密机制　　B.数据完整性机制　　C.访问控制机制
D.公证机制　　E.业务流填充机制

5. 数据保密性服务，主要涉及：加密机制、（　　）和（　　）。BE
A.加密机制　　B.路由控制机制　　C.访问控制机制
D.公证机制　　E.业务流填充机制

6. 认证服务，与加密机制、（　　）和（　　）相关。DE
A.业务机制　　B.路由控制机制　　C.访问控制机制
D.数字签名机制　　E.认证机制

7. 计算机病毒具有的特征包括：传染性、隐蔽性、潜伏性、（　　）和（　　）。AE
A.破坏性　　B.活跃性　　C.公开性　　D.自主性　　E.针对性

8. 常见的加密算法包括哪些：（　　）。ACE
A.3DES　　B.Hash　　C.AES　　D.MD5　　E.RSA

9. RSA 密钥的长度可以是：（　　）CDE
A.128 位　　B.256 位　　C.512 位　　D.1024 位　　E.2048 位

10. PPP 身份验证方法包括（　　）。BD
A.IPSec　　B.PAP　　C.EAP　　D.CHAP　　E.TLS

11. 提供认证、授权和计账功能的标准，包括:（　　）。AE
A. RADIUS　　B.ICMP　　C.EAP　　D.EIGRP　　E. TACACS

12. IPsec 是开放标准的一个框架，包括两个主要协议：（　　）BC
A. UDP　　B.AH　　C.ESP　　D.RIP　　E.OSPF

第 4 章 网络系统数据保护

判断题：

1. 应用数据主要是指保证业务系统正常运行所使用的系统目录、用户目录、系统配置文件、网络配置文件、应用配置文件、存取权限控制等。（　　）F
2. 系统数据主要是指操作系统、数据库系统安装的各类软件包和应用系统执行程序。（　　）T
3. 备份软件是备份系统的核心，负责维护所有的备份配置信息（涉及客户端、介质代理、备份设备等）。（　　）F
4. 备份系统的组件包括备份管理系统、备份客户端、备份软件和备份介质。（　　）F

5. 常见的网络数据备份系统，按其架构不同可以分为7种备份组网方式。（　　）F
6. 基于局域网（LAN-Base）结构是最简单的备份组网方式。在大多数情况下，这种备份是使用服务器主机上自带的备份介质，而备份操作往往也是通过手工操作的方式进行的。（　　）F
7. 与LAN-Base结构相比，LAN-Free结构让多台服务器共享备份介质，备份数据不再经过局域网，而直接从磁盘阵列传到备份介质内。（　　）T
8. 目前，最常用的备份介质有磁带、硬盘、光盘、云存储等。（　　）T
9. 完全备份是在某一个时间点上对所有数据的一个完全复制。这种备份方式的优点是备份速度快，备份数据量较少，没有重复的备份数据。（　　）F
10. 目标端重复数据删除是先将数据从业务中心传到备份中心，在备份中心存储时再删除重复数据。这种方法不会占用源端资源，但也不能节省传输带宽。（　　）T
11. Windows Server Backup是单服务器备份解决方案。不能使用一个服务器上的Windows Server Backup备份多个服务器上的数据。（　　）T
12. 灾难恢复是指将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。（　　）T
13. 灾难恢复工作包括灾难发生后的应急响应与处置、信息系统在灾难备份中心的恢复和重新运行、业务系统的灾后重建和回退工作。（　　）T
14. 恢复点目标（Recovery Point Object，RPO）是指故障后恢复数据和服务上线所需的时间量。（　　）F
15. 将某种业务的RPO设置为6小时，表示该业务能容忍最多6小时的数据丢失，所以必须每6小时至少执行一次备份，同时还要考虑执行备份所需的时间。（　　）T
16. 数据的备份是整个灾备系统的基础。通常可以将灾难恢复方案分为离线灾难恢复和在线灾难恢复。（　　）T
17. 容灾可认为是低级别的备份，容灾是备份的基础。（　　）F
18. 备份的主要目标是保证数据安全性，保存的是历史数据，恢复时间相对长；而容灾的主要目标是防止生产数据丢失或数据中心遭受毁灭性灾难，快速恢复，保证业务连续性。（　　）T
19. 简单来说，云存储就是将数据资源放到云计算平台上供人读写的一种方案。（　　）T
20. 服务可用性是指用户可使用数据和服务的时间百分比（通常以周作为单位）。（　　）F
21. 同步远程复制能够向异地提供最新的数据，但应用程序会因等待写入完成指示而被延迟一段时间。（　　）T
22. 异步远程复制对应用程序性能的影响最小，而且异地磁盘系统在数据的更新程度也不会有任何延迟。（　　）F

单选题：

1. 从数据用途角度来说，一般可将需要备份的数据分为系统数据、基本数据、应用数据、（　　）数据。A
   A.临时　　B.永久　　C.交换　　D.稀疏
2. （　　）数据主要是指业务系统的所有业务数据，对数据的安全性、准确性、完整性、一致性要求很高，而且变化频繁。B
   A.系统　　B.应用　　C.基础　　D.缓存
3. 备份系统的组件包括：备份管理系统、备份客户端、（　　）和备份介质。C
   A.备份对象　　B.备份软件　　C.备份网络　　D.备份路由
4. 备份管理系统，主要包含（　　）和备份管理服务器，负责备份策略管理和备份作业监控，以及读取备份客户端的数据并把数据写入备份介质。B
   A.备份对象　　B. 备份软件　　C.备份网络　　D.备份路由
5. 在一些大型的备份管理系统中，备份服务管理服务器通常由备份服务器和（　　）组成。A
   A. 介质服务器　　B. 备份介质　　C.文件服务器　　D.备份文件
6. 备份客户端是指需要备份数据的业务主机，它负责提供要备份的数据，一般需安装（　　）。C
   A.备份软件服务器端程序　　B.备份介质
   C.备份软件客户端代理程序　　D.备份管理软件
7. 备份介质是指备份数据存储的媒介，一般为磁盘阵列、物理磁带库或者虚拟带库、光盘塔、（　　）。B
   A.软盘　　B.云存储　　C.U盘　　D.移动硬盘
8. 最常见的网络数据备份系统按其架构不同可以分为：（　　）结构、基于局域网（LAN-Base）结构、不依赖局域网（LAN-Free）结构和不依赖服务器（Server-Free）结构。C
   A.基于数据类型　　B.基于用户　　C.基于主机　　D.基于应用
9. （　　）是小型办公环境最常使用的备份组网方式。在这种结构中，预先配置一台服务器作为备份管理服务器，它负责整个企业系统的备份操作。备份介质接在某台服务器上，当需要备份数据时，备份对象把数据通过网络传输

