[第四章 计算机信息系统安全技术 2](#_Toc15442)

[第五章 信息安全保密基础 25](#_Toc12336)

[第六章 数据库系统 48](#_Toc20329)

[第七章 工具软件 71](#_Toc10743)

[第八章 统一工作平台 81](#_Toc14226)

[第九章 广东地税“大集中”征管系统体系 105](#_Toc9502)

[第十章 广东地税“大集中”数据库结构及维护技术 121](#_Toc3790)

[第十一章 广东地税“大集中模式”其他信息系统介绍 155](#_Toc6771)

[第十二章 广东地税应用系统建设与维护 166](#_Toc15960)

[第十三章 信息技术普及知识 181](#_Toc23386)

第四章 计算机信息系统安全技术

一、单项选择题（在每个小题的备选答案中，只有一个答案最符合题意，请将其代码填在该题的括号内。）

1.下面哪项不属于Windows Server 2003的安全特性（ ）。（D）

A.Internet连接防火墙（ICF） B.软件限制策略

C.网页服务器安全性 D.增强的ETC

解析:Windows Server 2003的安全特性包括Internet连接防火墙（ICF）、软件限制策略、网页服务器安全性、凭证管理器、Internet认证服务器和远程认证拨号用户服务器(IAS/RADIUS)、增强的EFS等。

2.windows内置两个用户账号有Administrator和（ ）。（A）

A.Guest B.user C.Jack D.name

解析:windows内置两个用户账号：Administrator（系统管理员）和Guest（临时客户）账号。

3.域是网络对象的分组，域中的所有对象都存储在（ ）下。（B）

A.User Diredtory B.Active Directory

C.Temp Directory D.Windows Directory

解析:根据域的概念，域是网络对象的分组，域中的所有对象都存储在Active Directory下。

4.以下哪项不属于Windows应用程序与服务的安全策略（ ）。（C）

A.IIS服务

B.FTP服务

C.Windows外置服务

D.Internet Explorer浏览器以及Runas服务

解析:常见Windows应用程序与服务的安全策略包括 IIS服务、FTP服务、Windows内置服务、Internet Explorer浏览器以及Runas服务的安全策略。

5.关于Windows安全审核以下哪种说法是正确的（ ）。（D）

A.Windows安全审核指利用组策略、本地策略、站点策略以及专门软件限制病毒、木马及游戏等应用程序在客户端的运行

B.Windows安全审核指制作系统紧急恢复盘，备份系统文件

C.Windows安全审核指设定系统异常停止时Windows的对应策略

D.Windows安全审核指系统负责监视各种与安全性有关的事件

解析:根据Windows安全审核的概念，Windows安全审核是指系统负责监视各种与安全性有关的事件。

6.以下哪种说法是正确的（ ）。（B）

A.vi编辑器是UNIX系统下最常用的图形编辑器

B.UNIX的文件管理基本命令包括mkdir、chgrp、ln、cut、dd、find、grep、tar等命令

C.UNIX系统中有一个名为/abc/passwd的文件，专门用来存放用户账号的数据信息

D.UNIX系统具有开放性，用户单一性、多任务环境，功能强大、实现高效，提供丰富的网络功能和支持多处理器等特征

解析:选项A的正确说法是vi编辑器是UNIX系统下最常用的文本编辑器；选项C的正确说法是UNIX系统中有一个名为/etc/passwd的文件，专门用来存放用户账号的数据信息；选项D的正确说法是UNIX系统具有开放性，多用户、多任务环境，功能强大、实现高效，提供丰富的网络功能和支持多处理器等特征。

