连云港专业技术继续教育—网络信息安全总题库及答案

**信息安全技术试题及答案**

**信息安全网络基础：**

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. 由于传输的内容不同，电力线可以与网络线同槽铺设。**×**

8. 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. **√**

9. 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。**√**

10. 机房内的环境对粉尘含量没有要求。**×**

11. 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。**√**

12. 纸介质资料废弃应用碎纸机粉碎或焚毁。**√**

**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，磁带是应用得最广的介质。**√**

4. 增量备份是备份从上次完全备份后更新的全部数据文件。**×**

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。**×**

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. 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

4. 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

5. 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

6. 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

7. 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

8、IBM TSM Fastback 是一款什么软件（ ）

A、防病毒产品； B、入侵防护产品； C、上网行为管理产品； D、数据存储备份产品

9、IBM TSM Fastback产品使用的什么技术（ )

A、磁盘快照； B、文件拷贝； C、ISCSI技术； D、磁盘共享

12、IBM TSM Fastback产品DR（远程容灾）功能备份的是什么（ ）

A、应用系统； B、本地备份的数据； C、文件系统； D、数据库

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

4、数据安全备份有几种策略（ ）

A、全备份； B、增量备份； C、差异备份； D、手工备份

5、建立Disaster Recovery（容灾系统）的前提是什么（ ）多选

A、自然灾害（地震、火灾，水灾...)； B、人为灾害（错误操作、黑客攻击、病毒发作...)

C、技术风险（设备失效、软件错误、电力失效...）

6、IBM TSM Fastback 可以支持数据库系统包括（ ）多选

A、MS SQL； B、Oracle； C、DB2； D、MY SQL

7、IBM TSM Fastback 可以支持的存储介质包括（ ）

A、磁带介质； B、磁盘介质； C、磁带库； D、磁盘柜

**基础安全技术**

系统安全

一、判断题

1. 常见的操作系统包括 DOS 、UNIX 、Linux、Windows 、 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 Microsoft Windows 、 UNIX 、 Linux 等 ); 另一些的内核与壳关系紧 密 ( 如 UNIX 、 Linux 等内核及壳只是操作层次上不同而已。**×**

3. 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。**×**

4.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**√**

5. 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。**×**

6. 数据库安全只依靠技术即可保障。**×**

7. 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。**×**

8. 数据库管理员拥有数据库的一切权限。**√**

9. 完全备份就是对全部数据库数据进行备份。**√**

二、单选题

1.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

2.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

3. 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

4. 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

5 、.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

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.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