到备份介质中。D

A.基于数据类型结构　　B.基于用户结构

C.基于主机结构　　D.基于局域网结构

10. （　）是建立在SAN基础上的解决方案，是指数据无须通过局域网而直接进行备份。A

A.不依赖局域网（LAN-Free）结构　　B.不依赖应用（Application-Free）结构

C.不依赖主机（Host-Free）结构　　D.不依赖用户（User-Free）结构

11. 在（　）中，备份服务器仍参与备份过程，但负担大大减轻，因为它的作用只是指挥，而且不涉及数据的装载和运输，不是主要的备份数据通道。C

A.不依赖局域网（LAN-Free）结构　　B.不依赖应用（Application-Free）结构

C.不依赖服务器（Server-Free）结构　　D.不依赖用户（User-Free）结构

12. 常用的数据备份方式有完全备份、差异备份以及（　）。D

A.间隔备份　　B.差分备份　　C.副本备份　　D. 增量备份

13. （　）是以最近一次完全备份为基准，对最近一次完全备份后到进行此种备份的这段时间内，发生变化的数据进行备份。B

A.完全备份　　B.差异备份　　C.副本备份　　D. 增量备份

14. （　）是以最近一次备份为基准，对最近一次备份后到进行此种备份的这段时间内，发生变化的数据进行备份。D

A.完全备份　　B.差异备份　　C.副本备份　　D. 增量备份

15. （　）可以通过软件或硬件来实现，它把存储的文件切成小块，再比较每个小块的区别，然后对重复的数据块只保留一个副本。A

A. 重复数据删除　　B.差异数据删除　　C.副本数据删除　　D. 增量数据删除

16. 每年99.9%的服务可用性意味着数据和服务每年的计划外停机时间不得超过0.1%，以一年365天，每天24小时为例，一年的停机时间不得超过（　）。A

A. 8.76小时　　B.8.76分钟　　C.4.38小时　　D. 4.38分钟

17. 每年99.95%的服务可用性意味着数据和服务每年的计划外停机时间不得超过0.05%，以一年365天，每天24小时为例，一年的停机时间不得超过（　）。C

A. 8.76小时　　B.8.76分钟　　C.4.38小时　　D. 4.38分钟

18. 《信息安全技术信息系统灾难恢复规范》（GB/T 20988—2007）中定义的灾难恢复能力分为（　）个等级。C

A. 三　　B.五　　C.六　　D.八

19. 灾难恢复体系规划设计包括灾难恢复需求分析、策略制定、技术体系规划、（　）等方面。B

A.风险分析　　B. 资源规划　　C.灾难恢复目标规划　　D.备份网络技术

20. 灾难恢复需求分析能力包括对风险分析、（　）和灾难恢复目标制定3个方面，对其分析结果进行评估，以确保企业灾难恢复需求分析的结论符合企业业务恢复要求。C

A. 技术体系规划　　B. 资源规划　　C. 业务影响分析　　D. 策略制定

21. 基于数据库的复制方式可将远程数据库复制分为实时复制、（　）和存储转发复制。B

A.快速复制　　B. 定时复制　　C.完整复制　　D. 差异复制

22. 国际标准Share78对灾难恢复解决方案从低到高分为（　）种不同层次。C

A.三　　B.五　　C.七　　D.九

23. 国际标准Share78对灾难恢复解决方案从低到高分为多个不同层次,针对每个层次都有相应的容灾方案。其中(　　)级是最高级别的灾难恢复方案（零数据丢失）。C

A.0　　B.1　　C.6　　D.8

24. 国际标准Share78对灾难恢复解决方案从低到高分为多个不同层次,针对每个层次都有相应的容灾方案。其中(　　)级是成本最低的灾难恢复方案（无异地备份）。A

A.0　　B.1　　C.6　　D.8

多选题：

1. Windows Server Backup是Windows Server 2016操作系统提供的一项备份功能，它提供的操作接口包括：管理控制台和（　）。BC

A.backup命令　　B.wbadmin命令　　C. Windows PowerShell命令

D.ssh命令　　E.telnet命令

2. 灾难恢复的重要指标包括：服务可用性、恢复点目标、（　）等。AB

A.恢复时间目标　　B.保留目标　　C.应用响应时间
D.网络往返延迟　　E.操作系统可靠性

3. 网络系统管理员可以使用 Windows Server Backup 备份：完整服务器、系统状态、（　）和（　）等。CD
A. 仅单个设备的驱动程序　　B.仅注册表数据　　C. 仅单个文件和文件夹
D. 仅 Hyper-V 主机上的单个虚拟机　　E.仅系统页面文件

第 5 章 网络测量

判断题：

1. 网络测量是利用测量工具检测网络设备或网络系统运行状态、获取网络性能参数的过程。（　）T
2. 根据测量过程中是否向网络系统中注入探测数据包，可以将测量方式分为主动测量和被动测量。（　）T
3. 被动测量会向网络中注入额外的数据包，从而对网络的实际行为造成影响，可能会遮盖网络行为的本来面目，因此，测量结果也会造成一定的偏差。（　）F
4. 数据的预处理是要对采集到的数据包进行分类、过滤、计数和归并。（　）T
5. 数据分析结果通常有两种交付形式：一是统计报表，二是可视化图形。（　）T
6. 传输控制协议（Transmission Control Protocol，TCP）是面向数据报文的传输层协议。在基于 TCP 的主动测量过程中，测量主机需要向被测量主机发送探测数据包，但通信双方之间的传输没有明确的连接（类似于邮件传输），通信双方是对等的，单次传输的最大数据量取决于具体的网络。（　）F
7. 在测量单向时延时，首先应该使测量节点 A 和测量节点 B 的时间同步，然后在节点 A 形成一个 64 字节的 UDP 数据包，获取节点 A 的时间后在包头部加载一个时间戳（A）并立即发出，当节点 B 完整地接收到这个数据包后，立即获取接收时间（B），则“B 减 A”的值即为该链路的单向时延。（　）T
8. 带宽通常表示网络传输路径或链路的传输容量，即数据包的传输速度。（　）T
9. 链路带宽是指源节点到目的节点之间性能最低的链路所能达到的最大传输速度，也就是该传输路径所能提供给一个业务流的最大传输速度。（　）F
10. 丢包率是单位时间内传输中丢失的数据包与所有数据包的比值。数据包丢失一般是由网络拥塞引起的，当丢包率超过 15%时，可能会导致网络不可用。（　）T
11. 吞吐量是描述网络设备转发速度的性能指标。其度量单位通常是字节/秒（Byte/s）。（　）F
12. ipconfig 命令是个使用频率极高的测试命令，其主要功能是使用 ICMP（Internet Control Message Protocol，网络控制报文协议）数据包来测试从源端到目的端网络的连通性，它可以快速准确地判断网络故障。（　）F
13. 在Windows操作系统的命令提示符窗口中输入“ping 127.0.0.1”，能够判断本机的TCP/IP协议设置是否正常。（　）F
14. arp 命令用于显示和修改地址解析协议（Address Resolution Protocol，ARP）缓存表的内容。（　）T
15. netstat 命令用于显示 TCP 连接、当前计算机正在监听的端口、以太网统计信息、IP 路由表、IPv4 统计信息、IPv6 统计信息等。（　）T
16. tracert 命令用来跟踪源与目标节点之间的所有路由器。（　）T
17. 主动测量方法的优点包括：不依赖于被测量对象的测量能力，能直接测量和分析网络性能；适合端到端的网络性能测量，对于所关注的内容只要在本地发送测试数据包，然后观察网络的响应即可；测量方式不涉及用户的网络信息，所以对用户而言安全性好。（　）T
18. 因为 TCP 协议是面向连接的，所以通过测试 TCP 的性能反映发送端与接收端之间的性能参数。（　）T
19. ping 命令还能显示 TTL（Time To Live，生存期）值，该值是由发送端主机设置的，它的作用是防止数据包在 IP 网络中永不终止地转发下去。（　）T
20. 在 Windows 操作系统的命令提示符窗口中输入 arp-a 命令，会显示所有网卡接口的 ARP 缓存表。（　）T