7.以下哪项不属于UNIX文件系统特点（ ）。（C）

A.文件系统的组织是分级树形结构

B.文件的物理结构为混合索引式文件结构

C.采用空闲表法管理空闲盘块

D.引入索引节点概念

解析:UNIX文件系统特点包括文件系统的组织是分级树形结构、文件的物理结构为混合索引式文件结构、采用了成组链接法管理空闲盘块、引入了索引节点概念。

8.以下哪个不是UNIX下入侵检测的方法（ ）。（B）

A.检查系统密码文件，查看passwd文件的修改日期

B.使用vi aef|grep inetd命令，查看进程中有没有奇怪进程

C.检查系统守护进程，检查文件/etc/inetd.conf

D.使用netstat命令，检查网络连接和监听端口

解析：使用ps aef|grep inetd命令，查看进程中有没有奇怪进程。

9.UNIX的备份命令Tar是（ ）。（A）

A.用于磁带机备份

B.把整个文件系统拷贝到备份介质上。

C.恢复整个文件系统

D.提取单个文件

解析:UNIX的备份命令包括：Tar（用于磁带机）、Dump（把整个文件系统拷贝到备份介质上）、Restore（恢复整个文件系统或提取单个文件）。

10.在UNIX系统中错误日志是由（ ）。（B）

A.lastlog执行 B.syslogd执行 C.WTMP执行 D.pgpe执行

解析: 在UNIX系统中错误日志是由syslogd执行。

11.以下哪个不是数据库审计类型（ ）。（C）

A.语句审计 B.特权审计 C.程序审计 D.对象审计

解析:数据库审计类型包括语句审计、特权审计、对象审计三种。

12.数据库的数据备份方法包括：冷备份、（ ）和逻辑备份三种。（A）

A.热备份 B.程序备份 C.字段备份 D.字节备份

解析:数据备份的方法包括：冷备份、热备份和逻辑备份三种。

13.数据库的热备份依赖于（ ）进行备份。（B）

A.数据库的系统文件 B.数据库的日志文件

C.数据库的硬件配置文件 D.注册表文件

解析:热备份依赖于数据库的日志文件进行备份。

14.数据库的语句审计，是对某种类型的（ ）语句审计。（C）

A.C++ B.Basic C.SQL D.JAVA

解析:数据库的语句审计，是对某种类型的SQL语句审计，不指定结构或对象。

15.（ ）是指使数据库的数据全部或部分丢失，并影响正在存取出错介质上的数据的事务。（B）

A.系统故障 B.介质故障 C.网络故障 D.文件故障

解析:介质故障是指外存故障，介质故障使数据库的数据全部或部分丢失，并影响正在存取出错介质上的数据的事务。

16.电子计算机机房应设火灾自动报警系统，并应符合现行国家标准（ ）的规定。（A）

A.《火灾自动报警系统设计规范》 B.《电力设计规范》

C.《消防设备规范》 D.《机房电源设计规范》

解析:电子计算机机房应设火灾自动报警系统，并应符合现行国家标准《火灾自动报警系统设计规范》的规定。

17.以下哪个说法是正确的（ ）。（C）

A.主机房不宜采用感烟探测器。

B.当主机房内设置空调设备时，不应受主机房内电源切断开关的控制。

C.凡设置二氧化碳或卤代烷固定灭火系统及火灾探测器的电子计算机机房，其吊顶的上、下及活动地板下，均应设置探测器和喷嘴。

D.电子计算机机房的安全设计还应符合现行国家标准《计算机病毒安全防护要求》的规定。

解析:选项A的正确说法是主机房不采用感烟探测器；选项B的正确说法是当主机房内设置空调设备时，应受主机房内电源切断开关的控制；选项D的正确说法是电子计算机机房的安全设计还应符合现行国家标准《计算站场地安全要求》的规定。

18.以下哪项不属于机房防盗要求（ ）。（A）

A.放置计算机设备的建筑物应该比较显眼，要用相关的标志标明机房所在地

B.机房门窗应具备防盗措施，如加固门窗和安装监视器等

C.机房贵重设备应配置具有防盗功能的安全保护设备，如各种锁定装置、入侵报警器等

D.严格人员出入登记制度，加强机房管理责任制

解析:机房防盗要求包括：放置计算机设备的建筑物应该比较隐蔽，不要用相关的标志标明机房所在地;机房门窗应具备防盗措施，如加固门窗和安装监视器等;机房贵重设备应配置具有防盗功能的安全保护设备，如各种锁定装置、入侵报警器等;严格人员出入登记制度，加强机房管理责任制。

19. 关于电磁干扰的描述正确的是（ ）。（D）

A.电磁干扰是电子设备的杂散电磁能量通过导线获得空间向外扩散

B.电磁干扰只能通过红外线途径向外传播

C.电磁干扰是指通过降低电磁噪声增加辐射泄漏信息的总体信噪比，达到“掩盖”真实信息的目的

D.电磁干扰是指无用的电磁信号对接收的有用的电磁信号造成的扰乱

解析:选项A的正确说法是电磁泄漏是指电子设备的杂散电磁能量通过导线获得空间向外扩散；选项B的正确说法是电磁泄漏和电磁干扰都是通过辐射和传导等两种途径向外传播；选项C的正确说法是电磁防护的其中一个措施是通过增加电磁噪声降低辐射泄漏信息的总体信噪比，达到“掩盖”真实信息的目的。

