信息安全技术教程习题及答案

第一章 概述

一、判断题

1. 信息网络的物理安全要从环境安全和设备安全两个角度来考虑。√

2. 计算机场地可以选择在公共区域人流量比较大的地方。×

3. 计算机场地可以选择在化工厂生产车间附近。×

4. 计算机场地在正常情况下温度保持在 18~28 摄氏度。√

5. 机房供电线路和动力、照明用电可以用同一线路。×

6. 只要手干净就可以直接触摸或者擦拔电路组件，不必有进一步的措施。×

7. 备用电路板或者元器件、图纸文件必须存放在防静电屏蔽袋内，使用时要远离静电敏感器件。√

8. 屏蔽室是一个导电的金属材料制成的大型六面体，能够抑制和阻挡电磁波在空气中传播。√

9. 屏蔽室的拼接、焊接工艺对电磁防护没有影响。×

10. 由于传输的内容不同，电力线可以与网络线同槽铺设。×

11. 接地线在穿越墙壁、楼板和地坪时应套钢管或其他非金属的保护套管，钢管应与接地线做电气连通. √

12. 新添设备时应该先给设备或者部件做上明显标记，最好是明显的无法除去的标记 ,以防更换和方便查找赃物。√

13.TEMPEST 技术，是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器 件、集成电路、连接线、显示器等采取防辐射措施于从而达到减少计算机信息泄露的最终目的。√

14. 机房内的环境对粉尘含量没有要求。×

15. 防电磁辐射的干扰技术，是指把干扰器发射出来的电磁波和计算机辐射出来的电磁波混合在一起，以掩盖原泄露信息的内容和特征等，使窃密者即使截获这一混合信号也无法提取其中的信息。√