单选题：

1. 通过发送（　）数据包，可以获得网络往返时延、丢包率与连通性等参数。A
A.ICMP　　B.RIP　　C.PHP　　D.MAC
2. （　）会向网络中发送特定的探测数据包，网络系统管理员通过对探测数据包所受网络影响而发生特性变化的分析，得到网络状态和性能参数。B
A.被动测量　　B. 主动测量　　C.单点测量　　D.协作式测量
3. 按照网络测量点的位置，可以分为端系统测量和（　）。D

A.被动测量　　B. 主动测量　　C.单点测量　　D.中间系统测量

4. 网络测量技术的基本要求是有效性、高速测量、准确性和（　）。C

A.隐蔽性　　B. 调节性　　C. 实时性　　D.变化性

5. 从网络测量系统的功能角度，网络测量系统的体系结构从底层到高层分别为数据采集层、数据管理层、（　）和数据表示层。A

A. 数据分析层　　B.数据传输层　　C.数据应用层　　D.数据处理层

6. 数据管理功能包括基于数据管理和（　）管理。B

A.病毒　　B.事件　　C.用户　　D.计算机

7. 基础数据分析包括三方面功能：基本统计功能、（　）和数据关联分析 C

A.事件分析　　B.数据库分析　　C.性能趋势预测　　D.可靠性趋势预测

8. （　）通常采用便携式测量仪表，在网络中的某个节点上安置测量系统或测量仪表进行测量。D

A.集中式测量　　B.分布式测量　　C.多点测量　　D.单点测量

9. 在（　）体系中，测量节点是完整的测量系统，它们分布在网络中的多个位置，既可以独立地进行网络测量，也可以将测量数据发送到测量中央服务器。B

A.集中式测量　　B.分布式测量　　C.双点测量　　D.单点测量

10. 主动测量方法可以利用 TCP/IP 协议中的（　）、TCP、UDP 等协议来发送探测数据包进行测量。A

A.ICMP　　B.ARP　　C.IPX　　D.AppleTalk

11. TCP 连接的建立与断开采用（　）的方式。B

A. “三次握手+三次断开”　　B. “三次握手+四次断开”

C. “四次握手+三次断开”　　D. “四次握手+四次断开”

12. SNMP 协议提供了三类操作，包括：Get、Set 和（　）。D

A.Renew　　B.Answer　　C.Ask　　D.Trap

13. 与带宽相关的参数有：链路带宽、瓶颈带宽、（　）等。B

A.时延带宽　　B. 可用带宽　　C.总体带宽　　D.最小带宽

14. （　）是 Windows 操作系统中的一个系统命令，用于显示本机的 TCP/IP 网络配置值。C

A.ping　　B. netstat　　C.ipconfig　　D.arp

15. 在 Windows 操作系统的计算机上运行的 ping 命令会发送 4 个 ICMP 回送请求数据包，每个数据包为（　）。B

A. 32 比特　　B. 32 字节　　C.16 字节　　D. 16 比特

16. 输入 netstat （　）命令，则显示活动的 TCP 连接、地址和端口号（以数字形式表示）。C

A. -t　　B.-q　　C.-n　　D.-i

17. （　）命令用来跟踪源与目标节点之间的所有路由器。C

A. arp　　B.netstat　　C. tracert　　D.ping

18. 可以使用（　）组合键，打开 Windows 任务管理器。A

A. Ctrl+Shift+Esc　　B. Ctrl+Alt+Esc

C. Shift+Alt+Esc　　D. Ctrl+Tab+Esc

多选题：

1. 网络测量的功能按照测量对象，可分为三大类：（　）ABE

A.网络性能测量　　B. 业务性能测量　　C.应用可靠性测量

D.数据库性能测量　　E. 网络流量测量

2. TCP/IP 网络性能指标可以从物理层、数据链路层、（　）、传输层和（　）5 个层次来分析。DE

A.管理层　　B.表示层　　C.会话层　　D.网络层　　E. 应用层

3. 在 Windows 资源监视器中，可以查看到的选项卡包括：（　）、（　）、内存、磁盘、（　）。ACD

A.概述　　B.服务　　C.CPU　　D.网络　　E. 详细信息

第 6 章 网络故障管理

判断题：

1. 网络链路的问题通常是由网卡、跳线、信息插座、交换机、UPS 等设备和服务配置引起的。（　）F

2. 网络故障大致可以分为 4 类，即应用故障、协议故障、操作故障和服务故障。（　）F

3. 数据包分析工具是一种可以捕获和记录网络数据包的工具，可以帮助网络系统管理员解决网络问题、检查网络安全隐患、显示数据包传输状态、学习网络传输协议。（　）T
4. 大部分的网络是基于 TCP/IP 协议构建的，网络系统管理员在排除网络故障时，可以参考 TCP/IP 协议的分层思想。（　）T
5. 数据链路层负责在网络层与传输层之间进行信息传输，数据帧的封装、解封装、差错校验等。（　）F
6. 网络层提供用户服务，如网页服务、电子邮件服务、文件传输服务、域名查询服务等。（　）F
7. 在 Cisco 公司的交换机上，可以使用 show vlan 命令查看交换机配置的 VLAN 相关信息（　）T

单选题：

1. 网络故障排查流程：描述网络故障现象、收集可能的网络故障原因信息、（　）、网络故障分析、事后记录和总结。B

   A.联系网络管理员　　B. 建立诊断计划　　C.立即修改当前配置　　D.查看日志
2. 网络服务故障主要包括 3 个方面：服务器硬件故障、网络操作系统故障和（　）。C