20.基于镜像数据库的恢复是指（ ）。（B）

A.当数据库失效时，可取最近一次的数据库备份来恢复数据库，即把备份的数据拷贝到原数据库所在的位置上

B.当主库出现故障时，可由镜像磁盘继续提供使用，同时DBMS自动利用镜像磁盘数据进行恢复

C.当数据库失效时，通过事务的回滚和重做可把数据库恢复到故障前某一时刻

D.使用操作系统恢复光盘对数据库进行恢复

解析:基于镜像数据库的恢复是当主库出现故障时，可由镜像磁盘继续提供使用，同时DBMS自动利用镜像磁盘数据进行恢复。

21.在Windows中，存储计算机配置和缺省用户设置的注册表数据被保存在（　）目录中。（C）

A.Program Files\Java

B.Program Files\Oracle

C.system32\config

D.Documents and Settings\Administrator

解析:计算机配置和缺省用户设置的注册表数据在Windows中被保存在system32/config目录中的五个文件中：DEFAULT，SAM，SECURITY，SOFTWARE，SYSTEM，NTUSER.DAT。

22. 常见文件系统NTFS是（　）。（C）

A.File Allocation Table（文件分配表），是一个简单的文件系统，最初为DOS操作系统设计，适用于小容量的磁盘，具有简单的目录结构。

B.文件系统的文件分配表簇标识为32位，具有更强的寻址能力，能够比FAT16更有效地管理磁盘，支持长文件格式和Unicode编码。

C.windows NT推出的一种具有较好的容错性和安全性的全新的文件系统，具有原子事务、综合的安全模型、基于软件的数据冗余方案等等新特性。

D.UNIX推出的一种具有较好的容错性和安全性的全新的文件系统，具有原子事务、综合的安全模型、基于软件的数据冗余方案等等新特性。

解析:选项A是FAT文件系统；选项B是FAT32文件系统；选项D是UNIX系统。

23．（　）是UNIX的一个功能强大的命令解释器，是UNIX系统对外的接口界面。（D）

A.SHEID B.BASH C.TAR D.Shell

解析:Shell是UNIX的一个功能强大的命令解释器，是UNIX系统对外的接口界面。

24.关于UNIX系统，以下哪个说法不正确（　）。（C）

A.连接时间日志，由多个程序执行。它把记录写入到/var/log/

wtmp文件和/var/run/utmp文件，1ogin等程序会更新wtmp和utmp文件，使系统管理员能够跟踪到谁在何时登录到系统

B.UNIX文件许可机制将用户分为三类：文件所有者(u)、同组用户(g)、其他用户(o)，而三种用户对应的权限则分为：读、写和执行等三种

C.错误日志，由系统内核执行。当一个进程终止时，为每个进程往进程统计文件（pacet或acct）中写一个记录，进程统计的目的是为系统中的基本服务提供命令使用统计

D.UNIX文件备份策略包括第0天备份、完全备份、增量式备份、特别备份

解析:进程统计日志，由系统内核执行。当一个进程终止时，为每个进程往进程统计文件（pacet或acct）中写一个记录，进程统计的目的是为系统中的基本服务提供命令使用统计。错误日志，由syslogd执行。各种系统守护进程、用户程序和内核通过syslog向var/log/messages文件报告值得注意的事件。