16. 有很高使用价值或很高机密程度的重要数据应采用加密等方法进行保护。√

17. 纸介质资料废弃应用碎纸机粉碎或焚毁。√

二、单选题

1. 以下不符合防静电要求的是

A. 穿合适的防静电衣服和防静电鞋　B. 在机房内直接更衣梳理　C. 用表面光滑平整的办公家具

D. 经常用湿拖布拖地

2. 布置电子信息系统信号线缆的路由走向时，以下做法错误的是

A. 可以随意弯折　　B. 转弯时，弯曲半径应大于导线直径的 10 倍

C. 尽量直线、平整　　D. 尽量减小由线缆自身形成的感应环路面积

3. 对电磁兼容性 (Electromagnetic Compatibility, 简称 EMC) 标准的描述正确的是

A. 同一个国家的是恒定不变的　B. 不是强制的　C. 各个国家不相同　D. 以上均错误

4. 物理安全的管理应做到

A. 所有相关人员都必须进行相应的培训，明确个人工作职责

B. 制定严格的值班和考勤制度，安排人员定期检查各种设备的运行情况

C. 在重要场所的进出口安装监视器，并对进出情况进行录像

D. 以上均正确

三、多选题

1. 场地安全要考虑的因素有

A. 场地选址　B. 场地防火　C. 场地防水防潮 D. 场地温度控制 E. 场地电源供应

2. 火灾自动报警、自动灭火系统部署应注意

A. 避开可能招致电磁干扰的区域或设备　B. 具有不间断的专用消防电源

C. 留备用电源　D. 具有自动和子动两种触发装置

3. 为了减小雷电损失，可以采取的措施有

A. 机房内应设等电位连接网络　B. 部署 UPS

C. 设置安全防护地与屏蔽地

D. 根据雷击在不同区域的电磁脉冲强度划分，不同的区域界面进行等电位连接 E. 信号处理电路

4. 会导致电磁泄露的有

A. 显示器　B. 开关电路及接地系统　C. 计算机系统的电源线　D. 机房内的电话线　E. 信号处理电路

5. 磁介质的报废处理，应采用

A. 直接丢弃　B.砸碎丢弃　C. 反复多次擦写 D.内置电磁辐射干扰器

6. 静电的危害有

A. 导致磁盘读写错误，损坏磁头，引起计算机误动作

B. 造成电路击穿或者毁坏

C. 电击，影响工作人员身心健康

D. 吸附灰尘

7. 防止设备电磁辐射可以采用的措施有

A. 屏蔽机　　B. 滤波

C. 尽量采用低辐射材料和设备、D.内置电磁辐射干扰器

四、问答题

1. 物理安全包含哪些内容 ？

2. 解释环境安全与设备安全的联系与不同。

第三章

容灾与数据备份

一、判断题

1. 灾难恢复和容灾具有不同的含义。×

2. 数据备份按数据类型划分可以分成系统数据备份和用户数据备份。√

3. 对目前大量的数据备份来说，磁带是应用得最泞的介质。√

4. 增量备份是备份从上 J 知韭行完全备份后更拔的全部数据文件。×

5. 容灾等级通用的国际标准 SHARE 78 将容灾分成了六级。×

6. 容灾就是数据备份。×

7. 数据越重要，容灾等级越高。√

8. 容灾项目的实施过程是周而复始的。√

9. 如果系统在一段时间内没有出现问题，就可以不用再进行容灾了。×

10.SAN 针对海量、面向数据块的数据传输，而 NAS 则提供文件级的数据访问功能。√

11. 廉价磁盘冗余阵列 (RAID), 基本思想就是将多只容量较小的、相对廉价的硬盘进行有机组合，使其性能超过一只昂贵的大硬盘。√

二、单选题

1. 代表了当灾难发生后，数据的恢复程度的指标是

A.RPO B.RTO C.NRO D.SDO

2. 代表了当灾难发生后，数据的恢复时间的指标是

A.RPO B.RTO C.NRO D.SD0

3. 我国《重要信息系统灾难恢复指南》将灾难恢复分成了级

A. 五　　B. 六　　C. 七　　D. 八

4. 下图是一一一存储类型的结构图。

A.NAS　　B.SAN　　C.以上都不是

5. 容灾的目的和实质是

A. 数据备份　B.心理安慰　C. 保持信息系统的业务持续性　D.系统的有益补充

6. 容灾项目实施过程的分析阶段，需要进行

A. 灾难分析　　B. 业务环境分析

C. 当前业务状况分析　　D. 以上均正确

7. 目前对于大量数据存储来说，容量大、成本低、技术成熟、广泛使用的介质是一一一。

A.磁盘　　B. 磁带　　c. 光盘　　D. 自软盘

8. 下列叙述不属于完全备份机制特点描述的是一一一。

A. 每次备份的数据量较大　　B. 每次备份所需的时间也就校长

C. 不能进行得太频繁　D. 需要存储空间小

9. 下面不属于容灾内容的是

A. 灾难预测 B.灾难演习 C. 风险分析 D.业务影响分析

三、多选题

1. 信息系统的容灾方案通常要考虑的要点有一一。

A. 灾难的类型　　B. 恢复时间

C. 恢复程度　　D. 实用技术

E 成本

2. 系统数据备份包括的对象有一一一。

A. 配置文件　　B.日志文件 C. 用户文档　D.系统设备文件

3. 容灾等级越高，则一一一。

A. 业务恢复时间越短 C. 所需要成本越高　　B. 所需人员越多　　D. 保护的数据越重要

四、问答题

1. 容灾的含义是什么 ？容灾过程包括哪些内容 ？

2. 容灾与备份之间是什么关系 ？

3. 容灾等级通用的国际标准 SHARE 78 将容灾划分成几个层次 ？简单概述各层次的特点。