   A.人为故障　　B.诊断故障　　C. 网络服务故障　　D.文件故障
3. 数据链路层的故障主要表现在通信双方的（　）封装协议是否一致。C

   A.四层　B.三层　C. 二层　D.一层
4. 电缆测试仪是针对 OSI 模型的第（　）层设计的。D

   A.四层　B.三层　C. 二层　D.一层

多选题：

1. 网络故障大致可以分为 4 类，即链路故障、协议故障、（　）和（　）。AC

   A.配置故障　　B.应用故障　　C.服务故障　　D.操作故障　　E.人为故障
2. 数据帧封装格式包括：HDLC、（　）和、（　）等。DE

   A.RIP　　B.ARP　　C.ICMP　　D. PPP　　E. Frame-Realy

第 7 章 网络计费管理

判断题：

1. 基于使用时间的计费最早应用于传统电话，它是根据用户使用网络的时间长短来收取用户费用的一种计费方法。（　）T
2. 代理服务器能够记录用户的 IP 地址、帐户、请求时间、访问地址、信息长度等详细数据，可以进行分类统计和记账。（　）T
3. 基于访问日志的数据采集方式既可以对 IP 地址进行流量计费，又可以对用户流量计费。（　）F
4. 基于流量计费是根据用户在一段时间内所使用的全部网络流量（发送和接收）统计数据来收取用户费用的一种计费方式。（　）T

单选题：

1. 计费管理的组件包括：计费数据的采集和存储；（　）；与用户、管理员之间的人机交互界面。B

   A. 数据的处理　B. 数据的分析和统计　C.数据的过滤　D.数据的筛分
2. 计费管理可以用来确定网络中每一种服务的价值，包括（　）类服务、软件类服务和人工服务。A

   A. 硬件　B. 设备　C.人工　D.协议
3. （　）的计费是根据用户在一段时间内所使用的全部网络流量（发送和接收）统计数据来收取用户费用的一种计费方式。D

   A. 基于时间　B.基于服务　C.统一费用　D. 基于网络流量
4. 住宅的宽带接入服务，当用户订购服务之后，可以按月或按年支付费用，并随意访问 Internet。这种计费方式属于（　）的计费。C

   A. 基于时间　B.基于服务　C.统一费用　D. 基于网络流量
5. （　）是一种网络监测功能，可以收集流入和流出网络接口的 IP 数据包。D

   A. NetCollect　B.NetMon　C.NetMonitor　D. NetFlow
6. NetFlow 通过将数据包中的多个关键字段相结合来定义一个“流”，最初定义了（　）个关键字段。C

A. 五　B.六　C.七　D.四

多选题：

1. 当前许多计费系统采用三层体系结构，分别对应表示层、（　）和（　）。DE

A.会话层　B.管理层　C.消费层　D.应用层　E.数据层

2. 可以基于（　）等网络设备来实现基于流量的计费。BCE

A.中继器　B. 路由器　C. 防火墙　D.集线器　E. 代理服务器

配伍题

1.

①	网络管理		a	负责分析和统计历史数据，建立性能基线和性能分析的模型，预测网络性能的长期趋势。
②	性能分析		b	是指对网络的运行状态进行监测和控制，使其能够安全、可靠、高效、经济地为客户提供服务。
③	SNMP		c	是一种将企业内部网络与外部网络分离的方法，是在企业内部网络和外部网络之间所施加的安全防范系统。
④	防火墙		d	是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用，并且能自我复制的一组计算机指令或者程序代码。
⑤	计算机病毒		e	定义了一系列网络管理规范标准，提供了一个用来监测网络状态、管理配置文件、收集网络数据和检测网络行为的工具。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、b　2、a　3、e　4、c　5、d

2.

①	MIB		a	是一种对称密钥算法。
②	Kerberos		b	建立在网络层之上，可以保护网关之间、主机之间或网关与主机之间的路径安全。
③	DES		c	是 Netscape 公司首先提出了一个标准，一个传输层安全协议，用以保障在 Internet 上数据传输的安全。
④	IPSec		d	是一个存储网络管理信息的数据库，由被管理对象组成。
⑤	SSL		e	是一种基于票据（Ticket）的认证方式，其设计目标是通过使用一台中央服务器提供“票据”，而网络中提供资源的服务器和访问资源的客户端之间使用这个“票据”相互识别。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、d　2、e　3、a　4、b　5、c

3.

①	备份客户端		a	用于指定已锁定的帐户在自动解锁之前保持锁定状态的时长。
②	云存储		b	能够确保某个实体身份的可靠性，可分为两种类型。
③	CMIP		c	指一个以数据存储和管理为核心的云计算系统。
④	帐户锁定时间		d	是构建于 OSI 参考模型上的网络管理协议，与之相关的 CMIS（Common Management Information Service，通用管理信息服务）定义了获取、控制和接收有关被管理对象运行状态的服务。
⑤	认证服务		e	是指需要备份数据的业务主机，它负责提供要备份的数据，一般需安装备份软件客户端代理程序。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、e　2、c　3、d　4、a　5、b

4.

①	完全备份		a	是指通过网络系统管理员快速地检查问题并启动恢复过程的工具，使得网

				络服务的可靠性得到增强。
②	故障管理		b	通常是位于企业网络边界上的一个小盒子，通过硬件和软件的结合达到隔离内外网络的目的。
③	业务流填充机制		c	是在某一个时间点上对所有数据的一个完全复制。
④	特洛伊木马		d	是把自己伪装成为善意应用程序（进程）的恶意软件程序。
⑤	硬件防火墙		e	通过在数据传输过程中传送随机数的方式，混淆真实的数据，加大数据破解的难度，提高数据的保密性。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、c 2、a 3、e 4、 d 5、b

5.

①	差异备份		a	通常是在网络的入口对通过的数据包进行选择，只有满足条件的数据包才能通过（进入企业内部网络），否则被抛弃。
②	认证服务		b	提供对通信中对等实体和数据来源的鉴别。
③	缓冲区		c	是一种寄存于文档或模板的宏中的计算机病毒。
④	宏病毒		d	是指应用程序或操作系统用来保存数据的临时区域。
⑤	包过滤防火墙		e	是以最近一次完全备份为基准，对最近一次完全备份后到进行差异备份的这段时间内，发生变化的数据进行备份。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、e 2、b 3、d 4、c 5、a

6.

①	增量备份		a	防止参与某次通信的任何一方事后否认本次通信或通信内容。
②	抗抵赖性服务		b	把明文变为一种编码（如 ASCII 编码），选择一个等长的随机字符串作为密钥，对二者进行逐位异或运算得到密文。
③	一次性填充加密		c	是一种数据链路层协议，被设计用于点对点连接中传递数据，使用用户名和密码进行验证，并协调两个设备使用的网络协议。
④	密码散列（Hash）函数		d	是以最近一次备份（包括完全备份、差异备份、增量备份）为基准，对最近一次备份后到进行增量备份的这段时间内，发生变化的数据进行备份。
⑤	PPP		e	被设计用来验证和确保数据完整性。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、d 2、a 3、b 4、e 5、c

7.

