连云港市远程教育信息安全技术考试答案解读

一判断题

第二章物理内存

1、信息网络的物理安全要从环境和设备两个角度来考虑（对）

2、计算机场地可以选择在公共区域人流量比较大的地方（错）

3、计算机场地可以选择在化工生产车间附件（错）

4、计算机场地在正常情况下温度保持在职 18 至此 28 摄氏度。（对）

5、机房供电线路和动力、照明用电可以用同一线路（错）

6、只要手干净就可以直接触摸或者擦拨电路组件，不必有进一步的措施（错）

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。（对）

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。（对）

9、屏蔽室的拼接、焊接工艺对电磁防护没有影响。（错）

10、由于传输的内容不同，电力结可以与网络线同槽铺设。（错）

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。（对）

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。（对）

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，从而达到减少计算机信息泄露的最终目的。（对）

14、机房内的环境对粉尘含量没有要要求。（错）

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。（对）

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。（对）

17、纸介资料废弃应用碎纸机粉碎或焚毁。（对）

第三章容灾与数据备份

1、灾难恢复和容灾具有不同的含义。（错）

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。（对）

3、对目前大量的数据备份来说，磁带是应用得最广的介质。（对）

4、增量备份是备份从上次进行完全备份后更改的全部数据文件。（错）

5、容灾等级通用的国际标准 SHARE 78 将容灾分成了六级。（错）

6、容灾就是数据备份。（错）

7、数据越重要，容灾等级越高。（对）

8、容灾项目的实施过程是周而复始的。（对）

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（错）

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。（对）

11、廉价磁盘冗余陈列（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结合，使其性能超过一只昂贵的大硬盘。（对）

第四章基础安全技术

1、对称密码体制的特征是：加密密钥和解密密钥完全相同，或者一个密钥很容易从另一个密钥中导出。（对）

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。

（对）

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。（对）

4、对信息的这种防篡改、防删除、防插入的特性为数据完整性保护。（对）

5、PKI 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。（对）

第五章系统安全

1、常见的操作系统包括 DOS、OS/

2、UNLX、XENIX、Linux、Windows、Netware、Ora-cle 等。（错）

2、操作系统在概念上一般分为两部份：内核（Kernel）以及壳（Shell），有些操作系统的内核与壳完全分开（如 Microsoft Windiws、UNIX、Linux 等）；另一些的内核与壳关系紧密（如 UNIX、Linus 等），内核及壳只是操作层次上不同面已。（错）

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。（借）

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（Llcal Accounts）。（对）

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（错）

6、本地用户中的 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。（对）

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。（错）

8、全局组是由本域用户组成的，不能包含任何组，也不能包含其他的用户，全局组能在域中任何一台机器上创建。（错）

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。（对）

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。（错）

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限。例如，如果 Backup Operators 组有此权限，而 Lois 也有此权限。（对）

12、Windows 文件系统中，只有 Administrator 组和 Server 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。（错）

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。（错）

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。（对）

15、系统日志提供了一个颜色符号来表示问题的严重程度，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。（错）

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。（错）

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。（对）

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。（对）

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 只定义了人个操作系统内核。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。（错）

20、每个 UNIX/Linux 系统中都只有一个特权用户，就是 root 帐号。（错）

21、与 Winsows 系统不一样的是 UNIS/Linux 操作系统中不存在预置帐号。（错）

22、UNIX/Linux 系统中一个用户可以同时属于多个用户组（对）

23、标准的 UNIX/Linux 系统以属主（Owner）、（Group）、（World）三个粒度进行控制。特权用户不受这种访问控制的限制。（对）

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

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。（对）

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。（错）

27、UNIX/Linux 系统中查看进程信息的 who 命令用于显示全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。（错）

28、Httpd.conf 是 Web 服务器的主配文件，由管理员进行配置，Srm.conf 是 Web 服务器的资源配置文件，Access.conf 是设置访问权限文件。（对）

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删除。（错）

30、UNIX/Linux 系统中的/etc/passwd 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地/etc/passwd 文件中）。（错）

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。（错）

32、数据库安全只依靠技术即可保障。（错）

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。（错）

34、数据库的强身份认证与强制访问控制是同一概念。（错）

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。（对）

36、数据库视图可以通过 INSERT 或 UPDA TE 语句生成。（错）

37、数据库加密适宜采用公开密钥密码系统。（对）

38、数据库加密的时候，可以将关系运算的比较字段加密。（错）

39、数据库管理员拥有数据库的一切权限。（对）

40、不需要对数据库应用程序的开发者制定安全策略。（错）

41、使用 ID 登录 SQL Server 后，即可获得了访问数据库的权限。（错）

42、MS SQL Server 与 Sybase Server 的身份认证机制基本相同。（对）

43、SQL Server 不提供字段粒度的访问控制。（错）

44、MySQL 不提供字段粒度的访问控制。（对）

45、SQL Server 中，权限可以直接授予用户 ID。（对）

46、SQL 注入攻击不会威胁到操作系统的安全。（错）

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。（对）

48、完全备份就是对全部数据进行备份。（对）

第六章网络安全

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个系统。（对）

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 Proxy server）与动态包过滤器（Dynamic Packet Filter）。（对）