4. 设计一个以星期为周期的备份策略，并举例描述在其中某一天发生＇灾难如何恢复。

第四章

基础安全技术

一、判断题

1. 对称密码体制的特征是：加密密钥末日解密密钥完全相同，或者一个密钥很容易从另一个密钥中导出 √

2. 公钥密码体制算法用一个密钥进行加密，而用另一个不同但是有关的密钥进行解密。 √

3. 公钥密码体制有两种基本的模型：一种是加密模型，另一种是认证模型。 √

4. 对信息的这种防篡改、防删除、防插入的特性称为数据完整性＇保护。 √

5.P 阻是利用公开密钥技术所构建的、解决网络安全问题的、普遍适用的一种基础设施。 √

二、多选题

1.PKI 系统的基本组件包括斗 -一。

A. 终端实体 B.认证机构 C. 注册机构 D证书撤销列表发布者 E. 证书资料库 F.密钥管理中心

2. 数字证书可以存储的信息包括

A. 身份证号码、社会保险号、驾驶证号码

B. 组织工商注册号、组织组织机构代码、组织税号

C.IP 地址

D.Email 地址

3.PKI 提供的核心服务包括

A. 认证 B. 完整性 C. 密钥管理 D. 简单机密性 E. 非否认

第五章

系统安全

一、判断题

1. 常见的操作系统包括 DOS 、 OS/2 、τ UNIX 、 XENIX 、 LinukWindows 、 Netware 、 Oracle 等。 ×

2. 操作系统在概念上一般分为两部分：内核 (Kernel) 以及壳 (SheIl), 有些操作系统 的内核与壳完全分开（ 如 MicrosoftWindows 、 UNIX 、 Linux 等); 另一些的内核与壳关系紧 密（ 如 UNIX 、 Linux 等λ内核及壳只是操作层次上不同而已。 ×

3.Windows 系统中，系统中的用户帐号可以由任意系统用户建立。用户帐号中包含着用户的名称与密码、用户所属的组、用户的权利和用户的权限等相关数据。 ×

4.Windows 系统的用户帐号有两种基本类型：全局帐号 (Global Accounts) 和本地帐号(heal Accounts) √

5. 本地用户组中的 Users（ 用户 ）组成员可以创建用户帐号和本地组，也可以运行应用程序，但是不能安装应用程序，也可以关闭和锁定操作系统。 ×

6. 本地用户组中的 Guests-（ 来宾用户 ）组成员可以登录和运行应用程序，也可以关闭操作系统，但是其功能比 Users 有更多的限制。 √

7. 域帐号的名称在域中必须是唯一的，而且也不能和本地帐号名称相同，否则会引起混乱。 ×

8. 全局组是由本域的域用户组成的，不能包含任何组，也不能包含其他域的用户，全局组能在域中任何一台机器上创建。 ×

9. 在默认情况下，内置 Domain Admins 全局组是域的 Administrators 本地组的一个成员 ,也是域中每台机器 Administrator 本地组的成员 o √

10.Windows XP 帐号使用密码对访问者进行身份验证，密码是区分大小写的字符串，最多可包含 16 个字符。密码的有效字符是字母、数字、中文和符号。×

11. 如果向某个组分配了权限，则作为该组成员的用户也具有这一权阪 OA 例如，如果Backup Operators 组有此权限，而 his 又是该组成员，则 his 也有此权限。√

12.Windows 文件系统中，只有 Administrator 组和 Sewer Operation 组可以设置和去除共享目录，并且可以设置共享目录的访问权限。×

13. 远程访问共享目录中的目录和文件，必须能够同时满足共享的权限设置和文件目录
自身的权限设置。用户对共享所获得的最终访问权限将取决于共享的权限设置和目录的本地 权限设置中宽松一些的条件。×

14. 对于注册表的访问许可是将访问权限赋予计算机系统的用户组，如 Administrator 、Users 、 Creator/Owner 组等。√

15. 系统日志提供了一个颜色符号来表示问题的严重程疫，其中一个中间有字母 "!" 的黄色圆圈（ 或三角形 ）表示信息性问题，一个中间有字母 "i" 的蓝色圆圈表示一次警 告，而中间有 "stop" 字样（ 或符号叉 ）的红色八角形表示严重问题。×

16. 光盘作为数据备份的媒介优势在于价格便宜、速度快、容量大。×

17.Windows 防火墙能帮助阻止计算机病毒和蠕虫进入用户的计算机，但该防火墙不能检测或清除已经感染计算机的病毒和蠕虫√

18.Web 站点访问者实际登录的是该 Web 服务器的安全系统 ," 匿名 "Web 访问者都是以 IUSR 帐号身份登录的。√

19.UNIX 的开发工作是自由、独立的，完全开放源、码，由很多个人和组织协同开发的。 UNIX 只定义了个操作系统内核。所有的 UNIX 发行版本共享相同的内核源，但是，和内 核一起的辅助材料则随版本不同有很大不同。×

20. 每个 UNIX/Linux 系统中都只有一个特权用户，就是 root 帐号。×

21. 与 Windows 系统不一样的是 UNIXAAinux 操作系统中不存在预置帐号。×

22.UNIX/IAinux 系统中一个用户可以同时属于多个用户组。√

23. 标准的 UNIX/Limk 系统以属主 (Omer) 、属组 (Group) 、其他人 (World) 三个粒度进行控制。特权用户不受这种访问控制的限制。√