3.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

4. 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

**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. 软件防火墙就是指个人防火墙。**×**

3. 防火墙必须要提供 VPN 、 NAT 等功能。**×**

4. 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。**√**

5. 只要使用了防火墙，企业的网络安全就有了绝对的保障。**×**

6. 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。**√**

7. 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 。**√**

8. 所有的漏洞都是可以通过打补丁来弥补的。**×**

9. 通过网络扫描，可以判断目标主机的操作系统类型。**√**

10. 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。**×**

11. 计算机病毒可能在用户打开 "txt" 文件时被启动。**√**

12. 在安全模式下木马程序不能启动。**×**

13. 大部分恶意网站所携带的病毒就是脚本病毒。**√**

14. 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。**√**

二、单选题

1. 防火墙提供的接入模式不包括一一一。

A. 网关模式 B.透明模式 C. 混合模式 D.旁路接入模式

2. 下面关于 DMZ 区的说法错误的是

A. 通常 DMZ 包含允许来自互联网的通信可进入的设备，如 Web 服务器、 FTP 服务器、 SMTP 服务器和 DNS 服务器等

B. 内部网络可以无限制地访问外部网络以及 DMZ

C.DMZ 可以访问内部网络

D. 有两个 DMZ 的防火墙环境的典型策略是主防火墙采用 NAT 方式工作，而内部防 火墙采用透明模式工作以减少内部网络结构的复杂程度

3. 下面病毒出现的时间最晚的类型是

A. 携带特洛伊术马的病毒 B. 以网络钓鱼为目的的病毒

C. 通过网络传播的蠕虫病毒 D.OEice 文档携带的宏病毒

4. 不能防止计算机感染病毒的措施是

A. 定时备份重要文件

B. 经常更新操作系统

C. 除非确切知道附件内容，否则不要打开电子邮件附件

D. 重要部门的计算机尽量专机专用与外界隔绝

5. 企业在选择防病毒产品时不应该考虑的指标为

A. 产品能够从一个中央位置进行远程安装、升级 '

B. 产品的误报、漏报率较低

C. 产品提供详细的病毒活动记录

D. 产品能够防止企业机密信息通过邮件被传出

6. 病毒传播的途径有

A. 移动硬盘 B. 内存条

C. 电子邮件 D. 聊天程序

E 网络浏览

7. 可能和计算机病毒有关的现象有

A. 可执行文件大小改变了

B. 在向写保护的 U 盘复制文件时屏幕上出现 U 盘写保护的提示

C. 系统频繁死机

D. 内存中有来历不明的进程

E. 计算机主板损坏

**应用安全**

一、判断题

1. 运行防病毒软件可以帮助防止遭受网页仿冒欺诈。**√**

2. 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。**√**

3. 网络钓鱼的目标往往是细心选择的一些电子邮件地址。**√**

4. 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。**×**

5. 在来自可信站点的电子邮件中输入个人或财务信息是安全的。**×**

6. 可以采用内容过滤技术来过滤垃圾邮件。**√**

7. 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。**√**

8. 随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模块成为信息安全领域的一个发展趋势**√**

9 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才肤内容。**√**

10. 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。**√**

11. 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。**×**

二、单选题

1. 以下不会帮助减少收到的垃圾邮件数量的是一一一。

A. 使用垃圾邮件筛选器帮助阻止垃圾邮件 .

B. 共享电子邮件地址或即时消息地址时应小心谨慎

C. 安装入侵检测软件

D. 收到垃圾邮件后向有关部门举报

三、多选题

1. 下列邮件为垃圾邮件的有

A. 收件人无法拒收的电子邮件

B. 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件 C. 含有病毒、色情、反动等不良信息或有害信息的邮件

D. 隐藏发件人身份、地址、标题等信息的电子邮件

E. 含有虚假的信息源、发件人、路由等信息的电子邮件

2. 垃圾邮件带来的危害有

A. 垃圾邮件占用很多互联网资源

B. 垃圾邮件浪费广大用户的时间和精力

C. 垃圾邮件提高了某些公司做广告的效益

D. 垃圾邮件成为病毒传播的主要途径

E. 垃圾邮件迫使企业使用最新的操作系统

3. 网页防篡改技术包括

A. 网站采用负载平衡技术 B. 防范网站、网页被篡改

C. 访问网页时需要输入用户名和口令 D. 网页被篡改后能够自动恢复

E 采用 HITPS 协议进行网页传输主

4. 网络钓鱼常用的手段有

A. 利用垃圾邮件 B. 利用假冒网上银行、网上证券网站

C. 利用虚假的电子商务 D. 利用计算机病毒

E. 利用社会工程学

5. 内容过滤的目的包括

A. 阻止不良信息对人们的侵害

B. 规范用户的上网行为，提高工作效率

C. 防止敏感数据的泄漏

D. 遏制垃圾邮件的蔓延

E. 减少病毒对网络的侵害

7. 内容过滤技术的应用领域包括

A. 防病毒 B.网页防篡改 C. 防火墙 D.入侵检测 E. 反垃圾邮件

|  |  |
| --- | --- |
| 1282 | 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. |
|  | A 正确 B 错误 |
| 1283 | 计算机场地可以选择在公共区域人流量比较大的地方。 |
|  | A 正确 B 错误 |
| 1284 | 计算机场地可以选择在化工厂生产车间附近。 |
|  | A 正确 B 错误 |
| 1285 | 计算机场地在正常情况下温度保持在18～28摄氏度。 |
|  | A 正确 B 错误 |
| 1286 | 机房供电线路和动力、照明用电可以用同一线路。 |
|  | A 正确 B 错误 |
| 1287 | 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。 |
|  | A 正确 B 错误 |
| 1288 | 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。 |
|  | A 正确 B 错误 |
| 1289 | 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。 |
|  | A 正确 B 错误 |
| 1290 | 屏蔽室的拼接、焊接工艺对电磁防护没有影响。 |
|  | A 正确 B 错误 |
| 1291 | 由于传输的内容不同，电力线可以与网络线同槽铺设。 |
|  | A 正确 B 错误 |
| 1292 | 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。地线做电气连通。 |
|  | A 正确 B 错误 |
| 1293 | 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。 |
|  | A 正确 B 错误 |
| 1294 | 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。 |
|  | A 正确 B 错误 |
| 1295 | 机房内的环境对粉尘含量没有要求。 |
|  | A 正确 B 错误 |
| 1296 | 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。 |
|  | A 正确 B 错误 |
| 1297 | 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。 |
|  | A 正确 B 错误 |
| 1298 | 纸介质资料废弃应用碎纸机粉碎或焚毁。 |
|  | A 正确 B 错误 |
| 1299 | 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 |
| 1300 | 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 |
| 1301 | 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 |
| 1302 | 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 |
| 1303 | 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 |
| 1304 | 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 具有自动和手动两种触发装置 |
| 1305 | 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 |
| 1306 | 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 |
| 1307 | 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 专用强磁工具清除 |
| 1308 | 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 |
| 1309 | 防止设备电磁辐射可以采用的措施有\_\_\_\_。 |
|  | A 屏蔽 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 |
| 1310 | 灾难恢复和容灾具有不同的含义。 |
|  | A 正确 B 错误 |
| 1311 | 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。 |
|  | A 正确 B 错误 |
| 1312 | 对目前大量的数据备份来说，磁带是应用得最广的介质。 |
|  | A 正确 B 错误 |
| 1313 | 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。 |
|  | A 正确 B 错误 |
| 1314 | 容灾等级通用的国际标准SHARE 78将容灾分成了六级。 |
|  | A 正确 B 错误 |
| 1315 | 容灾就是数据备份。 |
|  | A 正确 B 错误 |
| 1316 | 数据越重要，容灾等级越高。 |
|  | A 正确 B 错误 |
| 1317 | 容灾项目的实施过程是周而复始的。 |
|  | A 正确 B 错误 |
| 1318 | 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。 |
|  | A 正确 B 错误 |
| 1319 | 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。 |
|  | A 正确 B 错误 |
| 1320 | 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。 |
|  | A 正确 B 错误 |
| 1321 | 代表了当灾难发生后，数据的恢复程度的指标是\_\_\_\_。 |
|  | A RPO B RTOC NROD SDO |
| 1322 | 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 NROD SDO |
| 1323 | 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 |
| 1324 | 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 |
| 1325 | 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 |
| 1326 | 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\_\_\_\_。 |
|  | A 磁盘 B 磁带 C 光盘D 软盘 |