①	访问控制服务		a	入侵者可以拦截网络中正常的通信数据，并修改和控制通信双方的 TCP 会话，而通信的双方却毫不知情，入侵者就可以使用抓包软件查看双方的通信内容。
②	基于主机的入侵检测系统		b	是使用不同的密钥进行加密和解密的一种加密算法。
③	RSA		c	对资源提供保护，防止非授权的访问和操纵。
④	中间人攻击		d	是一种网络服务，允许一个网络终端（如客户端计算机）通过这个服务与另一个网络终端（如 Web 服务器、邮件服务器、DNS 服务器）进行非直接的连接。
⑤	代理		e	运行在受保护设备上（如计算机）的，用于监测主机操作系统和系统本地用户的状况。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、c 2、e 3、b 4、a 5、d

8.

①	SNMP 的 Trap 报文		a	拥有管理本台计算机的所有权限和权利。
②	数据加密		b	是一种单向函数，这使得从给定输入数据计算出散列值很容易，但要从散列值反向计算出输入数据则不可行。
③	管理员帐户		c	用于代理主动向管理站通告重要事件的报文。
④	MD5		d	主要是指业务系统的所有业务数据，对数据的安全性、准确性、完整性、一致性要求很高，而且变化频繁。
⑤	应用数据		e	是防止未经授权的用户访问敏感信息的手段，这就是人们通常理解的安全措施，也是其他安全方法的基础。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、c 2、e 3、a 4、b 5、d

9.

①	帐户锁定阈值		a	是针对整个网络的入侵检测系统，包括对网络中的所有主机、网络设备进行入侵行为的监测和响应。
②	泛洪		b	用于指定在用户帐户被锁定之前允许登录失败的次数。
③	流加密		c	主要是指保证业务系统正常运行所使用的系统目录、用户目录、系统配置文件、网络配置文件、应用配置文件、存取权限控制等。
④	基础数据		d	是将数据包与密钥生成二进制比特流进行异或运算的加密过程。
⑤	基于网络的入侵检测系统		e	是指入侵者可以向网络中发送大量的无用数据包，使网络设备（如交换机）满负荷或超负荷运行，导致网络性能下降，甚至瘫痪。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、b 2、e 3、d 4、c 5、a

10.

①	事件数据库。		a	是指备份数据由备份客户端到备份服务器的传输路径。
②	端口认证		b	是指用户可使用数据和服务的时间百分比（通常以年作为单位）。
③	备份网络		c	是指在网络设备（如路由器、交换机）上进行的测量。
④	服务可用性		d	是指允许远程用户通过某个进入点（端口）访问另一个网络。
⑤	中间系统测量		e	负责存放有关事件的各种中间过程数据和最终数据，它可以是面向对象的复杂数据库，也可以是简单的文本文件。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、e 2、d 3、a 4、b 5、c

11.

①	数据保密性服务		a	可以防止对任何资源的非授权访问，确保只有经过授权的实体才能访问相应的资源。
②	数据完整性服务		b	采用加密手段，防止数据被破解后泄露。
③	访问控制服务		c	能够确保某个实体身份的可靠性。
④	认证服务		d	为数据发送方选择安全的网络通信路径，避免发送方使用不安全路径发送数据而受到攻击，以提高数据的安全性。
⑤	路由控制机制		e	可防止未授权的对数据的修改操作。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、b　　2、e　　3、a　　4、c　　5、d

12.

①	硬件防火墙		a	接受来自内部网络用户的通信，然后与外部网络服务器建立单独连接，而不允许内部网络与外部网络直接通信，它在应用层的通信中扮演着一个消息传递者的角色。
②	应用层防火墙		b	负责数据转发的独立系统,它由网关路由器建立通信双方的两个 TCP 连接，即一个连接网关与内部网络，另一个连接网关与外部网络。
③	状态检测防火墙		c	监视、分析用户及系统活动，查找非法用户和合法用户的越权操作。
④	电路层防火墙		d	又称动态包过滤防火墙，是包过滤的功能扩展
⑤	入侵检测系统		e	通常是位于企业网络边界上的一个小盒子，通过硬件和软件的结合达到隔离内外网络的目的。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、e　　2、a　　3、d　　4、b　　5、c

13.

①	蠕虫		a	入侵者可以拦截网络中正常的通信数据，并修改和控制通信双方的 TCP 会话，而通信的双方却毫不知情，入侵者就可以使用抓包软件查看双方的通信内容。
②	特洛伊木马		b	把自己伪装成为善意应用程序（进程）的恶意软件程序。
③	中间人攻击		c	是指入侵者可以向网络中发送大量的无用数据包，使网络设备（如交换机）满负荷或超负荷运行，导致网络性能下降，甚至瘫痪。
④	泛洪		d	入侵者利用或操控企业内部人员，获取他们所需要的信息，包括电话诈骗；试图套出公司员工的名字和口令；伪装成为合法人员。
⑤	社会工程攻击		e	可以占领计算机的内存空间，以自我复制的方式从一台计算机通过网络蔓延到另一台计算机。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、e　　2、b　　3、a　　4、c　　5、d

14.

①	替换加密		a	把明文变为一种编码（如 ASCII 编码），选择一个等长的随机字符串作为密钥，对二者进行逐位异或运算（两个值不相同，则异或结果为 1，否则异或结果为 0）得到密文。
②	换位加密		b	将明文分成 64 位的块，对每个块进行 19 次变换（替换和换位），其中 16 次变换由 56 位的密钥的不同排列形式控制，最后产生 64 位的密文块。
③	一次性填充		c	用一个字母替换另一个字母。
④	DES		d	按照一定的规律重排字母的顺序。
⑤	RSA		e	其密钥的长度通常是 512 位~2 048 位，它的安全性基于大素数分解的困难性。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、c　　2、d　　3、a　　4、b　　5、e

15.

①	MD5		a	用于封装多种网络层协议（如 IP、IPX、AppleTalk）报文并通过同一条

				PPP 数据链路发送它们。
②	NCP		b	以明文方式发送密码，也就是没有经过加密，因此如果在传输进程中被拦截，密码有可能外泄，比较不安全。
③	PAP		c	默认使用 TCP49 端口，并且对不同的设备采用不同的授权、认证和计账方法。
④	TACACS+		d	是一种单向函数，这使得从给定输入数据计算出散列值很容易，但要从散列值反向计算出输入数据则不可行。
⑤	SSL 记录协议		e	建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、d 2、a 3、b 4、c 5、e

16.

①	TLS		a	提供代理服务的计算机或其他网络设备。
②	IPsec		b	是指故障后恢复数据和服务上线所需的时间量。
③	Proxy Server		c	对 SSL 进行了改进，用于保证 Web 通信以及其他流行协议的安全。
④	CIDF		d	将入侵检测系统分为 4 个组件：事件产生器、事件分析器、事件数据库、响应单元。
⑤	RTO		e	提供的安全功能包括：保密性、完整性、身份验证和安全密钥交换。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、c 2、e 3、a 4、d 5、b

17.