3、软件防火墙就是指个人防火墙。（错）

4、网络地址端口转换（NAPT）把内部地址映射到外部网络的一个 IP 地址的不同端口上。（对）

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朴做出任何调整就可以把防火墙接入网络。（对）

6、防火墙安全策略一旦设定，就不能再做任何改变。（错）

7、对于防火墙的管理可直接通过 Telnet 进行。（错）

8、防火墙规则集的内容决定了防火墙的真正功能。（对）

9、防火墙必须要提供 VPN、NAT 等功能。（错）

10、防火墙对用户只能通过用户和口令进行认证。（错）

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份也是十分必要的。（对）

12、只要使用了防火墙，企业的网络安全就有了绝对保障。（错）

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。（对）

14、iptable 可配置具有状态包过滤机制的防火墙。（对）

15、可以将外部可访问的服务器放置在内部保护网络中。（错）

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。（对）

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（对）

18、主动响应和被动响应是相互对立的，不能同时采用。（错）

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。（对）

20、针对入侵者采取措施是主动响应中最好的响应措施。（错）

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。（对）

22、性能“瓶颈”是当前入侵防御系统面临的一个挑战。（对）

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。（错）

24、与入侵检测系统不同，入侵防御系统采用在线（inline）方式运行。（对）

25、蜜罐技术是种被动响应措施。（错）

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。（对）

27、入侵检测系统可以弥补企业安全防御系统中安全缺陷和漏洞。（错）

28、使用误用检测技术的入侵检测系统很难检测到新的攻击行为和原有攻击行为的变种。（对）

29、在早期用集线路（hub）作为连接设备的网络中使用的基于网络的入侵检测系统，在交换网络中不做任何改变，一样可以用来监听整个网络。（错）

30、可以通过技术手段，一次性弥补所有的安全漏洞。（错）

31、漏洞只可能存在于操作系统中，数据库等其他软件系统还会存在漏洞。（错）

32、防火墙中不可能存在漏洞（错）

33、基于主机的漏洞扫描不需要有主机的管理员权限。（错）

34、半连接扫描也需要完成 TCP 协议的三次握手过程。（错）

35、使用漏洞库匹配的方法进行扫描，可以发现所有的漏洞。（错）

36、所有的漏洞都是可以通过打补丁来弥补的。（错）

37、通过网络扫描，可以判断目标主机的操作系统类型。（对）

38、x-scan 能够进行端口扫描。（对）

39、隔离网闸采用的是物理隔离技术。（对）

40、“安全通道隔离”是一种逻辑隔离。（错）

41、隔离网闸两端的网络之间不存在物理连接。（对）

42、QQ 是与朋友联机聊天的好工具，不必担心病毒。（错）

43、在计算机上安装防病毒软件之后，就不必担心计算机受到病毒攻击。（错）

44、计算机病毒可能在用户打开“txt”文件时被启动。（对）

45、在安全模式下木马程序不能启动。（错）

46、特征代码技术是检测已知计算机病毒的最简单、代价最小的技术。（对）

47、家里的计算机没有联网，所以不会感染病毒。（错）

48、计算机病毒的传播离不开人的参与，遵循一定的准则就可以避免感染病毒。（错）

49、校验和技术只能检测已知的计算机病毒。（错）

50、采用 Rootkit 技术的病毒可以运行在内核模式中。（对）

51、企业内部只需在网关和各服务器上安装防病毒软件，客户端不需要安装。（错）

52、大部分恶习意网站所携带的病毒就是脚本病毒。（对）

53、利用互联网传播已经成为了计算机病毒传播的一个发展趋势。（对）

第七章应用安全

1、基于规则的方法就是在邮件标题和邮件内容中寻找特定的模式，其优点是规则可以共享，因此它的推广性很强。（对）

2、反向查询方法可以让接收邮件的互联网报务商确认邮件发送者是否就是如其所言的真实地址。（对）

3、SenderID 可以判断出电子邮件的确切来源，因此，可以降低垃圾邮件以及域名欺骗等行为发生的可能。（对）

4、DKIM（DomainKeys Identifed Mail）技术以和 DomainKeys 相同的方式用 DNS 发布的公开密钥验证签名，并且利用思科的标题签名技术确保一致性。（对）