| 1327 | 下列叙述不属于完全备份机制特点描述的是\_\_\_\_。 |
|  | A 每次备份的数据量较大B 每次备份所需的时间也就较长C 不能进行得太频繁 D 需要存储空间小 |
| 1328 | 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 |
| 1329 | 信息系统的容灾方案通常要考虑的要点有\_\_\_\_。 |
|  | A 灾难的类型 B 恢复时间 C 恢复程度 D 实用技术 E 成本 |
| 1330 | 系统数据备份包括的对象有\_\_\_\_。 |
|  | A 配置文件 B 日志文件 C 用户文档 D 系统设备文件 |
| 1331 | 容灾等级越高，则\_\_\_\_。 |
|  | A 业务恢复时间越短 B 所需人员越多 C 所需要成本越高 D 保护的数据越重要 |
| 1332 | 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。 |
|  | A 正确 B 错误 |
| 1333 | 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。 |
|  | A 正确 B 错误 |
| 1334 | 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。 |
|  | A 正确 B 错误 |
| 1335 | 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。 |
|  | A 正确 B 错误 |
| 1336 | 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。 |
|  | A 正确 B 错误 |
| 1337 | PKI系统的基本组件包括\_\_\_\_。 |
|  | 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 |
| 1338 | 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 |
| 1339 | 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 |
| 1340 | 常见的操作系统包括DOS、0S／2、UNIX、XENIX、Linux、Windows、Netware、Oracle等。 |
|  | A 正确 B 错误 |
| 1341 | 操作系统在概念上一般分为两部分：内核(Kernel)以及壳(Shell)，有些操作系统的内核与壳完全分开(如Microsoft Windows、UNIX、Linux等)；另一些的内核与壳关系紧密(如UNIX、Linux等)，内核及壳只是操作层次上不同而已。 |
|  | A 正确 B 错误 |
| 1342 | 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。 |
|  | A 正确 B 错误 |
| 1343 | Windows系统的用户帐号有两种基本类型：全局帐号(GlobalAccounts)和本地帐号(LocalAccounts)。 |
|  | A 正确 B 错误 |
| 1344 | 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。 |
|  | A 正确 B 错误 |
| 1345 | 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。 |
|  | A 正确 B 错误 |
| 1346 | 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。 |
|  | A 正确 B 错误 |
| 1347 | 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。 |
|  | A 正确 B 错误 |
| 1348 | 在默认情况下，内置DomainAdmins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。 |
|  | A 正确 B 错误 |
| 1349 | 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。 |
|  | A 正确 B 错误 |
| 1350 | 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BackupOperators组有此权限，而Lois又是该组成员，则Lois也有此权限。 |
|  | A 正确 B 错误 |
| 1351 | Windows文件系统中，只有Administrator组和ServerOperation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。 |
|  | A 正确 B 错误 |
| 1352 | 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。 |
|  | A 正确 B 错误 |
| 1353 | 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。 |
|  | A 正确 B 错误 |
| 1354 | 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。 |
|  | A 正确 B 错误 |
| 1355 | 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。 |
|  | A 正确 B 错误 |
| 1356 | 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。 |
|  | A 正确 B 错误 |
| 1357 | 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。 |
|  | A 正确 B 错误 |
| 1358 | 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只定义了一个操作系统内核。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。 |
|  | A 正确 B 错误 |
| 1359 | 每个UNIX／Linux系统中都只有一个特权用户，就是root帐号。 |
|  | A 正确 B 错误 |
| 1360 | 与Windows系统不一样的是UNIX／Linux操作系统中不存在预置帐号。 |
|  | A 正确 B 错误 |
| 1361 | UNIX／Linux系统中一个用户可以同时属于多个用户组。 |
|  | A 正确 B 错误 |
| 1362 | 标准的UNIX／Linux系统以属主(Owner)、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。 |
|  | A 正确 B 错误 |
| 1363 | 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。 |
|  | A 正确 B 错误 |
| 1364 | UNIX／Linux系统和Windows系统类似，每一个系统用户都有一个主目录。 |
|  | A 正确 B 错误 |
| 1365 | 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。 |
|  | A 正确 B 错误 |
| 1366 | UNIX／Linux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。 |
|  | A 正确 B 错误 |
| 1367 | Httpd.conf是Web服务器的主配置文件，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。 |
|  | A 正确 B 错误 |
| 1368 | 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。 |
|  | A 正确 B 错误 |
| 1369 | UNIX／Linux系统中的／etc／shadow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／etc／passwd文件中)。 |
|  | A 正确 B 错误 |
| 1370 | 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。 |
|  | A 正确 B 错误 |
| 1371 | 数据库安全只依靠技术即可保障。 |
|  | A 正确 B 错误 |
| 1372 | 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。 |
|  | A 正确 B 错误 |
| 1373 | 数据库的强身份认证与强制访问控制是同一概念。 |
|  | A 正确 B 错误 |
| 1374 | 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。 |
|  | A 正确 B 错误 |
| 1375 | 数据库视图可以通过INSERT或UPDATE语句生成。 |
|  | A 正确 B 错误 |
| 1376 | 数据库加密适宜采用公开密钥密码系统。 |
|  | A 正确 B 错误 |
| 1377 | 数据库加密的时候，可以将关系运算的比较字段加密。 |
|  | A 正确 B 错误 |
| 1378 | 数据库管理员拥有数据库的一切权限。 |
|  | A 正确 B 错误 |
| 1379 | 不需要对数据库应用程序的开发者制定安全策略。 |
|  | A 正确 B 错误 |
| 1380 | 使用登录ID登录SQL Server后，即获得了访问数据库的权限。 |
|  | A 正确 B 错误 |
| 1381 | MS SQL Server与Sybase SQL Server的身份认证机制基本相同。 |
|  | A 正确 B 错误 |
| 1382 | SQL Server不提供字段粒度的访问控制。 |
|  | A 正确 B 错误 |
| 1383 | MySQL不提供字段粒度的访问控制。 |
|  | A 正确 B 错误 |
| 1384 | SQL Server中，权限可以直接授予用户ID。 |
|  | A 正确 B 错误 |
| 1385 | SQL注入攻击不会威胁到操作系统的安全。 |
|  | A 正确 B 错误 |
| 1386 | 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。 |
|  | A 正确 B 错误 |
| 1387 | 完全备份就是对全部数据库数据进行备份。 |
|  | A 正确 B 错误 |
| 1388 | 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 C 七 D 八 |
| 1389 | 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 |
| 1390 | Windows系统安装完后，默认隋况下系统将产生两个帐号，分别是管理员帐号和\_\_\_\_。 |
|  | A 本地帐号B 域帐号 C 来宾帐号 D 局部帐号 |
| 1391 | 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 |
| 1392 | —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\_\_\_\_和\_\_\_\_。 |
|  | A 12 8B 14 10C 12 10 D 14 8 |
| 1393 | 符合复杂性要求的WindowsXP帐号密码的最短长度为\_\_\_\_。 |
|  | A 4 B 6 C 8D 10 |
| 1394 | 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\_\_\_\_。 |
|  | A kedaB kedaliu C kedawuj D dawu |
| 1395 | 某公司的工作时间是上午8点半至12点，下午1点555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\_\_\_\_。 |
|  | A 上午8点B 中午12点C 下午3点 D 凌晨l点 |
| 1396 | 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\_\_\_\_。 |
|  | 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 |
| 1397 | 在正常情况下，Windows 2000中建议关闭的服务是\_\_\_\_。 |
|  | A TCP／IP NetBIOS Helper Service B Logical Disk ManagerC Remote Procedure CallD Security Accounts Manager |
| 1398 | FTP(文件传输协议，File Transfer Protocol，简称FFP)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\_\_\_\_。 |