①	ICMP		a	采用“三次握手+四次断开”的方式来建立与断开连接。
②	Frame-Realy		b	是 TCP/IP 协议族中的网络管理协议，定义了传送管理信息的协议消息格式、管理站和代理之间进行消息传送的规则，能对 IP 网络中不同类型的设备进行监控和管理。
③	TCP		c	用于显示本机的 TCP/IP 网络配置值。
④	SNMP		d	是 TCP/IP 协议族中 IP 层的一个重要协议，提供了差错报告和 IP 设备间重要信息交换的机制，被广泛应用于网络的管理和主动测量方法之中。
⑤	ipconfig		e	一种二层数据帧的封装格式。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、d 2、e 3、a 4、b 5、c

18.

①	数字电压表		a	可以在网络中的每一帧中提供应用层、传输层、网络层和数据链路层信息。
②	时域反射计		b	可用于进行链路连通性测试，可以测量诸如交直流电压、电流、电阻、电容以及电缆连续性等参数，利用这些参数可以检测物理连通性。
③	电缆测试仪		c	可以对所连接的网络进行网络监视，判断网络运行是否正常，还可以进行协议分析，能够对网络上的协议或者通信问题进行故障诊断。
④	协议分析仪		d	可用于确定电缆断开的具体位置。通过电缆定时发送脉冲，监听反射回来的信号。
⑤	网络管理软件		e	针对 OSI 模型的第一层设计的，它只能用来测试电缆而不能测试网络的其他设备。

①：___ ②：___ ③：___ ④：___ ⑤：___

正确答案： 1、b　　2、d　　3、e　　4、a　　5、c

操作题

第 2 章　网络用户配置管理

1. 在一台安装了 Windows 操作系统的服务器 Server1 上，管理员需要创建一个帐户策略，以确保用户必须使用复杂的密码。

   要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，展开“帐户密码”-> _____

步骤 3：在右侧窗格中，右击_____，并单击“属性”

步骤 4：在弹出的对话框中，选中_____选项，然后单击“确定”。

步骤 5：关闭“本地安全策略”窗口。

【答案选项】

A.密码必须符合复杂性要求。

B.登录服务器 Server1，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。

C.密码策略。

D.已禁用。

E.密码长度最小值。

F.已启用。

正确答案： 1、B　　2、C　　3、A　　4、F

2. 在一台安装了 Windows 操作系统的服务器 Server2 上，管理员需要创建一个帐户策略，以确保用户密码长度最小值为 8 字符。

   要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，展开“帐户密码”-> _____

步骤 3：在右侧窗格中，右击_____，并单击“属性”

步骤 4：在弹出的对话框中，在文本框中输入_____，然后单击“确定”。

步骤 5：关闭“本地安全策略”窗口。

【答案选项】

A.密码长度最小值。

B.登录服务器 Server2，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。

C.密码策略。

D. 已启用。

E. 密码必须符合复杂性要求。

F.8。

正确答案： 1、B　　2、C　　3、A　　4、F

3. 在一台安装了 Windows 操作系统的服务器 Server3 上，管理员需要创建一个帐户策略，以确保用户密码最长使用期限为 30 天。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，展开“帐户密码” ，然后单击_____

步骤 3：在右侧窗格中，右击_____，并单击“属性”

步骤 4：在弹出的对话框中，在文本框中输入_____，然后单击“确定”。

步骤 5：关闭“本地安全策略”窗口。

【答案选项】

A. 密码最长使用期限。

B.登录服务器 Server3，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。

C.密码策略。

D. 已启用。

E.密码长度最小值。

F.30。

正确答案： 1、B 2、C 3、A 4、F

4. 在一台安装了 Windows 操作系统的服务器 Server4 上，管理员需要创建一个帐户策略，以确保用户密码最短使用期限为 1 天。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，展开“帐户密码” ，然后单击_____

步骤 3：在右侧窗格中，右击_____，并单击“属性”

步骤 4：在弹出的对话框中，在文本框中输入_____，然后单击“确定”。

步骤 5：关闭“本地安全策略”窗口。

【答案选项】

A. 密码最短使用期限。

B.登录服务器 Server4，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。

C.密码策略。

D. 已启用。

E.密码长度最小值。

F.1。

正确答案： 1、B 2、C 3、A 4、F

5. 在一台安装了 Windows 操作系统的服务器 Server5 上，管理员需要创建一个帐户策略，以实现用户在 30 分钟内输错 5 次密码后，其帐户被自动锁定 30 分钟。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，展开“帐户密码”，然后单击 _____

步骤 3：在右侧窗格中，右击_____，并单击“属性”

步骤 4：在弹出的对话框中，在文本框中输入_____，然后单击“确定”。在“建议的数值改动”对话框中，单击“确定”。

步骤 5：关闭“本地安全策略”窗口。

【答案选项】

A.帐户锁定阈值。

B.30。
C.帐户锁定策略。
D.登录服务器 Server5，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。
E.5。
F.帐户锁定时间。
正确答案： 1、D　　2、C　　3、A　　4、E

6. 在一台安装了 Windows 操作系统的服务器 Server6 上，管理员需要创建一个帐户策略，以实现用户在 20 分钟内输错 7 次密码后，其帐户被自动锁定 20 分钟。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:
步骤 1：登录服务器 Server6，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。
步骤 2：在左侧导航栏中，展开“帐户密码” ，然后单击“帐户锁定阈值”。
步骤 3：在右侧窗格中，右击_____，并单击“属性”
步骤 4：在弹出的对话框中，在文本框中输入_____，然后单击“确定”。在“建议的数值改动”对话框中，单击“确定”。
步骤 5：在右侧窗格中，右击_____，并单击“属性”。
步骤 6：在弹出的对话框中，在文本框中输入_____，然后单击“确定”。在“建议的数值改动”对话框中，单击“确定”。
步骤 7：关闭“本地安全策略”窗口。
【答案选项】
A.帐户锁定阈值。
B.20。
C.帐户锁定策略。
D.登录服务器 Server6，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 secpol.msc，单击“确定”。
E.7。
F.帐户锁定时间。
正确答案：1、A　　2、E　　3、F　　4、B

第 3 章　网络安全

7. 在一台安装了 Windows 操作系统的服务器 Server7 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server7）的 80 端口。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:
步骤 1：_____
步骤 2：在左侧导航栏中，右击“入站规则”并单击“新建规则”。在“规则类型”对话框中，选择“自定义”选项，单击“下一步”。
步骤 3：在“程序”对话框中，单击“下一步”。
步骤 4：_____
步骤 5：在“作用域”对话框中，在“此规则应用于哪些本地 IP 地址”选项下方，选中“下列 IP 地址”选项，在下方文本框中输入服务器 Server7 的 IP 地址，然后单击“添加”；在“此规则应用于哪些远程 IP 地址”选项下方，选中“任何 IP 地址”选项，然后单击“下一步”。
步骤 6：_____
步骤 7：在“配置文件”对话框中，单击“下一步”。
步骤 8：_____