24.UNIX/Linux 系统中，设置文件许可位以使得文件的所有者比其他用户拥有更少的权限是不可能的。×

25.UNIX/Linux 系统和 Windows 系统类似，每一个系统用户都有一个主目录。√

26.UNIX/Linux 系统加载文件系统的命令是 mount, 所有用户都能使用这条命令。×

27.UNIXAm1x 系统中查看进程信息的 who 命令用于显示登录到系统的用户情况，与 w命令不同的是 ,who 命令功能更加强大 ,who 命令是 w 命令的一个增强版。×

28.Httpd.conf 是 Web 服务器的主配置文件，由管理员进行配置 ,Sm.cod 是 Web 服务器的资源配置文件 ,Access-cod 是设置访问权限文件。√

29. 一个设置了粘住位的目录中的文件只有在用户拥有目录的写许可，并且用户是文件和目录的所有者的情况下才能被删除。×

30.UNIX/ImIX 系统中的 /etdshadow 文件含有全部系统需要知道的关于每个用户的信息(加密后的密码也可能存于 /etdpasswd 文件中) 。×

31. 数据库系统是一种封闭的系统，其中的数据无法由多个用户共享。×

32. 数据库安全只依靠技术即可保障。×

33. 通过采用各种技术和管理手段，可以获得绝对安全的数据库系统。×

34. 数据库的强身份认证与强制访问控制是同一概念。×

35. 用户对他自己拥有的数据，不需要有指定的授权动作就拥有全权管理和操作的权限。√

36. 数据库视图可以通过 INSERT 或 UPDATE 语句生成。×

37. 数据库加密适宜采用公开密钥密码系统。√

38. 数据库加密的时候，可以将关系运算的比较字段加密。×

39. 数据库管理员拥有数据库的一切权限。√

40. 不需要对数据库应用程序的开发者制定安全策略。×

41. 使用登录 ID 登录 SQL Sewer 后，即获得了访问数据库的权限。×

42.MS SQL Sewer 与 Sybase SQL Semr 的身份认证机制基本相同。√

43.SQL Sewer 不提供字段粒度的访问控制。×

44.MySQL 不提供字段粒度的访问控制。√

45.SQL Sewer 中，权限可以直接授予用户 ID √

46.SQL 注入攻击不会威胁到操作系统的安全。×

47. 事务具有原子性，其中包括的诸多操作要么全做，要么全不做。√

48. 完全备份就是对全部数据库数据进行备份。√

二、单选题

1. 美国国防部发布的可信计算机系统评估标准〈 TCSEC) 定义了个等级。

A. 五　　B. 六龟　　C. 七　　D. 八

2.Windows 系统的用户帐号有两种基本类型，分别是全局帐号和

A. 本地帐号　　B. 域帐号　　C. 来宾帐号D. 局部帐号

3.Windows 系统安装完后，默认情况下系统将产生两个帐号，分别是管理员帐号和二一。

A. 本地帐号 B. 域帐号　　C. 来宾帐号　　D. 局部帐号

4. 计算机网络组织结构中有两种基本结构，分别是域和

A. 用户组　　B. 工作组　　C. 本地组　　D. 全局组

5. 一般常见的 WIMNs 操作系统与 Iinux 系统的管理员密码最大长度分别为一一一和一一一。

A. 12 8　　B.14 10 、　　C.12 10　　D.14 8

6. 符合复杂性要求的 Wihdows XP 帐号密码的最短长度为一一一。

A.4　　B.6　　C.8　　D.10

7. 设置了强制密码历史后，某用户设置密码 kedawu 失败，该用户可能的原密码是一一一。

A.keda　　B.kedaliu　　C.kedawuj　　D.dawu

8. 某公司的工作时间是上午 8 点半至 12 点，下午 1 点至 5 点半，每次系统备份需要一个半小时，下列适合作为系统数据备份的时间是一一一。

A. 上午 8 点　　B. 中午 12 点　　C. 下午 3 点　　D. 凌晨 1 点

9.Window 系统中对所有事件进行审核是不现实的，下面不建议审核的事件是一一一。

A. 用户登录及注销　　B. 用户及用户组管理　C. 用户打开关闭应用程序　D. 系统重新启动和关机

10. 在正常情况下 ,Windows 2000 中建议关闭的服务是一一一。

A.TCP/IP NetBIOS Helper ServiceB. Logical Disk Manager

C.Remote Procedure Call　　D.Security Accounts Manager

11.FTP(文件传输协议 ,File Transfer Protocol, 简称 HP) 服务、 SMTP(简单邮件传 输协议 ,Simple Mail Transfer Protocol, 简称 SMTP) 服务、 HTTP(超文本传输协议 ,Hyper Text Transport Protocol, 简称 HTTP) 、 HTIPS(加密并通过安全端口传输的另一种 HTIm 服务分别对应的端口是