|  | A 25 21 80 554 B 21 25 80 443 C 21 110 80 554D 21 25 443 554 |
| 1399 | 下面不是UNIX／Linux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 |
| 1400 | 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 |
| 1401 | 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NFSDaemon 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NFSDaemon，其中安全性能较强的是基于内核的NFSDaemonC UNIX系统中现只有一种NFS服务器，就是基于内核的NFSDaemon，原有的用户空间Daemon已经被淘汰，因为NFSDaemon安全性能较好D UNIX系统中现只有一种NFS服务器，就是基于内核的Daemon，原有的用户空间NFSDaemon已经被淘汰，因为Daemon安全性能较好 |
| 1402 | 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 tarB cpio C umask D backup |
| 1403 | 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—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 |
| 1404 | UNIX工具(实用程序，utilities)在新建文件的时候，通常使用\_\_\_\_作为缺省许可位，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 888D 888 999 |
| 1405 | 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／groupC 设置足够强度的帐号密码D 使用shadow密码 |
| 1406 | UNIX／Linux系统中，下列命令可以将普通帐号变为root帐号的是\_\_\_\_。 |
|  | A chmod命令B ／bin／passwd命令C chgrp命令 D ／bin／su命令 |
| 1407 | 有编辑／etc／passwd文件能力的攻击者可以通过把UID变为\_\_\_\_就可以成为特权用户。 |
|  | A -1 B 0 C 1D 2 |
| 1408 | 下面不是保护数据库安全涉及到的任务是\_\_\_\_。 |
|  | 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 |
| 1409 | 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 |
| 1410 | 关于用户角色，下面说法正确的是\_\_\_\_。 |
|  | A SQL Server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 |
| 1411 | 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D 自主原则 |
| 1412 | 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 |
| 1413 | 有关数据库加密，下面说法不正确的是\_\_\_\_。 |
|  | 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 |
| 1414 | 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 |
| 1415 | 下面不是SQL Server支持的身份认证方式的是\_\_\_\_。 |
|  | A Windows NT集成认证B SQL Server认证C SQL Server混合认证 D 生物认证 |
| 1416 | 下面\_\_\_\_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RDBMSD 开放源码数据库 |
| 1417 | 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 |
| 1418 | 下面不是Oracle数据库支持的备份形式的是\_\_\_\_。 |
|  | A 冷备份 B 温备份 C 热备份D 逻辑备份 |
| 1419 | 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 |
| 1420 | 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 |
| 1421 | 根据SahzerJ.H、SchroederM.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 |
| 1422 | 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 |
| 1423 | 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(SecurityAccountManager，简称SAM)模块 B Windows系统的注册(WinLogon)模块 C 本地安全认证(10calSecurityAuthority，简称LSA)模块 D 安全引用监控器模块 |
| 1424 | 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\_\_\_\_。 |
|  | A DomainAdmins组 B DomainUsers组 C DomainReplicators组 D Domain Guests组 |
| 1425 | 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(ApplicationsLog) D 用户日志(UserLog) |
| 1426 | 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 |
| 1427 | UNIX／Linux系统中的密码控制信息保存在／etc／passwd或／ect／shadow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 密码最近的改变时间 D 密码有效的最大天数 |
| 1428 | 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\_\_\_\_。 |
|  | A 利用HTYP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 |
| 1429 | 数据库访问控制的粒度可能有\_\_\_\_。 |
|  | A 数据库级 B 表级 C 记录级(行级) D 属性级(字段级) E 字符级 |
| 1430 | 下面标准可用于评估数据库的安全级别的有\_\_\_\_。 |
|  | A TCSEC B ITSEC C CC DBMS.PP D GB 17859——1999 E TDI |
| 1431 | 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 模式对象设计 E 外部对象审计 |
| 1432 | SQL Server中的预定义服务器角色有\_\_\_\_。 |
|  | A sysadmin B serveradmin C setupadmin D securityadmin E processadmin |
| 1433 | 可以有效限制SQL注入攻击的措施有\_\_\_\_。 |
|  | A 限制DBMS中sysadmin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 |
| 1434 | 事务的特性有\_\_\_\_。 |
|  | A 原子性(Atomicity) B 一致性(Consistency) C 隔离性(1solation) D 可生存性(Survivability) E 持续性(Durability) |
| 1435 | 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 |
| 1436 | 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。 |
|  | A 正确 B 错误 |
| 1437 | 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(DynamicPacketFilter)。 |
|  | A 正确 B 错误 |
| 1438 | 软件防火墙就是指个人防火墙。 |
|  | A 正确 B 错误 |
| 1439 | 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。 |
|  | A 正确 B 错误 |
| 1440 | 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。 |
|  | A 正确 B 错误 |
| 1441 | 防火墙安全策略一旦设定，就不能在再做任何改变。 |
|  | A 正确 B 错误 |
| 1442 | 对于防火墙的管理可直接通过Telnet进行。 |
|  | A 正确 B 错误 |
| 1443 | 防火墙规则集的内容决定了防火墙的真正功能。 |
|  | A 正确 B 错误 |
| 1444 | 防火墙必须要提供VPN、NAT等功能。 |
|  | A 正确 B 错误 |
| 1445 | 防火墙对用户只能通过用户名和口令进行认证。 |
|  | A 正确 B 错误 |
| 1446 | 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。 |
|  | A 正确 B 错误 |
| 1447 | 只要使用了防火墙，企业的网络安全就有了绝对的保障。 |
|  | A 正确 B 错误 |
| 1448 | 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。 |
|  | A 正确 B 错误 |
| 1449 | iptables可配置具有状态包过滤机制的防火墙。 |
|  | A 正确 B 错误 |
| 1450 | 可以将外部可访问的服务器放置在内部保护网络中。 |
|  | A 正确 B 错误 |
| 1451 | 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。 |
|  | A 正确 B 错误 |
| 1452 | 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。 |
|  | A 正确 B 错误 |
| 1453 | 主动响应和被动响应是相互对立的，不能同时采用。 |
|  | A 正确 B 错误 |
| 1454 | 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。 |
|  | A 正确 B 错误 |
| 1455 | 针对入侵者采取措施是主动响应中最好的响应措施。 |
|  | A 正确 B 错误 |
| 1456 | 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。 |
|  | A 正确 B 错误 |
| 1457 | 性能“瓶颈”是当前入侵防御系统面临的一个挑战。 |
|  | A 正确 B 错误 |
| 1458 | 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。 |
|  | A 正确 B 错误 |
| 1459 | 与入侵检测系统不同，入侵防御系统采用在线(inline)方式运行。 |
|  | A 正确 B 错误 |
| 1460 | 蜜罐技术是一种被动响应措施。 |
|  | A 正确 B 错误 |
| 1461 | 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。 |
|  | A 正确 B 错误 |
| 1462 | 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。 |
|  | A 正确 B 错误 |
| 1463 | 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。 |
|  | A 正确 B 错误 |
| 1464 | 在早期用集线器(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子网。 |
|  | A 正确 B 错误 |
| 1465 | 可以通过技术手段，一次性弥补所有的安全漏洞。 |
|  | A 正确 B 错误 |
| 1466 | 漏洞只可能存在于操作系统中，数据库等其他软件系统不会存在漏洞。 |