25. UNIX对系统用户登陆的安全审计的工具有（　）。（A）

A.lastlog和WTMP程序 B.sdslog程序

C.UUMP程序 D.DUMP和CAMP程序

解析:对系统用户登陆的安全审计，审计工具有lastlog和WTMP程序。

26.以下关于数据库的说法不正确的是（　）。（D）

A.数据库的完整性包括数据库物理完整性和逻辑完整性

B.数据库的保密性指不允许未经授权的用户存取数据

C.数据库的可用性，指不应拒绝授权用户对数据库的正常操作，同时保证系统的运行效率并提供用户友好的人机交互

D.物理完整性包括语义完整性和操作完整性

解析:逻辑完整性指对数据逻辑结构的保护，包括语义完整性和操作完整性。

27.以下关于数据库安全管理原则的哪种说法不正确（　）。（C）

A.账号安全原则：包括更改默认密码、应用适当的密码设置、登录失败时实施账号锁定、对数据提供有限制的访问权限、禁止休眠状态的用户账号、管理账号的生命周期等

B.有效设计原则：企业应针对自己的应用和数据库活动定义设计策略

C.最大原则：从需求和工作职能两方面严格限制对数据库的访问权，最大原则可确保数据库功能限制和对特定数据的访问

D.管理细分和委派原则：通过功能细分和可信赖的用户群进一步细分数据库管理的责任和角色，委派管理有助于灵活解决为员工重设密码等常见问题

解析:最小原则：从需求和工作职能两方面严格限制对数据库的访问权，最小原则可确保数据库功能限制和对特定数据的访问。

28.以下哪个是数据库加密的特点（　）。（A）

A.数据库密码系统应采用公开密钥，采用多级密钥结构

B.数据库密码系统应采用私有密钥，采用多级密钥结构

C.数据库密码系统应采用公开密钥，采用单级密钥结构

D.数据库密码系统应采用私有密钥，采用单级密钥结构

解析:数据库加密的特点包括数据库密码系统应采用公开密钥；采用多级密钥结构。

29.以下关于机房静电的防护措施哪个不正确（　）。（A）

A.机房内应使用地毯、挂毯等物品

B.机房计算机系统应有一套合理的接地与屏蔽系统

C.机房内应保持一定的湿度，在干燥季节应该加湿

D.机房内工作台面及座椅的材料应该是导静电的，而且必须进行静电接地

解析:机房内应严禁使用地毯、挂毯等容易产生静电的物品。

30.以下关于电磁防护措施哪个不正确（　）。（A）

A.将计算机和辅助设备用非屏蔽材料封闭起来

B.滤波电路可以让一定频率范围的电信号通过而阻止其他频率的信号

C.将信息系统系统中需要重点防护的设备从系统中分离出来，加以特别保护

D.选用低辐射设备防止计算机辐射泄密的根本措施

解析:电磁防护措施中的屏蔽措施是指将计算机和辅助设备用屏蔽材料封闭起来。

二、多项选择题（在每个小题的备选答案中，至少有两个或两个以上个答案最符合题意，请将其代码填在该题的括号内。）

1.在Windows系统中，以下哪些属于用户账号管理及组的管理（　）。（ABCD）

A.添加用户账号 B.管理用户账号

C.添加组 D.指定用户隶属的组

解析:用户账号管理及组的管理包括添加用户账号、管理用户账号、添加组、指定用户隶属的组、管理组等操作。

2.常用备份和恢复Windows系统的方法（　）。（ABC）

A.通过制作系统紧急恢复盘，备份系统文件

B.备份硬件配置文件

C.备份注册表文件

D.重新安装Windows操作系统

解析:常用备份和恢复Windows系统的方法包括：通过制作系统紧急恢复盘，备份系统文件；备份硬件配置文件；备份注册表文件；制作系统的启动盘；备份整个系统；创建系统还原点；设定系统异常停止时Windows的对应策略。

3.UNIX常用的文件类型有哪些（　）。（ABC）

A.普通文件 B.目录文件 C.特殊文件 D.原始文件

解析:UNIX常用的文件类型包括普通文件、目录文件和特殊文件等三种类型。

4.常见的UNIX系统漏洞有哪些（　）。（ABCD）

A.BIND域名系统漏洞 B.明文服务

C.CDEToolTalk安全漏洞 D.Buffer Overflow漏洞

解析:常见的UNIX系统漏洞包括BIND域名系统漏洞、远程过程调用(RPC)漏洞、Apache网页服务器漏洞、UNIX常见的弱口令或者弱口令的认证帐户、明文服务、UNIX “login”程序漏洞、UNIX通信功能CDEToolTalk安全漏洞、UNIX主机常见的Buffer Overflow漏洞。

5.以下哪些不是X-Window基本操作命令（　）。（CD）

A.startx B.xlsfonts C.xlttoms D.ssbxhost

解析:X-Window基本操作命令包括启动X-Window系统—startx；.显示设置工具—system-config-display；计算显示设备VESA驱动GTF模式命令行工具—gtf；显示客户端程序—xlsclients；显示X Server使用的字体—xlsfonts；显示X服务器的基本定义—xlsatoms；控制访问X Server的主机—xhost；设置X-Window系统使用偏好—xset。