A.25 21 80 554　B.21 25 80 443　　C.21 110 80 554　　D.21 25 443 554

12. 下面不是 UNIX/L 垃 111x 操作系统的密码设置原则的是

A. 密码最好是英文字母、数字、标点符号、控制字符等的结合

B. 不要使用英文单词，容易遭到字典攻击

C. 不要使用自己、家人、宠物的名字

D. 一定要选择字符长度为 8 的字符串作为密码

13.UNIX/Linux 操作系统的文件系统是结构。

A. 星型　　B. 树型　C. 网状　D.环型

14. 下面说法正确的是

A.UNIX 系统中有两种 NFS 服务器，分别是基于内核的 NFS Daemon 和用户空间Daemon, 其中安全性能较强的是基于内核的 NFS Daemon

B.UNIX 系统中有两种 NFS 服务器，分别是基于内核的 Daemon 和用户空间 NFS Dae- mon, 其中安全性能较强的是基于内核的 NFS Daemon资

C.UNIX 系统中现只有一种 NFS 服务器，就是基于内核的 NFS Daemon, 原有的用户 空间 Daemon 已经被淘汰，因为 NFS Daemon 安全性能较好

D.UNIX 系统中现只有一种 lYFS 服务器，就是基于内核的 Daemon, 原有的用户空间 NFS Daemon 已经被淘汰，因为 Daemon 安全性能较好