|  | A 正确 B 错误 |
| 1467 | 防火墙中不可能存在漏洞。 |
|  | A 正确 B 错误 |
| 1468 | 基于主机的漏洞扫描不需要有主机的管理员权限。 |
|  | A 正确 B 错误 |
| 1469 | 半连接扫描也需要完成TCP协议的三次握手过程。 |
|  | A 正确 B 错误 |
| 1470 | 使用漏洞库匹配的方法进行扫描，可以发现所有的漏洞。 |
|  | A 正确 B 错误 |
| 1471 | 所有的漏洞都是可以通过打补丁来弥补的。 |
|  | A 正确 B 错误 |
| 1472 | 通过网络扫描，可以判断目标主机的操作系统类型。 |
|  | A 正确 B 错误 |
| 1473 | x-scan能够进行端口扫描。 |
|  | A 正确 B 错误 |
| 1474 | 隔离网闸采用的是物理隔离技术。 |
|  | A 正确 B 错误 |
| 1475 | “安全通道隔离”是一种逻辑隔离。 |
|  | A 正确 B 错误 |
| 1476 | 隔离网闸两端的网络之间不存在物理连接。 |
|  | A 正确 B 错误 |
| 1477 | QQ是与朋友联机聊天的好工具，不必担心病毒。 |
|  | A 正确 B 错误 |
| 1478 | 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。 |
|  | A 正确 B 错误 |
| 1479 | 计算机病毒可能在用户打开“txt”文件时被启动。 |
|  | A 正确 B 错误 |
| 1480 | 在安全模式下木马程序不能启动。 |
|  | A 正确 B 错误 |
| 1481 | 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。 |
|  | A 正确 B 错误 |
| 1482 | 家里的计算机没有联网，所以不会感染病毒。 |
|  | A 正确 B 错误 |
| 1483 | 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。 |
|  | A 正确 B 错误 |
| 1484 | 校验和技术只能检测已知的计算机病毒。 |
|  | A 正确 B 错误 |
| 1485 | 采用Rootkit 技术的病毒可以运行在内核模式中。 |
|  | A 正确 B 错误 |
| 1486 | 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。 |
|  | A 正确 B 错误 |
| 1487 | 大部分恶意网站所携带的病毒就是脚本病毒。 |
|  | A 正确 B 错误 |
| 1488 | 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。 |
|  | A 正确 B 错误 |
| 1489 | 防火墙是\_\_\_\_在网络环境中的应用。 |
|  | A 字符串匹配 B 访问控制技术 C 入侵检测技术D 防病毒技术 |
| 1490 | iptables中默认的表名是\_\_\_\_。 |
|  | A filter B firewallC natD mangle |
| 1491 | 包过滤防火墙工作在OSI网络参考模型的\_\_\_\_。 |
|  | A 物理层B 数据链路层 C 网络层 D 应用层 |
| 1492 | 通过添加规则，允许通往192.168.0.2的SSH连接通过防火墙的iptables指令是\_\_\_\_。 |
|  | A iptables -F INPUT -d 192.168.0.2 -p tcp--dport 22 -j ACCEPTB iptables -A INPUT -d 192.168.0.2 -p tcp--dport 23 -j ACCEPT C iptables -A FORWARD -d 192.168.0.2 -p tcp--dport22 -j ACCEPT D iptables -A FORWARD -d 192.168.0.2 -p tcp--dport 23 -j ACCEPT |
| 1493 | 防火墙提供的接入模式不包括\_\_\_\_。 |
|  | A 网关模式B 透明模式C 混合模式 D 旁路接入模式 |
| 1494 | 关于包过滤防火墙说法错误的是\_\_\_\_。 |
|  | A 包过滤防火墙通常根据数据包源地址、目的地址、端口号和协议类型等标志设置访问控制列表实施对数据包的过滤B 包过滤防火墙不检查OSI网络参考模型中网络层以上的数据，因此可以很快地执行 C 包过滤防火墙可以有效防止利用应用程序漏洞进行的攻击 D 由于要求逻辑的一致性、封堵端口的有效性和规则集的正确性，给过滤规则的制定和配置带来了复杂性，一般操作人员难以胜任管理，容易出现错误 |
| 1495 | 关于应用代理网关防火墙说法正确的是\_\_\_\_。 |
|  | A 基于软件的应用代理网关工作在OSI网络参考模型的网络层上，它采用应用协议代理服务的工作方式实施安全策略 B 一种服务需要一种代理模块，扩展服务较难 C 和包过滤防火墙相比，应用代理网关防火墙的处理速度更快D 不支持对用户身份进行高级认证机制。一般只能依据包头信息，因此很容易受到“地址欺骗型”攻击 |
| 1496 | 关于NAT说法错误的是\_\_\_\_。 |
|  | A NAT允许一个机构专用Intranet中的主机透明地连接到公共域中的主机，无需内部主机拥有注册的(已经越采越缺乏的)全局互联网地址B 静态NAT是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址C 动态NAT主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态NAT就会分配给用户一个IP地址，当用户断开时，这个IP地址就会被释放而留待以后使用 D 动态NAT又叫做网络地址端口转换NAPT |
| 1497 | 下面关于防火墙策略说法正确的是\_\_\_\_。 |
|  | A 在创建防火墙策略以前，不需要对企业那些必不可少的应用软件执行风险分析B 防火墙安全策略一旦设定，就不能在再作任何改变 C 防火墙处理人站通信的缺省策略应该是阻止所有的包和连接，除了被指出的允许通过的通信类型和连接 D 防火墙规则集与防火墙平台体系结构无关 |
| 1498 | 下面关于DMZ区的说法错误的是\_\_\_\_。 |
|  | A 通常DMZ包含允许来自互联网的通信可进入的设备，如Web服务器、FTP服务器、SMTP服务器和DNS服务器等B 内部网络可以无限制地访问外部网络以及DMZ C DMZ可以访问内部网络 D 有两个DMZ的防火墙环境的典型策略是主防火墙采用NAT方式工作，而内部防火墙采用透明模式工作以减少内部网络结构的复杂程度 |
| 1499 | 在PDRR模型中，\_\_\_\_是静态防护转化为动态的关键，是动态响应的依据。 |
|  | A 防护 B 检测 C 响应D 恢复 |
| 1500 | 从系统结构上来看，入侵检测系统可以不包括\_\_\_\_。 |
|  | A 数据源B 分析引擎 C 审计 D 响应 |
| 1501 | 通用入侵检测框架(CIDF)模型中，\_\_\_\_的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。 |
|  | A 事件产生器 B 事件分析器C 事件数据库D 响应单元 |
| 1502 | 基于网络的入侵检测系统的信息源是\_\_\_\_。 |
|  | A 系统的审计日志B 系统的行为数据C 应用程序的事务日志文件 D 网络中的数据包 |
| 1503 | 误用入侵检测技术的核心问题是\_\_\_\_的建立以及后期的维护和更新。 |
|  | A 异常模型B 规则集处理引擎 C 网络攻击特征库 D 审计日志 |
| 1504 | \_\_\_\_是在蜜罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个蜜罐，来构成一个黑客诱捕网络体系架构。 |
|  | A 蜜网 B 鸟饵C 鸟巢D 玻璃鱼缸 |
| 1505 | 下面关于响应的说法正确的是\_\_\_\_。 |
|  | A 主动响应和被动响应是相互对立的，不能同时采用B 被动响应是入侵检测系统中的唯一响应方式C 入侵检测系统提供的警报方式只能是显示在屏幕上的警告信息或窗口 D 主动响应的方式可以是自动发送邮件给入侵发起方的系统管理员请求协助以识别问题和处理问题 |
| 1506 | 下面说法错误的是\_\_\_\_。 |
|  | A 由于基于主机的入侵检测系统可以监视一个主机上发生的全部事件，它们能够检测基于网络的入侵检测系统不能检测的攻击B 基于主机的入侵检测可以运行在交换网络中 C 基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描 D 基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击，因为应用程序日志并不像操作系统审计追踪日志那样被很好地保护 |
| 1507 | 使用漏洞库匹配的扫描方法，能发现\_\_\_\_。 |
|  | A 未知的漏洞 B 已知的漏洞 C 自行设计的软件中的漏洞D 所有漏洞 |
| 1508 | 下面\_\_\_\_不可能存在于基于网络的漏洞扫描器中。 |
|  | A 漏洞数据库模块B 扫描引擎模块C 当前活动的扫描知识库模块 D 阻断规则设置模块 |
| 1509 | 网络隔离技术，根据公认的说法，迄今已经发展了\_\_\_\_个阶段。 |
|  | A 六 B 五 C 四D 三 |
| 1510 | 下面关于隔离网闸的说法，正确的是\_\_\_\_。 |
|  | A 能够发现已知的数据库漏洞B 可以通过协议代理的方法，穿透网闸的安全控制 C 任何时刻，网闸两端的网络之间不存在物理连接 D 在OSI的二层以上发挥作用 |
| 1511 | 关于网闸的工作原理，下面说法错误的是\_\_\_\_. |
|  | A 切断网络之间的通用协议连接B 将数据包进行分解或重组为静态数据；对静态数据进行安全审查，包括网络协议检查和代码扫描等 C 网闸工作在OSI模型的二层以上 D 任何时刻，网闸两端的网络之间不存在物理连接 |
| 1512 | 当您收到您认识的人发来的电子邮件并发现其中有意外附件，您应该\_\_\_\_。 |
|  | A 打开附件，然后将它保存到硬盘B 打开附件，但是如果它有病毒，立即关闭它 C 用防病毒软件扫描以后再打开附件 D 直接删除该邮件 |
| 1513 | 下面病毒出现的时间最晚的类型是\_\_\_\_. |
|  | A 携带特洛伊木马的病毒 B 以网络钓鱼为目的的病毒 C 通过网络传播的蠕虫病毒D Office文档携带的宏病毒 |
| 1514 | 某病毒利用RPCDCOM缓冲区溢出漏洞进行传播，病毒运行后，在％System％文件夹下生成自身的拷贝nvchip4.exe，添加注册表项，使得自身能够在系统启动时自动运行。通过以上描述可以判断这种病毒的类型为\_\_\_\_。 |
|  | A 文件型病毒B 宏病毒 C 网络蠕虫病毒 D 特洛伊木马病毒 |
| 1515 | 采用“进程注入”可以\_\_\_\_。 |
|  | A 隐藏进程B 隐藏网络端口 C 以其他程序的名义连接网络 D 以上都正确 |
| 1516 | 下列关于启发式病毒扫描技术的描述中错误的是\_\_\_\_。 |
|  | A 启发式病毒扫描技术是基于人工智能领域的启发式搜索技术B 启发式病毒扫描技术不依赖于特征代码来识别计算机病毒 C 启发式病毒扫描技术不会产生误报，但可能会产生漏报 D 启发式病毒扫描技术能够发现一些应用了已有机制或行为方式的病毒 |
| 1517 | 不能防止计算机感染病毒的措施是\_\_\_\_\_。 |
|  | A 定时备份重要文件 B 经常更新操作系统C 除非确切知道附件内容，否则不要打开电子邮件附件D 重要部门的计算机尽量专机专用与外界隔绝 |
| 1518 | 企业在选择防病毒产品时不应该考虑的指标为\_\_\_\_。 |
|  | A 产品能够从一个中央位置进行远程安装、升级B 产品的误报、漏报率较低C 产品提供详细的病毒活动记录 D 产品能够防止企业机密信息通过邮件被传出 |
| 1519 | 防火墙通常阻止的数据包包括\_\_\_\_。 |
|  | A 来自未授权的源地址且目的地址为防火墙地址的所有入站数据包(除Email传递等特殊用处的端口外) B 源地址是内部网络地址的所有入站数据包 C 所有ICMP类型的入站数据包 D 来自未授权的源地址，包含SNMP的所有入站数据包 E 包含源路由的所有入站和出站数据包 |
| 1520 | 目前市场上主流防火墙提供的功能包括\_\_\_\_。 |
|  | A 数据包状态检测过滤 B 应用代理 C NAT D VPN E 日志分析和流量统计分析 |
| 1521 | 防火墙的局限性包括\_\_\_\_。 |
|  | A 防火墙不能防御绕过了它的攻击 B 防火墙不能消除来自内部的威胁 C 防火墙不能对用户进行强身份认证 D 防火墙不能阻止病毒感染过的程序和文件进出网络 |
| 1522 | 防火墙的性能的评价方面包括\_\_\_\_。 |
|  | A 并发会话数 B 吞吐量 C 延时 D 平均无故障时间 |
| 1523 | 下面关于防火墙的维护和策略制定说法正确的是\_\_\_\_。 |
|  | A 所有防火墙管理功能应该发生在使用了强认证和加密的安全链路上 B Web界面可以通过SSL加密用户名和密码。非Web的图形界面如果既没有内部加密，也没有SSL，可以使用隧道解决方案，如SSH C 对防火墙策略进行验证的最简单的方法是，获得防火墙配置的拷贝，然后把这些拷贝和根据已定义的策略产生的期望配置进行比较 D 对防火墙策略进行验证的另一种方式通过使用软件对防火墙配置进行实际测试 E 渗透分析可以取代传统的审计程序 |