6.UNIX的文件备份策略有（　）。（ACD）

A.第0天备份 B.减量式备份 C.完全备份 D.增量式备份

解析:文件备份策略：第0天备份、完全备份、增量式备份、特别备份。

7.数据库加密的特点有哪些（　）。（AB）

A.数据库密码系统应采用公开密钥

B.采用多级密钥结构

C.数据库密码系统应采用私有密钥

D.采用一级密钥结构

解析:数据库加密的特点包括数据库密码系统应采用公开密钥；采用多级密钥结构。

8.常用的数据库加密技术有哪些（　）。（ABC）

A.基于文件的数据库加密技术 B.基于记录的数据库加密技术

C.子密钥数据库加密技术 D.备份数据库的密码

解析:常用的数据库加密技术包括基于文件的数据库加密技术，基于记录的数据库加密技术，子密钥数据库加密技术等。

9.数据库的安全管理原则包括（　）。（ABCD）

A.管理细分和委派原则 B.最小权限原则

C.账号安全原则 D.有效审计原则

解析:数据库的安全管理原则包括管理细分和委派原则、最小权限原则、账号安全原则、有效审计原则。

10.以下哪些机房防护的说法是正确的（　）。（ABCD）

A.机房计算机系统应有一套合理的接地与屏蔽系统

B.机房要保证安装防静电地板

C.使用符合要求的不间断电源UPS

D.机房内工作台面及座椅的材料应该是导静电的，而且必须进行静电接地

解析:机房静电的防护措施包括机房内应严禁使用地毯、挂毯等容易产生静电的物品；机房计算机系统应有一套合理的接地与屏蔽系统；机房要保证安装防静电地板；机房内工作台面及座椅的材料应该是导静电的，而且必须进行静电接地；机房内应保持一定的湿度，在干燥季节应该加湿。

11.以下关于Windows Server 2003用户密码设置的基本原则哪些是正确的（　）。（ABCD）

A.用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符

B.用户密码不要太规则，不要使用用户姓名、生日、电话号码以及常用单词作为密码

C.根据Windows系统密码的散列算法原理，密码长度设置应超过7位，最好为14位

D.密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上且包含密码的文件是只读的

解析:Windows Server 2003 用户密码设置的基本原则：用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符；用户密码不要太规则，不要使用用户姓名、生日、电话号码以及常用单词作为密码；根据Windows系统密码的散列算法原理，密码长度设置应超过7位，最好为14位；密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上且包含密码的文件是只读的。

12. windows内置的用户账号有（　）。（AD）

A.Administrator B.User C.Name D.Guest

解析:windows内置两个用户账号：Administrator（系统管理员）和Guest（临时客户）账号。

13. 在Windows中，计算机配置和缺省用户设置的注册表数据被保存在system32/config目录中的哪些文件中（　）。（ACD）

A.DEFAULT B.ADMIN C.SECURITY D.SOFTWARE

解析:计算机配置和缺省用户设置的注册表数据在Windows中被保存在system32/config目录中的五个文件中：DEFAULT，SAM，SECURITY，SOFTWARE，SYSTEM，NTUSER.DAT。

14.保护注册表的方法有哪些（　）。（ABCD）

A.使用Windows备份软件

B.在安全模式下复制注册表文件

C.使用微软配置备份来备份注册表文件

D.导出注册表

解析:保护注册表的方法包括使用Windows备份软件，在安全模式下复制注册表文件，使用微软配置备份来备份注册表文件，导出注册表。

15.以下哪些是常见的Windows应用程序与服务的安全策略（　）。（BC）

A.IOS服务 B.FTP服务

C.Windows内置服务 D.Runer服务的安全策略

解析:常见Windows应用程序与服务的安全策略包括 IIS服务、FTP服务、Windows内置服务、Internet Explorer浏览器以及Runas服务的安全策略。