15. 下面不是 UNIX/Linux 系统中用来进行文件系统备份和恢复的命令是

A.tar　　B.cpio　　C.umask　　D.backup

16.Backup 命令的功能是用于完成 UNIX/Linux 文件的备份，下面说法不正确的是 A.Backup E-C 命令用于进行完整备份

B.Backup-p 命令用于进行增量备份

C.Backup-f 命令备份由 file 指定的文件

D.Backup-d 命令当备份设备为磁带时使用此选项

17.UNIX 工具 (实用程序 ,utilities) 在新建文件的时候，通常使用 可位，而在新建程序的时候，通常使用作为缺省许可位。

A.555 666　　B.666 777　　C.777 888　　D.888 999

18. 保障 UNIX/Linux 系统帐号安全最为关键的措施是

A. 文件 /etc/passwd 和 /etc/group 必须有写保护

B. 删除〈 etc/passwd 、 /etc/gmp

C. 设置足够强度的帐号密码

D. 使用 shadow 密码

19.UNIX/Linux 系统中，下列命令可以将普通帐号变为 mot 帐号的是

A.chmod 命令　　B./bin/passwd 命令 C.chgrp 命令　D./bin/su命令

20. 有编辑 /etdpasswd 文件能力的攻击者可以通过把 UID 变为一一一就可以成为特权用户。

A.-1　B.O　C.1　D.2

21. 下面不是保护数据库安全涉及到的任务是 O 品

A. 确保数据不能被未经过授权的用户执行存取操作

B. 防止未经过授权的人员删除和修改数据

C. 向数据库系统开发商索要源代码，做代码级检查

D. 监视对数据的访问和更改等使用情况

22. 下面不是数据库的基本安全机制的是

A. 用户认证　　B. 用户授权

C. 审计功能　　D. 电磁屏蔽

23. 关于用户角色，下面说法正确的是

A.SQL Sewer 中，数据访问权限只能赋予角色，而不能直接赋予用户

B. 角色与身份认证无关

C. 角色与访问控制无关

D. 角色与用户之间是一对一的映射关系

24. 下面原则是 DBMS 对于用户的访问存取控制的基本原则的是

A. 隔离原则　　B. 多层控制原则

C. 唯一性原则　　J　　D. 自主原则

25. 下面对于数据库视图的描述正确的是

A. 数据库视图也是物理存储的表

B. 可通过视图访问的数据不作为独特的对象存储，数据库内实际存储的是 SELECT语句

C. 数据库视图也可以使用 UPDATE 或 DELETE 语句生成

D. 对数据库视图只能查询数据，不能修改数据

26. 有关数据库加密，下面说法不正确的是一一一

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

27. 下面不是 Oracle 数据库提供的审计形式的是

A. 备份审计　　B. 语句审计

C. 特权审计　　D. 模式对象设计

28. 下面不是 SQL Sewer 支持的身份认证方式的是一一。

A.Windows NT 集成认证　　B.SQL Sewer 认证

C.SQL Sewer 混合认证　　D. 生物认证

29. 下面一一一不包含在 MySQL 数据库系统中。\

A. 数据库管理系统，即 DBMS　B. 密钥管理系统

C. 关系型数据库管理系统，即 RDBMS　　D. 开放源码数据库

30. 下面不是事务的特性的是

A. 完整性　　B. 原子性

C. 一致性　　D. 隔离性

31. 下面不是 Oracle 数据库支持的备份形式的是 4O

A. 冷备份　　B. 温备份

C. 热备份　　D. 逻辑备份

三、多选题

1. 操作系统的基本功能有

A. 处理器管理　B. 存储管理　C. 文件管理　D. 设备管理

2. 通用操作系统必需的安全性功能有

A. 用户认证 B. 文件和 I/0 设备的访问控制 C. 内部进程间通信的同步 D. 作业管理

3. 根据 blued-H 、 SchroedeI · M.D 的要求，设计安全操作系统应遵循的原则有

A. 最小特权　　B. 操作系统中保护机制的经济性

C. 开放设计、　　D. 特权分离

4.Windows 系统中的用户组包括

A. 全局组　　B. 本地组

C. 特殊组　　D. 标准组

5.Windows 系统登录流程中使用的系统安全模块有

A. 安全帐号管理 (Semrity Account Manager, 简称 SAM) 模块

B.Windows 系统的注册 (Winhgon) 模块

C. 本地安全认证 (Local Security Authority, 简称 LSA) 模块

D. 安全引用监控器模块

6. 域内置全局组安全控制非常重要，这些组只出现在域控制器中，包括一一 -O

A 电 Domain Admins 组　　B.Domain Users 组

C.Domain Replicators 组　　D.Domain Guests 组

7.Windows 系统中的审计日志包括

A. 系统日志 (SystemLog)　　B.安全日志(SecurityLog)

C. 应用程序日志 (App1icationshg)　　D.用户日志(UserLog)

8, 组成 UNIX 系统结构的层次有

A. 用户层　　B. 驱动层

C. 硬件层　　D. 内核层

9.UNIX/linux 系统中的密码控叫制信息保存在 /etc/passwd 或 /ect/st 时 ow 文件中，信息包含的内容有

A. 最近使用过的密码

B. 用户可以再次改变其密码必须经过的最小周期

C.已密码最近的改变时间

D 哇密码有效的最大天数

10.UNIX/Linux 系统中的 Apcache 服务器的主要安全缺陷表现在攻击者可以一一一。

A. 利用 HTTP 协议进行的拒绝服务攻击

B. 发动缓冲区溢出攻击

C .获得 root 权限

D. 利用 MDAC 组件存在一个漏洞，可以导致攻击者远程执行目标系统的命令

11. 数据库访问控制的粒度可能有一一一

A. 数据库级 B. 表级 C. 记录级（ 行级 ） D. 属性级 E. 字符级

12. 下面标准可用于评估数据库的安全级别的有

A.TCSEC. · B.IFTSEC

C.CC DBMS.PP D.GB17859-1999

E.TDI

13.Oracle 数据库的审计类型有

A. 语句审计 B.系统进程审计 C. 特权审计 D.模式对象审计 E. 外部对象审计

14.SQL Se 凹 er 中的预定义服务器角色有一一一一。

A.sysadmin B.serveradmm C.setupadmin D.securityadmin E.processadmin

15. 可以有效限制 SQL 注入攻击的措施有

A. 限制 DBWIS 中 sysadmiIL 用户的数量

B. 在 Web 应用程序中，不以管理员帐号连接数据库

C. 去掉数据库不需要的函数、存储过程

D. 对于输入的字符串型参数，使用转义

E. 将数据库服务器与互联网物理隔断

16. 事务的特性有

A. 原子性 (Atomicity) B. 一致性 (ConsistemL)

C. 隔离性 (Isolation) D. 可生存性 (Survivability)

E 持续性 (Durability)