| 1524 | 蜜罐技术的主要优点有\_\_\_\_。 |
|  | A 蜜罐技术属于被动响应，使用者没有成为刑事诉讼或民事诉讼对象的危险 B 收集数据的真实性，蜜罐不提供任何实际的业务服务，所以搜集到的信息很大可能性都是由于黑客攻击造成的，漏报率和误报率都比较低 C 可以收集新的攻击工具和攻击方法，不像目前的大部分防火墙和入侵检测系统只能根据特征匹配方法来检测已知的攻击 D 不需要强大的资金投入，可以用一些低成本的设备 E 可以及时地阻断网络入侵行为 |
| 1525 | 通用入侵检测框架(CIDF)模型的组件包括\_\_\_\_。 |
|  | A 事件产生器 B 活动轮廓 C 事件分析器 D 事件数据库 E 响应单元 |
| 1526 | 主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有\_\_\_\_。 |
|  | A 针对入侵者采取措施 B 修正系统 C 收集更详细的信息 D 入侵追踪 |
| 1527 | 随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器(sniffer)来监听整个子网的办法不再可行。可选择解决的办法有\_\_\_\_。 |
|  | A 不需要修改，交换网络和以前共享媒质模式的网络没有任何区别 B 使用交换机的核心芯片上的一个调试的端口 C 把入侵检测系统放在交换机内部或防火墙等数据流的关键入口、出口处 D 采用分接器(tap) E 使用以透明网桥模式接入的入侵检测系统 |
| 1528 | 入侵防御技术面临的挑战主要包括\_\_\_\_。 |
|  | A 不能对入侵活动和攻击性网络通信进行拦截 B 单点故障 C 性能“瓶颈” D 误报和漏报 |
| 1529 | 网络安全扫描能够\_\_\_\_。 |
|  | A 发现目标主机或网络 B 判断操作系统类型 C 确认开放的端口 D 识别网络的拓扑结构 E 测试系统是否存在安全漏洞 |
| 1530 | 主机型漏洞扫描器可能具备的功能有\_\_\_\_。 |
|  | A 重要资料锁定：利用安全的校验和机制来监控重要的主机资料或程序的完整性 B 弱口令检查：采用结合系统信息、字典和词汇组合等的规则来检查弱口令 C 系统日志和文本文件分析：针对系统日志档案，如UNIX的syslogs及NT的事件日志(EventLog)，以及其他文本文件的内容做分析 D 动态报警：当遇到违反扫描策略或发现已知安全漏洞时，提供及时的告警。告警可以采取多种方式，可以是声音、弹出窗口、电子邮件甚至手机短信等 E 分析报告：产生分析报告，并告诉管理员如何弥补漏洞 |
| 1531 | 下面对于x-scan扫描器的说法，正确的有\_\_\_\_。 |
|  | A 可以进行端口扫描 B 含有攻击模块，可以针对识别到的漏洞自动发起攻击 C 对于一些已知的CGI和RPC漏洞，x-scan给出了相应的漏洞描述以及已有的通过此漏洞进行攻击的工具 D 需要网络中每个主机的管理员权限 E 可以多线程扫描 |
| 1532 | 下面软件产品中，\_\_\_\_是漏洞扫描器。 |
|  | A x-scan B nmap C Internet Scanner D Norton AntiVirusE Snort |
| 1533 | 隔离网闸的三个组成部分是\_\_\_\_。 |
|  | A 漏洞扫描单元B 入侵检测单元 C 内网处理单元 D 外网处理单元 E 专用隔离硬件交换单元 |
| 1534 | 网闸可能应用在\_\_\_\_。 |
|  | A 涉密网与非涉密网之间 B 办公网与业务网之间 C 电子政务的内网与专网之间 D 业务网与互联网之间 E 局域网与互联网之间 |
| 1535 | 下面不是网络端口扫描技术的是\_\_\_\_。 |
|  | A 全连接扫描B 半连接扫描 C 插件扫描 D 特征匹配扫描 E 源码扫描 |
| 1536 | 按照2000年3月公布的《计算机病毒防治管理办法》对计算机病毒的定义，下列属于计算机病毒的有\_\_\_\_。 |
|  | A 某Word文档携带的宏代码，当打开此文档时宏代码会搜索并感染计算机上所有的Word文档 B 某用户收到来自朋友的一封电子邮件，当打开邮件附件时，邮件附件将自身发送给该用户地址簿中前五个邮件地址 C 某员工在公司内部使用的系统中加入一个逻辑炸弹，如果该员工在一年内被解雇则逻辑炸弹就会破坏系统D 黑客入侵了某服务器，并在其上安装了一个后门程序 E 某QQ用户打开了朋友发送来的一个链接后，发现每次有好友上线QQ都会自动发送一个携带该链接的消息 |
| 1537 | 病毒传播的途径有\_\_\_\_。 |
|  | A 移动硬盘 B 内存条 C 电子邮件 D 聊天程序 E 网络浏览 |
| 1538 | 可能和计算机病毒有关的现象有\_\_\_\_。 |
|  | A 可执行文件大小改变了 B 在向写保护的U盘复制文件时屏幕上出现U盘写保护的提示 C 系统频繁死机 D 内存中有来历不明的进程 E 计算机主板损坏 |
| 1539 | 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。 |
|  | A 正确 B 错误 |
| 1540 | 反向查询方法可以让接收邮件的互联网服务商确认邮件发送者是否就是如其所言的真实地址。 |
|  | A 正确 B 错误 |
| 1541 | SenderlD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。 |
|  | A 正确 B 错误 |
| 1542 | DKIM(Domain Keys Identified 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。 |
|  | A 正确 B 错误 |
| 1543 | 运行防病毒软件可以帮助防止遭受网页仿冒欺诈。 |
|  | A 正确 B 错误 |
| 1544 | 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。 |
|  | A 正确 B 错误 |
| 1545 | 网络钓鱼的目标往往是细心选择的一些电子邮件地址。 |
|  | A 正确 B 错误 |
| 1546 | 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。 |
|  | A 正确 B 错误 |
| 1547 | 在来自可信站点的电子邮件中输入个人或财务信息是安全的。 |
|  | A 正确 B 错误 |
| 1548 | 包含收件人个人信息的邮件是可信的。 |
|  | A 正确 B 错误 |
| 1549 | 可以采用内容过滤技术来过滤垃圾邮件。 |
|  | A 正确 B 错误 |
| 1550 | 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。 |
|  | A 正确 B 错误 |
| 1551 | 随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模块成为信息安全领域的一个发展趋势。 |
|  | A 正确 B 错误 |
| 1552 | 启发式技术通过查找通用的非法内容特征，来尝诩蝴IJ新形式和已知形式的非法内容。 |
|  | A 正确 B 错误 |
| 1553 | 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。 |
|  | A 正确 B 错误 |
| 1554 | 实时黑名单是简单黑名单的进—步发展，可以从根本上解决垃圾邮件问题。 |
|  | A 正确 B 错误 |
| 1555 | 贝叶斯过滤技术具有自适应、自学习的能力，目前已经得到了广泛的应用。 |
|  | A 正确 B 错误 |
| 1556 | 对网页请求参数进行验证，可以防止SQL注入攻击。 |
|  | A 正确 B 错误 |
| 1557 | 以下不会帮助减少收到的垃圾邮件数量的是\_\_\_\_。 |
|  | A 使用垃圾邮件筛选器帮助阻止垃圾邮件B 共享电子邮件地址或即时消息地址时应小心谨慎 C 安装入侵检测软件 D 收到垃圾邮件后向有关部门举报 |
| 1558 | 下列不属于垃圾邮件过滤技术的是\_\_\_\_。 |
|  | A 软件模拟技术 B 贝叶斯过滤技术C 关键字过滤技术D 黑名单技术 |
| 1559 | 下列技术不支持密码验证的是\_\_\_\_。 |
|  | A S／MIMEB PGPC AMTP D SMTP |
| 1560 | 下列行为允许的有\_\_\_\_。 |
|  | A 未经授权利用他人的计算机系统发送互联网电子邮件B 将采用在线自动收集、字母或者数字任意组合等手段获得的他人的互联网电子邮件地址用于出售、共享、交换或者向通过上述方式获得的电子邮件地址发送互联网电子邮件C 未经互联网电子邮件接收者明确伺意，向其发送包含商业广告内容的互联网电子邮件 D 爱选包含商业广告内容的互联网电子邮件时，在互联网电子邮件标题信息前部注明“广告”或者“AD'’字样 |
| 1561 | 下列技术不能使网页被篡改后能够自动恢复的是\_\_\_\_。 |
|  | A 限制管理员的权限 B 轮询检测C 事件触发技术D 核心内嵌技术 |
| 1562 | 以下不可以表示电子邮件可能是欺骗性的是\_\_\_\_。 |
|  | A 它要求您点击电子邮件中的链接并输入您的帐户信息B 传达出一种紧迫感 C 通过姓氏和名字称呼您 D 它要求您验证某些个人信息 |
| 1563 | 如果您认为您已经落入网络钓鱼的圈套，则应采取\_\_\_\_措施。 |
|  | A 向电子邮件地址或网站被伪造的公司报告该情形B 更改帐户的密码C 立即检查财务报表 D 以上全部都是 |
| 1564 | 内容过滤技术的含义不包括\_\_\_\_。 |
|  | A 过滤互联网请求从而阻止用户浏览不适当的内容或站点B 过滤流入的内容从而阻止潜在的攻击进入用户的网络系统C 过滤流出的内容从而阻止敏感数据的泄漏 D 过滤用户的输入从而阻止用户传播非法内容 |
| 1565 | 下列内容过滤技术中在我国没有得到广泛应用的是\_\_\_\_。 |
|  | A 内容分级审查 B 关键字过滤技术C 启发式内容过滤技术D 机器学习技术 |
| 1566 | 会让一个用户的“删除”操作去警告其他许多用户的垃圾邮件过滤技术是\_\_\_\_。 |
|  | A 黑名单B 白名单C 实时黑名单 D 分布式适应性黑名单 |
| 1567 | 不需要经常维护的垃圾邮件过滤技术是\_\_\_\_。 |
|  | A 指纹识别技术 B 简单DNS测试 C 黑名单技术D 关键字过滤 |
| 1568 | 下列关于网络钓鱼的描述不正确的是\_\_\_\_。 |
|  | A 网络钓鱼(Phishing)一词，是“Fishing”和“Phone”的综合体 B 网络钓鱼都是通过欺骗性的电子邮件来进行诈骗活动 C 为了消除越来越多的以网络钓鱼和电子曲6件欺骗的形式进行的身份盗窃和欺诈行为，相关行业成立了一个协会——反网络钓鱼工作小组D 网络钓鱼在很多方面和一般垃圾邮件有所不同，理解这些不同点对设计反网络钓鱼技术至关重要 |
| 1569 | 下面技术中不能防止网络钓鱼攻击的是\_\_\_\_。 |
|  | A 在主页的底部设有一个明显链接，以提醒用户注意有关电子邮件诈骗的问题B 利用数字证书(如 USB KEY)进行登录 C 根据互联网内容分级联盟(ICRA)提供的内容分级标准对网站内容进行分级 D 安装杀毒软件和防火墙、及时升级、打补丁、加强员工安全意识 |
| 1570 | 下列邮件为垃圾邮件的有\_\_\_\_。 |
|  | A 收件人无法拒收的电子邮件 B 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件 C 含有病毒、色情、反动等不良信息或有害信息的邮件 D 隐藏发件人身份、地址、标题等信息的电子邮件 E 含有虚假的信息源、发件人、路由等信息的电子邮件 |
| 1571 | 垃圾邮件带来的危害有\_\_\_\_。 |
|  | A 垃圾邮件占用很多互联网资源 B 垃圾邮件浪费广大用户的时间和精力 C 垃圾邮件提高了某些公司做广告的效益 D 垃圾邮件成为病毒传播的主要途径 E 垃圾邮件迫使企业使用最新的操作系统 |
| 1572 | 网页防篡改技术包括\_\_\_\_。 |
|  | A 网站采用负载平衡技术 B 防范网站、网页被篡改 C 访问网页时需要输入用户名和口令 D 网页被篡改后能够自动恢复 E 采用HTTPS协议进行网页传输 |
| 1573 | 网络钓鱼常用的手段有\_\_\_\_。 |
|  | A 利用垃圾邮件 B 利用假冒网上银行、网上证券网站 C 利用虚假的电子商务 D 利用计算机病毒 E 利用社会工程学 |
| 1574 | 内容过滤的目的包括\_\_\_\_。 |
|  | A 阻止不良信息对人们的侵害 B 规范用户的上网行为，提高工作效率 C 防止敏感数据的泄漏 D 遏制垃圾邮件的蔓延 E 减少病毒对网络的侵害 |
| 1575 | 下面技术为基于源的内容过滤技术的是\_\_\_\_。 |
|  | A 内容分级审查 B DNS过滤 C IP包过滤 D URL过滤 E 关键字过滤技术 |
| 1576 | 内容过滤技术的应用领域包括\_\_\_\_。 |
|  | A 防病毒 B 网页防篡改 C 防火墙 D 入侵检测 E 反垃圾邮件 |