16. Windows安全审核指系统负责监视各种与安全性有关的事件，被审核的事件类型包括（　）。（ABCD）

A.访问对象 B.用户和组账号的管理

C.用户登录 D.从系统注销

解析:Windows安全审核指系统负责监视各种与安全性有关的事件，被审核的事件类型包括：访问对象；用户和组账号的管理；用户登录以及从系统注销。

17. 以下哪些是UNIX系统具有的特征（　）。（CD）

A.封闭性 B.单用户、单任务环境

C.提供丰富网络功能 D.支持多处理器

解析:UNIX系统具有开放性，多用户、多任务环境，功能强大、实现高效，提供丰富的网络功能和支持多处理器等特征，UNIX系统由系统内核、常驻模块、shell等部分构成。

18.常用到的shell命令有哪些（　）。（ABD）

A.cp B.mv C.dir D.ls

解析:常用到的shell命令包括cp、mv、rm、mkdir、ls、ln、cat等命令。

19.UNIX文件系统特点有以下哪些（　）。（BCD）

A.文件系统的组织是星形结构

B.文件的物理结构为混合索引式文件结构

C.采用了成组链接法管理空闲盘块

D.引入了索引节点概念

解析:UNIX文件系统特点包括文件系统的组织是分级树形结构；文件的物理结构为混合索引式文件结构；采用了成组链接法管理空闲盘块；引入了索引节点概念。

20.UNIX文件加密工具有以下哪些（　）。（ABCD）

A.pgpe(加密) B.pgps(签名)

C.pgpv(确认/解密) D.pgpk(管理密钥)

解析:文件加密工具包括pgpe(加密)、pgps(签名)、pgpv(确认/解密)、pgpk(管理密钥)等的使用。

21. UNIX备份命令包括（　）。（ABC）

A.Tar B.Dump C.Restore D.Reset

解析:UNIX备份命令包括Tar（用于磁带机）、Dump（把整个文件系统拷贝到备份介质上）、Restore（恢复整个文件系统或提取单个文件）。

22.以下关于UNIX下对用户的安全审计方法哪些是正确的（　）。（ABD）

A.对系统用户登陆的安全审计，审计工具有lastlog和WTMP程序

B.对FTP服务的安全审计，使用syslog

C.对在线用户的安全审计，使用what或w查看UTMP日志记录

D.对网络的安全审计，使用syslog记录各种程序产生的日志记录

解析:UNIX下对用户的安全审计方法包括对系统用户登陆的安全审计，审计工具有lastlog和WTMP程序；对FTP服务的安全审计，使用syslog；对在线用户的安全审计，使用who或w查看UTMP日志记录；对网络的安全审计，使用syslog记录各种程序产生的日志记录。

23. 数据库审计的类型有哪些（　）。（ACD）

A.语句审计 B.数据审计 C.对象审计 D.特权审计

解析:数据库审计类型包括语句审计、特权审计、对象审计三种。

24. 以下哪些关于数据库备份方法的描述是正确的（　）。（BD）

A.热备份，此时数据库处于关闭状态，能够较好的保证数据库的完整性

B.逻辑备份，使用软件从数据库中提取数据并将结果写到一个文件上

C.冷备份，数据库正处于运行状态，这种方法依赖于数据库的日志文件进行备份

D.热备份，数据库正处于运行状态，这种方法依赖于数据库的日志文件进行备份

解析:选项A的正确说法是热备份，数据库正处于运行状态，这种方法依赖于数据库的日志文件进行备份；选项C的正确说法是冷备份，此时数据库处于关闭状态，能够较好的保证数据库的完整性。

25.以下哪些是网络核心机房的环境因素（　）。（ABCD）

A.供电系统 B.制冷系统 C.机柜系统 D.消防系统

解析:网络核心机房的环境因素包括供电系统、制冷系统、机柜系统、消防系统、监控系统等关键物理基础设施。

26.以下关于机房防盗要求的描述哪些是正确的（　）。（ABC）

A.机房门窗应具备防盗措施，如加固门窗和安装监视器等

B.机房贵重设备应配置具有防盗功能的安全保护设备，如各种锁定装置、入侵报警器等

C.严格人员出入登记制度，加强机房管理责任制

D.放置计算机设备的建筑物应该比较显眼，应用相关的标志标明机房所在地

解析:选项D的正确说法是机房防盗要求包括放置计算机设备的建筑物应该比较隐蔽，不要用相关的标志标明机房所在地。

27.以下哪些关于机房电磁防护的说法是正确的（　）。（ABCD）

A.电磁泄漏是指电子设备的杂散电磁能量通过导线获得空间向外扩散

B.电磁干扰指无用的电磁信号对接收的有用的电磁信号造成的扰乱

C.电磁泄漏和电磁干扰都可通过辐射等途径向外传播

D.电磁泄漏和电磁干扰都可通过传导等途径向外传播

解析:电磁泄漏、电磁干扰的原理：电磁泄漏是指电子设备的杂散电磁能量通过导线获得空间向外扩散；电磁干扰指无用的电磁信号对接收的有用的电磁信号造成的扰乱；电磁泄漏和电磁干扰都是通过辐射和传导等两种途径向外传播。