17. 数据库故障可能有

A. 磁盘故障 B. 事务内部的故障

C. 系统故障 D. 介质故障

E. 计算机病毒或恶意攻击

四、问答题

1. 简要叙述 Windows 系统的用户登录流程。

2. 什么是本地用户组 ？什么是域用户组 ？它们之间是什么关系 2

3. 保障 IIS 安全的主要方式有哪几种 ？分别简要说明。

4.Linux 系统的安全性与 Windows 系统的安全性相比较是否有优势 ？如果有，为什么会有这种优势 ？

5. 一般 UNIX/Linux 系统的密码文件存放在 /etc/passwd 文件中，文件中的条目格式为 user name:encrypted password:1mr ID:group ID:ID string:hom directory:login shell, 其中各字段分别代表了什么含义 ？

6.Linux 系统提供了哪些查看进程信息的系统调用 ？分别简单说明它们命令的功能。

7. 试解释 SQL 注入攻击的原理，以及对数据库可能产生的不利影响。

8. 对比 Oracle 数据库和 MS SQL Sewer 数据库的身份认证机制的异同。 9. 试解释数据库恢复的两种实现技术，并分别说明它们的用途。

第六章

网络安全

一、判断题

1. 防火墙是设置在内部网络与外部网络（ 如互联网 ）之间，实施访问控制策略的一个或一组系统 √

2. 组成自适应代理网关防火墙的基本要素有两个 ： 自适应代理服务器 (Adaptive Proxysewer) 与动态包过滤器 (Dynamic Packet Filter) 。 √

3. 软件防火墙就是指个人防火墙。 ×

4. 网络地址端口转换 (NMT) 把内部地址映射到外部网络的一个 IE 地址的不同端口上 √

5. 防火墙提供的透明工作模式，是指防火墙工作在数据链路层，类似于一个网桥。因此，不需要用户对网络的拓扑做出任何调整就可以把防火墙接入网络。 √

6. 防火墙安全策略一旦设定，就不能在再做任何改变。 ×

7. 对于防火墙的管理可直接通过 Telmt 进行。 ×

8. 防火墙规则集的内容决定了防火墙的真正功能。 √

9. 防火墙必须要提供 VPN 、 NAT 等功能。 ×

10. 防火墙对用户只能通过用户名和口令进行认证。 ×

11. 即使在企业环境中，个人防火墙作为企业纵深防御的一部分也是十分必要的。 √

12. 只要使用了防火墙，企业的网络安全就有了绝对的保障。 ×

13. 防火墙规则集应该尽可能的简单 ,- 规则集越简单，错误配置的可能性就越小，系统就越安全。 √

14.iptables 可配置具有状态包过滤机制的防火墙。 √

15. 可以将外部可访问的服务器放置在内部保护网络中。 ×

16. 在一个有多个防火墙存在的环境中，每个连接两个防火墙的计算机或网络都是DMZ 。 √

17. 入侵检测技术是用于检测任何损害或企图损害系统的机密性、完整性或可用性等行为的一种网络安全技术。 √

18. 主动响应和被动响应是相互对立的，不能同时采用。 ×

19. 异常入侵检测的前提条件是入侵性活动集作为异常活动集的子集，而理想状况是异常活动集与入侵性活动集相等。 √

20. 针对入侵者采取措施是主动响应中最好的响应措施。 ×

21. 在早期大多数的入侵检测系统中，入侵响应都属于被动响应。 √

22. 性能 " 瓶颈 " 是当前入侵防御系统面临的一个挑战。 √

23. 漏报率，是指系统把正常行为作为入侵攻击而进行报警的概率。 ×

24. 与入侵检测系统不同，入侵防御系统采用在线 Online) 方式运行。 √

25. 蜜罐技术是一种被动响应措施。 ×

26. 企业应考虑综合使用基于网络的入侵检测系统和基于主机的入侵检测系统来保护企业网络。在进行分阶段部署时，首先部署基于网络的入侵检测系统，因为它通常最容易安装和维护，接下来部署基于主机的入侵检测系统来保护至关重要的服务器。 √

27. 入侵检测系统可以弥补企业安全防御系统中的安全缺陷和漏洞。 ×