【答案选项】
A. 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。
B. 在“名称”对话框中，输入规则名称后，单击“下一步”。
C. 在“协议和端口”对话框中，选择“协议类型：TCP”、“本地端口：特定端口、80”，单击“下一步”。
D. 登录服务器 Server7，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
E. 登录服务器 Server7，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
F. 在“协议和端口”对话框中，选择“协议类型：TCP”、“远程端口：特定端口、80”，单击“下一步”。
正确答案： 1、E　　2、C　　3、A　　4、B

8. 在一台安装了 Windows 操作系统的服务器 Server8 上，管理员需要创建一个防火墙规则：拒绝此服务器（Server8）访问任何远程计算机的 443 端口的访问。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：_____
步骤 2：在左侧导航栏中，右击“出站规则”并单击“新建规则”。在“规则类型”对话框中，选择“自定义”选项，单击“下一步”。
步骤 3：在“程序”对话框中，单击“下一步”。
步骤 4：_____
步骤 5：在“作用域”对话框中，单击“下一步”。
步骤 6：_____
步骤 7：在“配置文件”对话框中，单击“下一步”。
步骤 8：_____
【答案选项】
A. 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。
B. 在“名称”对话框中，输入规则名称后，单击“下一步”。
C. 在“协议和端口”对话框中，选择“协议类型：TCP”、“本地端口：特定端口、443”，单击“下一步”。
D. 登录服务器 Server8，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
E. 登录服务器 Server8，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 在“协议和端口”对话框中，选择“协议类型：TCP”、“远程端口：特定端口、443”，单击“下一步”。
正确答案： 1、D　　2、F　　3、A　　4、B

9. 在一台安装了 Windows 操作系统的域控制器服务器 Server9 上，管理员需要设置 Windows 防火墙属性：记录被丢弃的数据包。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：_____
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击_____。
步骤 3：在弹出的对话框中，单击_____右侧的“自定义”。
步骤 4：在弹出的对话框中，在_____右侧的列表框中，选择“是”，然后单击“确定”。
步骤 5：返回上一级对话框，单击“确定”。
步骤 6：关闭“高级安全 Windows 防火墙”窗口。
【答案选项】
A. 日志。
B. 记录被丢弃的数据包。

C. 设置。
D. 登录服务器 Server9，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
E. 登录服务器 Server9，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 属性。
正确答案： 1、D　　2、F　　3、A　　4、B

10. 在一台安装了 Windows 操作系统的域控制器服务器 Server10 上，管理员需要设置 Windows 防火墙属性：将日志文件的保存路径设置为 D:\fw\fw.log。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：_____
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击_____。
步骤 3：在弹出的对话框中，单击_____右侧的“自定义”。
步骤 4：在弹出的对话框中，在_____右侧的文本框中输入“D:\fw\fw.log”，然后单击“确定”。
步骤 5：返回上一级对话框，单击“确定”。
步骤 6：关闭“高级安全 Windows 防火墙”窗口。
【答案选项】
A. 日志。
B. 名称。
C. 设置。
D. 登录服务器 Server10，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
E. 登录服务器 Server10，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 属性。
正确答案： 1、D　　2、F　　3、A　　4、B

11. 在一台安装了 Windows 操作系统的域控制器服务器 Server11 上，管理员需要设置 Windows 防火墙属性：将防火墙状态设置为：关闭。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1：_____
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击_____。
步骤 3：在弹出的对话框中，在_____右侧的列表框中，选择_____，然后单击“确定”。
步骤 4：关闭“高级安全 Windows 防火墙”窗口。
【答案选项】
A. 防火墙状态。
B. 阻止。
C. 关闭。
D. 登录服务器 Server11，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
E. 登录服务器 Server11，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 属性。
正确答案： 1、D　　2、F　　3、A　　4、C

12. 在一台安装了 Windows 操作系统的服务器 Server12 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server12）上的 iSCSI 服务。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，右击“入站规则”并单击“新建规则”。

步骤 3：在“规则类型”对话框中，选择_____选项，并在列表框中选择“iSCSI 服务”，单击“下一步”。

步骤 4：在“规则”对话框中，勾选_____选项，然后单击“下一步”。

步骤 5：_____

【答案选项】

A. 在“操作”对话框中，选中“阻止连接”选项，单击“完成”。

B. 在“名称”对话框中，输入规则名称后，单击“完成”。

C. 预定义。

D. 登录服务器 Server12，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。

E. 登录服务器 Server12，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。

F. iSCSI 服务。

正确答案： 1、E　　2、C　　3、F　　4、A

13. 在一台安装了 Windows 操作系统的服务器 Server13 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server13）上的所有程序。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，右击“入站规则”并单击“新建规则”。

步骤 3：在“规则类型”对话框中，选择_____选项，然后单击“下一步”。

步骤 4：在“程序”对话框中，选择_____选项，然后单击“下一步”。

步骤 5：_____

步骤 6：在“配置文件”对话框中，单击“下一步”。

步骤 8：在“名称”对话框中，输入规则名称后，单击“完成”。

【答案选项】

A. 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。

B. 在“名称”对话框中，输入规则名称后，单击“完成”。

C. 程序。

D. 登录服务器 Server13，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。

E. 登录服务器 Server13，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。

F. 所有程序。

正确答案： 1、E　　2、C　　3、F　　4、A

14. 在一台安装了 Windows 操作系统的服务器 Server14 上，管理员需要创建一个防火墙规则：仅拒绝此服务器（Server14）访问任何远程计算机的 TCP53 端口。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：_____

步骤 2：在左侧导航栏中，右击“出站规则”并单击“新建规则”。
步骤 3：在“规则类型”对话框中，选择_____选项，单击“下一步”。
步骤 3：在“协议和端口”对话框中，选择“TCP”，在_____右侧的文本框中输入 53，然后单击“下一步”。
步骤 4：在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。
步骤 5：在“配置文件”对话框中，单击“下一步”。
步骤 6：_____
【答案选项】
A. 特定远程端口。
B. 在“名称”对话框中，输入规则名称后，单击“下一步”。
C.所有远程端口。
D. 登录服务器 Server14，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
E. 登录服务器 Server14，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
F. 端口。
正确答案： 1、D　　2、F　　3、A　　4、B

15. 换位加密能够按照一定的规律重排字母的顺序。例如，以 LUCKY 作为密钥（在字母表中的出现顺序为 34125），对明文 HELLOWORLD 进行加密，会得到密文 LRLLHWEOOD，如下表所示。

密钥	L	U	C	K	Y
字母表中的顺序	3	4	1	2	5
明文	**H**	**E**	**L**	**L**	**O**
	W	**O**	**R**	**L**	**D**
密文	**LR**（C 列）**LL**（K 列）**HW**（L 列）**EO**（U 列）**OD**（Y 列）				

请参考上述加密方法，以 TONY 作为密钥，将明文 HAPPYNEWYEAR 转换为密文：P_____A_____H_____P_____
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【答案选项】
A.YY。
B.WR。
C.WY。
D.EA。
E.EN。
F.NE。
正确答案： 1、D　　2、F　　3、A　　4、B