5、运行防病毒软件可以帮助防止遭受网页仿冒欺诈。（对）

6、由于网络钓鱼通常利用垃圾邮件进行传播，因此，各种反垃圾邮件的技术也都可以用来反网络钓鱼。（对）

7、网络钓鱼的目标往往是细心选择的一些电子邮件地址。（对）

8、如果采用正确的用户名和口令成功登录网站，则证明这个网站不是仿冒的。（错）

9、在来自可信站点的电子邮件中输入个人或财务信息就是安全的。（错）

10、包含收件人个人信息的邮件是可信的。（错）

11、可以采用内容过滤技术来过滤垃圾邮件。（对）

12、黑名单库的大小和过滤的有效性是内容过滤产品非常重要的

指标。（对）

13、随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模式成为信息安全领域的一个发展趋势。（对）

14、启发式技术通过查找通用的非法内容特征，来尝试检测新形式和已知形式的非法内容。（对）

15、白名单方案规定邮件接收者只接收自己所信赖的邮件发送者所发送过来的邮件。（对）

16、实时黑名单是简单黑名单的进一步发展，可以从根本上解决垃圾邮件问题。（错）

17、贝叶斯过滤技术具有自适应、学习的能力，目前已经得到了广泛的应用。（对）

18、对网页请求参数进行验证，可以防止 SQL 注入攻击。（对）

二单选题

第二章物理安全

1、以下不符合防静电要求的是

B、在机房内直接更衣梳理

2、布置电子信息系统信号线缆的路由走向时，以下做错误的是

A、可以随意弯曲

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

C、各个国家不相同

4、物理安全的管理应做到

D、以上均正确

第三章容灾与数据备份

1、代表了当灾难发生后，数据的恢复程度指标是 A。

A、RPO

2、代表了当灾难发生后，数据的恢复时间的指标是 B。

B、RTO

3、我国《重要信息系统灾难恢复指南》将灾难恢复分成了六级

B、六级

4、下图是 SAN 存储类型的结构图。

B、SAN

5、容灾的目的和实质是 C。

C、保持信息系统的业务持续性

6、容灾项目实施过程的分析阶段，需要进行 D。

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 B。

B、磁带

8、下列叙述不属于完全备份机制特点描述的是 D。

D、需要存储空间小

9、下面不属于容灾内容的是 A。

A、灾难预测

第五章系统安全

1、美国国防部发布的可信计算机系统评估标准（TCSEC）定义了七个等级。

C、七

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。

A、本地帐号

3、Windows 系统安装完成后，默认情况下系统将产生两个帐号，分别是管理员帐号和 C。

C、来宾帐号

4、计算机网络组织结构中有两种基本结构，分别是域和 B。

B、工作组

5、一般常见的 Windows 操作系统与 Linux 系统的管理员密码最大长度分别为 14 和 8。

D、14 8

6、符合复杂性要求的 Window Xp 帐号密码的最短长度为 B。

B、6

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 C。

C、kedawuj

8、某公司工作时间是上午 8 点半至于 12 点，下午是 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 D。

D、凌晨 1 点

9、Windows 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 C。

C、用户打开关闭应用程序

10、在正常情况下，Windows 2000 中建议关闭的服务是 A。

A、TCP/IP NetBIOS Helper Server

11、FTP（文件传输协议，File Transfer Protocol，简称 FTP）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）、HTTPS（加密并通过安全端口传输的另一种 HTTP）服务分别对应的端口是 B。

B、21 25 80 443

12、下面不是 UNIX/Linux 操作系统的密码设置原则的是 D。

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 B 结构。

B、树型

14、下面说法正确的是 A。

A、UNIX 系统中有两种 NFS 服务器，分别是基于内核的 NFS Daemon

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 C。

C、umask

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 D。

D、Backup –d 命令当备份设备为磁带时使用此先项。

17、UNIX 工具（实用程序，utilities）在新建文件的时候，通常使用 666 作为缺省许可位，而在新建程序的时候，通常使用 777 作为缺省许可位。

B、666 777

18、保障 UNIX/Linux 系统帐号安全最为关键的措施是 A。

A、文件/etc/passwd 和/etx/group 必须有写保护

19、UNIX/Linux 系统中，下列命令可以将普通帐号变为 root 帐号的是 D。

D、/bin/su 命令

20、有编辑/etc/passwd 文件能力的攻击者可以通过把 UID 变为 B 就可以成为特权用户。

B、2

21、下面不是保护数据库安全涉及到的任务是 C。

C、向数据库系统开发商索要源代码，做代码检查。

22、下面不是数据库的基本安全机制的是 D。

D、电磁屏蔽

23、关于用户角色，下面说法正确的是 B。

B、角色与身份认证无关

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。

A、隔离原则

25、下面对于数据库视图的描述正确的是 B。

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

26、有关数据库加密，下面说法不正确的是 C。

C、字符串字段不能加密

27、下面不是 Oracle 数据库提供的审计形式的是 A。

A、备份审计

28、下面不是 SQL Server 支持的身份认证方式的是 D。