三、判断辨析题（正确的在题后的括号内划“√”；错误的在题后的括号内划“×”，改正并简述理由。）

1.密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上且包含密码的文件是只读的。（√）

2.计算机配置和缺省用户设置的注册表数据在Windows中只被保存在system32/config目录中的两个文件中：DEFAULT和NTER.DAT。（×）

解析：计算机配置和缺省用户设置的注册表数据在Windows中被保存在system32/config目录中的五个文件中：DEFAULT，SAM，SECURITY，SOFTWARE，SYSTEM，NTUSER.DAT。

3.UNIX文件许可机制将用户分为三类：文件所有者(u)、同组用户(g)、其他用户(o)，而三种用户对应的权限则分为：读、写和执行等三种。（√）

4.UNIX的文件管理基本命令包括mkdir、chgrp、ln、cut、dD.finD.grep、tar等命令。（√）

5.UNIX的入侵恢复步骤包括入侵恢复前期准备工作、取回对系统的控制权、系统入侵分析、系统恢复、提高系统安全性、系统重新接入Internet、更新安全策略等。（√）

6.数据库恢复的方法包括基于备份的恢复、基于运行时日志的恢复和基于镜像数据库的恢复。（√）

7.数据库加密就是将密文数据经过一定的交换(一般为变序和代替)变成明文数据。（×）

解析：数据库加密就是将明文数据经过一定的交换(一般为变序和代替)变成密文数据。

8.数据库系统故障主要是由于服务器在运行过程中，突然发生硬件错误(如CPU故障)、操作系统故障、DBMS错误、停电等原因造成的非正常中断，致使整个系统停止运行，所有事务全部突然中断。（√）

9.机房内应可以使用地毯、挂毯等的物品（×）

解析：机房内应严禁使用地毯、挂毯等容易产生静电的物品。

10.机房计算机设备的供电线路应使用专门线路。（√）

11. 用户账号能够让用户以授权的身份登录到计算机和域中并访问资源，windows内置两个用户账号：User（系统管理员）和Name（临时客户）账号。（×）

解析：用户账号能够让用户以授权的身份登录到计算机和域中并访问资源，windows内置两个用户账号：Administrator（系统管理员）和Guest（临时客户）账号。

12. UNIX系统中有一个名为/est/passwd的文件，专门用来存放用户账号的数据信息。（×）

解析：UNIX系统中有一个名为/etc/passwd的文件，专门用来存放用户账号的数据信息。

13. UNIX文件系统的组织是星形结构。（×）

解析：UNIX文件系统的组织是分级树形结构。

14. UNIX文件加密工具包括pfgf(加密)、plep(签名)、pgpv(确认/解密)、pgpk(管理密钥)等的使用。（×）

解析：UNIX文件加密工具包括pgpe(加密)、pgps(签名)、pgpv(确认/解密)、pgpk(管理密钥)等的使用。

15. UNIX为保障系统的安全运行提供了丰富的日志文件，其中连接时间日志，由多个程序执行。它把记录写入到/lar/log/wtmp文件和/lar/run/utmp文件。（×）

解析：UNIX为保障系统的安全运行提供了丰富的日志文件，其中连接时间日志，由多个程序执行。它把记录写入到/var/log/wtmp文件和/var/run/utmp文件。