1. **单项选择题**
2. Chinese Wall 模型的设计宗旨是：（A）。

A、用户只能访问哪些与已经拥有的信息不冲突的信息   
B、用户可以访问所有信息

C、用户可以访问所有已经选择的信息   
D、用户不可以访问哪些没有选择的信息

1. 安全责任分配的基本原则是：（C）。

A、“三分靠技术，七分靠管理” B、“七分靠技术，三分靠管理”

C、“谁主管，谁负责” D、防火墙技术

1. 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（B）不属于信息运行安全技术的范畴。

A、风险分析 B、审计跟踪技术 C、应急技术 D、防火墙技术

1. 从风险的观点来看，一个具有任务紧急性，核心功能性的计算机应用程序系统的开发和维护项目应该（A）。

A、内部实现 B、外部采购实现 C、合作实现 D、多来源合作实现

1. 从风险分析的观点来看，计算机系统的最主要弱点是（B）。

A、内部计算机处理 B、系统输入输出 C、通讯和网络 D、外部计算机处理

1. 从风险管理的角度，以下哪种方法不可取？（D）

A、接受风险 B、分散风险 C、转移风险 D、拖延风险

1. 当今IT的发展与安全投入，安全意识和安全手段之间形成（B）。

A、安全风险屏障 B、安全风险缺口 C、管理方式的变革 D、管理方式的缺口

1. 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（D）。

A、已买的软件 B、定做的软件 C、硬件 D、数据

1. 当一个应用系统被攻击并受到了破坏后，系统管理员从新安装和配置了此应用系统，在该系统重新上线前管理员不需查看：（C）

A、访问控制列表 B、系统服务配置情况

1. 审计记录 D、用户账户和权限的设置

10、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行（B）。

1. 逻辑隔离 B、物理隔离 C、安装防火墙 D、VLAN 划分

11、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？（D）

A、威胁、脆弱性 B、系统价值、风险

C、信息安全、系统服务安全 D、受侵害的客体、对客体造成侵害的程度业务

12、公司应明确员工的雇佣条件和考察评价的方法与程序，减少因雇佣不当而产生的安全风险。人员考察的内容不包括（B）。

A、身份考验、来自组织和个人的品格鉴定 B、家庭背景情况调查

C、学历和履历的真实性和完整性 D、学术及专业资格

13、计算机信息的实体安全包括环境安全、设备安全、（B）三个方面。

A运行安全 B、媒体安全 C、信息安全 D、人事安全

14、目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（B）

A、公安部 B、国家保密局

C、信息产业部 D、国家密码管理委员会办公室

15、目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（B）

A、GB/T 18336-2001 信息技术安全性评估准则

B、GB 17859-1999 计算机信息系统安全保护等级划分准则

C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构

D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

16、确保信息没有非授权泄密，即确保信息不泄露给非授权的个人、实体或进程，不为其所用，是指（C）。

A、完整性 B、可用性 C、保密性 D、抗抵赖性

17、如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（A）

A、自动软件管理 B、书面化制度 C、书面化方案 D、书面化标准

18、如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？（A）

A、计算风险 B、选择合适的安全措施

C、实现安全措施 D、 接受残余风险

19、软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（A）

A、软件中止和黑客入侵 B、远程监控和远程维护

C、软件中止和远程监控 D、远程维护和黑客入侵

20、 管理审计指（C）

A、保证数据接收方收到的信息与发送方发送的信息完全一致

B、防止因数据被截获而造成的泄密

C、对用户和程序使用资源的情况进行记录和审查

D、保证信息使用者都可

21、为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（A）

A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B、进行离职谈话，禁止员工账号，更改密码

C、让员工签署跨边界协议

D、列出员工在解聘前需要注意的所有责任

22、为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（D）

A、人际关系技能 B、项目管理技能 C、技术技能 D、沟通技能

23、我国的国家秘密分为几级？（A）

A、3 B、4 C、5 D、6

24、系统管理员属于（C）。

A、决策层 B、管理层

C、执行层 D、既可以划为管理层，又可以划为执行层

25、下列哪一个说法是正确的？（C）

A、风险越大，越不需要保护 B、风险越小，越需要保护

C、风险越大，越需要保护 D、越是中等风险，越需要保护

26、下面哪类访问控制模型是基于安全标签实现的？（B）

A、自主访问控制 B、强制访问控制

C、基于规则的访问控制 D、基于身份的访问控制

27、下面哪项能够提供最佳安全认证功能？（B）

A、这个人拥有什么 B、这个人是什么并且知道什么

C、这个人是什么 D、这个人知道什么

28、下面哪一个是国家推荐性标准？（A）

A、GB/T 18020-1999 应用级防火墙安全技术要求

B、SJ/T 30003-93 电子计算机机房施工及验收规范

C、GA243-2000 计算机病毒防治产品评级准则

D、ISO/IEC 15408-1999 信息技术安全性评估准则

29、下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（C）

A、对安全违规的发现和验证是进行惩戒的重要前提

B、惩戒措施的一个重要意义在于它的威慑性

C、处于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训

D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

30、下面哪一项最好地描述了风险分析的目的？（C）

A、识别用于保护资产的责任义务和规章制度

B、识别资产以及保护资产所使用的技术控制措施

C、识别资产、脆落性并计算潜在的风险

D、识别同责任义务有直接关系的威胁

31、下面哪一项最好地描述了组织机构的安全策略？（A）

A、定义了访问控制需求的总体指导方针

B、建议了如何符合标准

C、表明管理意图的高层陈述

D、表明所使用的技术控制措施的高层陈述

32、下面哪一种风险对电子商务系统来说是特殊的？（D）

A、服务中断 B、应用程序系统欺骗

C、未授权的信息泄露 D、确认信息发送错误

33、下面有关我国标准化管理和组织机构的说法错误的是？（C）

A、国家标准化管理委员会是统一管理全国标准化工作的主管机构

B、国家标准化技术委员会承担国家标准的制定和修改工作

C、全国信息安全标准化技术委员负责信息安全技术标准的审查、批准、编号和发布

D、全国信息安全标准化技术委员负责统一协调信息安全国家标准年度技术项目

34、项目管理是信息安全工程师基本理论，以下哪项对项目管理的理解是正确的？（A）

A、项目管理的基本要素是质量，进度和成本

B、项目管理的基本要素是范围，人力和沟通

C、项目管理是从项目的执行开始到项目结束的全过程进行计划、组织

D、项目管理是项目的管理者，在有限的资源约束下，运用系统的观点，方法和理论，对项目涉及的技术工作进行有效地管理

35、信息安全的金三角是（C）。

A、可靠性，保密性和完整性 B、多样性，冗余性和模化性

C、保密性，完整性和可用性 D、多样性，保密性和完整性

36、信息安全风险缺口是指（A）。

A、IT的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

37、信息安全风险应该是以下哪些因素的函数？（A）

A、信息资产的价值、面临的威胁以及自身存在的脆弱性等

B、病毒、黑客、漏洞等

C、保密信息如国家密码、商业秘密等

D、网络、系统、应用的复杂的程度

38、信息安全工程师监理的职责包括？（A）

A、质量控制，进度控制，成本控制，合同管理，信息管理和协调

B、质量控制，进度控制，成本控制，合同管理和协调

C、确定安全要求，认可设计方案，监视安全态势，建立保障证据和协调

D、确定安全要求，认可设计方案，监视安全态势和协调

39、信息安全管理最关注的是？（C）

A、外部恶意攻击 B、病毒对PC的影响

C、内部恶意攻击 D、病毒对网络的影响

40、信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（C）

A、信息的价值 B、信息的时效性

C、信息的存储方式 D、法律法规的规定

41、信息网络安全的第三个时代是（A）

A、主机时代，专网时代，多网合一时代 B、主机时代，PC时代，网络时代

C、PC时代，网络时代，信息时代 D、2001年，2002年，2003年

42、一个公司在制定信息安全体系框架时，下面哪一项是首要考虑和制定的？（A）

A、安全策略 B、安全标准 C、操作规程 D、安全基线

43、以下哪个不属于信息安全的三要素之一？（C）

A、机密性 B、完整性 C、抗抵赖性 D、可用性

44、以下哪一项安全目标在当前计算机系统安全建设中是最重要的？（C）

A、目标应该具体 B、目标应该清晰

C、目标应该是可实现的 D、目标应该进行良好的定义

45、以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（A）

A、制度和措施 B、漏洞分析

C、意外事故处理计划 D、采购计划

46、以下哪一项是对信息系统经常不能满足用户需求的最好解释？（C）

A、没有适当的质量管理工具 B、经常变化的用户需求

C、用户参与需求挖掘不够 D、项目管理能力不强

47、以下哪一种人给公司带来了最大的安全风险？（D）

A、临时工 B、咨询人员 C、以前的员工 D、当前的员工

48、以下哪种安全模型未使用针对主客体的访问控制机制？（C）

A、基于角色模型 B、自主访问控制模型