16. 换位加密能够按照一定的规律重排字母的顺序。例如，以 LUCKY 作为密钥（在字母表中的出现顺序为 34125），对明文 HELLOWORLD 进行加密，会得到密文 LRLLHWEOOD，如下表所示。

密钥	L	U	C	K	Y
字母表中的顺序	3	4	1	2	5
明文	**H**	**E**	**L**	**L**	**O**
	W	**O**	**R**	**L**	**D**
密文	**LR**（C 列）**LL**（K 列）**HW**（L 列）**EO**（U 列）**OD**（Y 列）				

请参考上述加密方法，以 CAT 作为密钥，将明文 HOWAREYOU 转换为密文：O_____O_____A_____W_____U
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【答案选项】
A. Y。
B. E。
C. C。

D. R。
E. T。
F. H。
正确答案： 1、D　　2、F　　3、A　　4、B

第 4 章　网络数据保护

17. 在一台安装了 Windows Server 操作系统的服务器 Server17 上，管理员需要创建一个备份计划：每天 23 点备份一次服务器上的所有数据（包括应用程序和系统状态）。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：登录服务器 Server17，在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”，打开“wbadmin”控制台窗口。

步骤 2：_____

步骤 3：在“开始”对话框中，单击“下一步”。

步骤 4：在“选择备份配置”对话框中，选中“整个服务器”选项，然后单击“下一步”。

步骤 5：_____

步骤 6：在“指定目标类型”对话框中，单击“下一步”。

步骤 7：_____

步骤 8：在弹出的对话框中，勾选可用的联机磁盘，然后单击“确定”。返回上一级对话框，勾选添加的磁盘，再单击“下一步”。

步骤 9：_____

步骤 10：在“确认”对话框中，单击“完成”。

步骤 11：_____

【答案选项】

A. 在“指定备份时间”对话框中，选中“每日一次”，并设置“选择时间”为 23:00，然后单击“下一步”。
B. 在“选择目标磁盘”对话框中，单击“显示所有可用磁盘”。
C. 在“wbadmin”控制台窗口左侧导航栏中，右击“本地备份”，并单击“备份计划...”。
D. 在“摘要”对话框中，单击“关闭”。
E. 弹出警告对话框，单击“是”。
F. 在“指定备份时间”对话框中，选中“每日多次”，然后单击“下一步”。
正确答案： 1、C　　2、A　　3、B　　4、E　　5、D

18. 在一台安装了 Windows Server 操作系统的服务器 Server18 上，管理员需要立即备份一次系统状态数据。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】:

步骤 1：登录服务器 Server18，在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”，打开“wbadmin”控制台窗口。

步骤 2：_____

步骤 3：在“备份选项”对话框中，单击“下一步”。

步骤 4：在“选择备份配置”对话框中，选中“自定义”选项，然后单击“下一步”。

步骤 5：_____

步骤 6：返回上一级对话框，单击“下一步”。

步骤 7：在“指定目标类型”对话框中，单击“下一步”。

步骤 9：_____

步骤 10：在“确认”对话框中，单击“备份”。

步骤 11：_____

【答案选项】

A. 在“选择要备份的项”对话框中，单击“添加项目”，并勾选“系统状态”选项，然后单击“确定”。

B. 在“选择备份目标”对话框中，选择备份目标，再单击“下一步”。
C. 在“wbadmin”控制台窗口左侧导航栏中，右击“本地备份”，并单击“一次性备份...”。
D. 在“摘要”对话框中，单击“关闭”。
E. 在“备份进度”对话框中，单击“关闭”。
F. 在“指定备份时间”对话框中，选中“每日多次”，然后单击“下一步”。
正确答案： 1、C 2、A 3、B 4、E

19. 在一台安装了 Windows Server 操作系统的服务器 Server19 上，管理员需要创建一个备份计划：每天 22 点备份一次服务器的本地磁盘 C：上的数据。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1:登录服务器 Server19,在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”,打开“wbadmin”控制台窗口。
步骤 2：_____
步骤 3：在“开始”对话框中，单击“下一步”。
步骤 4：在“选择备份配置”对话框中，选中“自定义”选项，然后单击“下一步”。
步骤 5：_____
步骤 6：在“指定备份时间”对话框中，选中“每日一次”，并设置“选择时间”为 22:00，然后单击“下一步”。
步骤 7：在“指定目标类型”对话框中，单击“下一步”。
步骤 8：_____
步骤 9：在弹出的对话框中，勾选可用的联机磁盘，然后单击“确定”。返回上一级对话框，勾选添加的磁盘，再单击“下一步”。
步骤 10：_____
步骤 11：在“确认”对话框中，单击“完成”。
步骤 12：_____
【答案选项】
A. 在“指定备份时间”对话框中，选中“每日一次”，并设置“选择时间”为 24:00，然后单击“下一步”。
B. 在“选择目标磁盘”对话框中，单击“显示所有可用磁盘”。
C. 在“wbadmin”控制台窗口左侧导航栏中，右击“本地备份”，并单击“备份计划...”。
D. 在“摘要”对话框中，单击“关闭”。
E. 弹出警告对话框，单击“是”。
F. 在“选择要备份的项”对话框中，单击“添加项目”，然后勾选“本地磁盘（C:）”选项，并单击“确定”，返回上一级对话框，单击“下一步”。
正确答案： 1、C 2、F 3、B 4、E 5、D

20. 在一台安装了 Windows Server 操作系统的服务器 Server20 上，管理员需要立即备份一次系统状态数据到远程共享文件夹\\w2016\bak。
要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。
【操作步骤】:
步骤 1:登录服务器 Server20,在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”,打开“wbadmin”控制台窗口。
步骤 2：_____
步骤 3：在“备份选项”对话框中，单击“下一步”。
步骤 4：在“选择备份配置”对话框中，选中“自定义”选项，然后单击“下一步”。
步骤 5：_____
步骤 6：返回上一级对话框，单击“下一步”。
步骤 7：_____
步骤 8：在“指定远程文件夹”对话框中，“位置”下方的文本框中输入“\\w2016\bak”，再单击“下一步”。

步骤 9：在“确认”对话框中，单击“备份”。
步骤 10：_____
【答案选项】
A. 在“选择要备份的项”对话框中，单击“添加项目”，并勾选“系统状态”选项，然后单击“确定”。
B. 在“指定目标类型”对话框中，选择“远程共享文件夹”选项，然后单击“下一步”。
C. 在“wbadmin”控制台窗口左侧导航栏中，右击“本地备份”，并单击“一次性备份...”。
D. 在“摘要”对话框中，单击“关闭”。
E. 在“备份进度”对话框中，单击“关闭”。
F. 在“指定备份时间”对话框中，选中“每日多次”，然后单击“下一步”。
正确答案： 1、C　　2、A　　3、B　　4、E