16.对系统用户登陆的安全审计，审计工具有lastlog和WTMP程序。（√）

17.数据库密码系统应采用私有密钥。采用单级密钥结构。（×）

解析：数据库密码系统应采用公开密钥。采用多级密钥结构。

18. 数据库审计类型包括评估审计、文书审计、分级审计三种。（×）

解析：数据库审计类型包括语句审计、特权审计、对象审计三种。

19. 数据备份的方法包括：冷备份、热备份和逻辑备份三种。（√）

20. 机房内工作台面及座椅的材料应该是导静电的，而且必须进行静电接地。（√）

21. 当主机房内设置空调设备时，应不受主机房内电源切断开关的控制。机房内的电源切断开关不应靠近工作人员的操作位置或主要出入口。（×）

解析：当主机房内设置空调设备时，应受主机房内电源切断开关的控制。机房内的电源切断开关应靠近工作人员的操作位置或主要出入口。

22. 机房防盗要求中放置计算机设备的建筑物应该比较显眼，应用相关的标志标明机房所在地。（×）

解析：机房防盗要求中放置计算机设备的建筑物应该比较隐蔽，不要用相关的标志标明机房所在地。

23. 电磁泄漏指无用的电磁信号对接收的有用的电磁信号造成的扰乱。（×）

解析：电磁干扰指无用的电磁信号对接收的有用的电磁信号造成的扰乱。

24. 电磁泄漏和电磁干扰都是通过辐射和传导等两种途径向外传播。（√）

四、简答题

1.请问WINDOWS文件系统中的FAT指的是什么？

答：FAT是File Allocation Table（文件分配表），是一个简单的文件系统，最初为DOS操作系统设计，适用于小容量的磁盘，具有简单的目录结构。

2.请简单描述什么是UNIX shell命令解析器？

答：Shell是UNIX的一个功能强大的命令解释器，是UNIX系统对外的接口界面。

3.请问什么是数据库审计？

答：数据库审计指监视和记录用户对数据库所施加的各种操作的机制。

4.请解释什么是数据库的安全管理原则中的最小原则。

答：最小原则是从需求和工作职能两方面严格限制对数据库的访问权，最小原则可确保数据库功能限制和对特定数据的访问。

5.Windows文件访问安全的措施有哪些？

答：Windows文件访问安全的措施包括使用EFS保护数据，部署基于NTFS的权限管理，启用文件审核管理，更安全地部署共享文件夹，限制用户空间使用，以及在写入数据时对数据的写入进行限制。

6.UNIX的文件加密工具包括哪些？

答：包括pgpe(加密)、pgps(签名)、pgpv(确认/解密)、pgpk(管理密钥)等的使用。

7.Windows系统监控审核与通信安全常用方法有哪些？

答：（1）日志、事件、性能日志和警报等的查看与使用。

（2）在通信安全中对端口进行限制、查看、关闭、屏蔽、启用等。

8.网络核心机房的环境因素有哪些？

答：包括供电系统、制冷系统、机柜系统、消防系统、监控系统等关键物理基础设施。

9.机房静电的危害有哪些？

答：静电对计算机的主要危害是由于静电噪声对电子线路的干扰，引起电位的瞬间改变，导致存储器中的信息丢失或误码。静电不仅会使计算机设备的运转出故障，还对影响操作人员的身心健康。

10.机房电源系统的防护措施有哪些？

答: （1）计算机设备的供电线路应使用专门线路。

（2）使用符合要求的不间断电源UPS。

（3）并配置应急电源、安全保护地、防雷接地。

11.在WINDOWS中，保护注册表的方法有哪些？

答：保护注册表的方法包括使用Windows备份软件，在安全模式下复制注册表文件，使用微软配置备份来备份注册表文件，导出注册表。

12.UNIX的文件备份策略有哪些？

答：文件备份策略包括：第0天备份、完全备份、增量式备份、特别备份。

13.常用的数据库加密技术有哪些？

答：常用的加密技术包括：基于文件的数据库加密技术，基于记录的数据库加密技术，子密钥数据库加密技术等。

14.数据库恢复的方法有哪些？

答：包括基于备份的恢复、基于运行时日志的恢复和基于镜像数据库的恢复。

15. UNIX的入侵恢复步骤是怎样的？

答：步骤为入侵恢复前期准备工作、取回对系统的控制权、系统入侵分析、系统恢复、提高系统安全性、系统重新接入Internet、更新安全策略等。

16. UNIX常用的文件类型有哪些？

答：包括普通文件、目录文件和特殊文件等三种类型。

17. 简述UNIX文件的许可机制。

答：UNIX将用户分为三类：文件所有者(u)、同组用户(g)、其他用户(o)，而三种用户对应的权限则分为：读、写和执行等三种。

18.简述机房电磁泄漏的原理。

答：机房电磁泄漏是指电子设备的杂散电磁能量通过导线获得空间向外扩散。