C、信息流模型 D、强制访问控制模型

49、以下哪种措施既可以起到保护的作用还能起到恢复的作用？（C）

A、对参观者进行登记 B、备份

C、实施业务持续性计划 D、口令

50、以下哪种风险被定义为合理的风险？（B）

A、最小的风险 B、可接受风险

C、残余风险 D、总风险

51、以下人员中，谁负有决定信息分类级别的责任？（B）

A、用户 B、数据所有者 C、审计员 D、安全官

52、有三种基本的鉴别的方式：你知道什么，你有什么,以及（C）。

A、你需要什么 B、你看到什么 C、你是什么 D、你做什么

53、在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（B）

A、自下而上 B、自上而下 C、上下同时开展 D、以上都不正确

54、在风险分析中，下列不属于软件资产的是（D）

A、计算机操作系统 B、网络操作系统

C、应用软件源代码 D、外来恶意代码

55、在国家标准中，属于强制性标准的是：（B）

A、GB/T XXXX-X-200X B、GB XXXX-200X

C、DBXX/T XXX-200X D、QXXX-XXX-200X

56、在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（A）

A、当信息安全事件的负面影响扩展到本组织意外时

B、只要发生了安全事件就应当公告

C、只有公众的什么财产安全受到巨大危害时才公告

D、当信息安全事件平息之后

57、在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？（A）

A、标准（Standard） B、安全策略（Security policy）

C、方针（Guideline） D、流程(Proecdure)

58、在信息安全管理工作中“符合性”的含义不包括哪一项？（C）

A、对法律法规的符合 B、对安全策略和标准的符合

C、对用户预期服务效果的符合 D、通过审计措施来验证符合情况

59、在许多组织机构中，产生总体安全性问题的主要原因是（A）。

A、缺少安全性管理 B、缺少故障管理

C、缺少风险分析 D、缺少技术控制机制

60、职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（D）

A、数据安全管理员 B、数据安全分析员

C、系统审核员 D、系统程序员

61、中国电信的岗位描述中都应明确包含安全职责，并形成正式文件记录在案，对于安全职责的描述应包括（D）。

A、落实安全政策的常规职责 B、执行具体安全程序或活动的特定职责

C、保护具体资产的特定职责 D、以上都对

62、终端安全管理目标：规范支撑系统中终端用户的行为，降低来自支撑系统终端的安全威胁，重点解决以下哪些问题？（A）。

A、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

B、终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

C、终端接入和配置管理；桌面及主机设置管理；终端防病毒管理

D、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理

63、著名的橘皮书指的是（A）。

A、可信计算机系统评估标准(TCSEC) B、信息安全技术评估标准（ITSEC）

C、美国联邦标准（FC） D、通用准则（CC）

64、资产的敏感性通常怎样进行划分？（C）

A、绝密、机密、敏感 B、机密、秘密、敏感和公开

C、绝密、机密、秘密、敏感和公开等五类

D、绝密、高度机密、秘密、敏感和公开等五类

65、重要系统关键操作操作日志保存时间至少保存（C）个月。

A、1 B、2 C、3 D、4

66、安全基线达标管理办法规定：BSS系统口令设置应遵循的内控要求是（C）

A、数字+字母 B、数字+字母+符号

C、数字+字母+字母大小写 D、数字+符号

67、不属于安全策略所涉及的方面是（D）。

A、物理安全策略 B、访问控制策略

C、信息加密策略 D、防火墙策略

68、“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（C）。

A、“普密”、“商密”两个级别 B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别

D、“一密”、“二密”，“三密”、“四密”四个级别

69、对MBOSS系统所有资产每年至少进行（A）次安全漏洞自评估。

A、1 B、2 C、3 D、4

70、下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（A）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

71、中国电信各省级公司争取在1-3年内实现CTG-MBOSS 系统安全基线“达标”（C）级以上。

A、A级 B、B级 C、C级 D、D级

72、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

73、获取支付结算、证劵交易、期货交易等网络金融服务的身份认证信息（B）组以上的可以被《中华人民共和国刑法》认为是非法获取计算机信息系统系统认定的“情节严重”。

A、5 B、10 C、-15 D、20

74、基准达标项满（B）分作为安全基线达标合格的必要条件。

A、50 B、60 C、70 D、80

75、《国家保密法》对违法人员的量刑标准是（A）。

A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑

B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑

C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑

D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

76、$HOME/.netrc文件包含下列哪种命令的自动登录信息？（C）

A、rsh B、ssh C、ftp D、rlogin

77、/etc/ftpuser文件中出现的账户的意义表示（A）。

A、该账户不可登录ftp B、该账户可以登录ftp C、没有关系 D、缺少

78、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

79、Linux系统/etc目录从功能上看相当于Windows的哪个目录？（B）

A、program files B、Windows C、system volume information D、TEMP

80、Linux系统格式化分区用哪个命令？（A）

A、fdisk B、mv C、mount D、df

81、在Unix系统中，当用ls命令列出文件属性时，如果显示-rwxrwxrwx,意思是（A）。

A、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示其他用户的访问权限

B、前三位rwx表示文件同组用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

C、前三位rwx表示文件同域用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

D、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示同域用户的访问权限

82、Linux系统通过（C）命令给其他用户发消息。

A、less B、mesg C、write D、echo to

83、Linux中，向系统中某个特定用户发送信息，用什么命令？（B）

A、wall B、write C、mesg D、net send

84、防止系统对ping请求做出回应，正确的命令是：（C）。

A、echo 0>/proc/sys/net/ipv4/icmp\_ehco\_ignore\_all

B、echo 0>/proc/sys/net/ipv4/tcp\_syncookies

C、echo 1>/proc/sys/net/ipv4/icmp\_echo\_ignore\_all

D、echo 1>/proc/sys/net/ipv4/tcp\_syncookies

85、NT/2K模型符合哪个安全级别？（B）

A、B2 B、C2 C、B1 D、C1

86、Red Flag Linux指定域名服务器位置的文件是（C）。

A、etc/hosts B、etc/networks C、etc/rosolv.conf D、/.profile

87、Solaris操作系统下，下面哪个命令可以修改/n2kuser/.profile文件的属性为所有用户可读、科协、可执行？（D）

A、chmod 744 /n2kuser/.profile B、 chmod 755 /n2kuser/.profile

C、 chmod 766 /n2kuser/.profile D、 chmod 777 /n2kuser/.profile

88、如何配置，使得用户从服务器A访问服务器B而无需输入密码？（D）

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhost文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/etc/hosts.equiv文件

89、Solaris系统使用什么命令查看已有补丁列表？（C）

A、uname –an B、showrev C、oslevel –r D、swlist –l product ‘PH??’

90、Unix系统中存放每个用户信息的文件是（D）。

A、/sys/passwd B、/sys/password C、/etc/password D、/etc/passwd

91、Unix系统中的账号文件是（A）。

A、/etc/passwd B、/etc/shadow C、/etc/group D、/etc/gshadow

92、Unix系统中如何禁止按Control-Alt-Delete关闭计算机？（B）

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

93、Unix中。可以使用下面哪一个代替Telnet，因为它能完成同样的事情并且更安全？（B）

A、S-TELNET B、SSH C、FTP D、RLGON

94、Unix中，默认的共享文件系统在哪个位置？（C）

A、/sbin/ B、/usr/local/ C、/export/ D、/usr/

95、Unix中，哪个目录下运行系统工具，例如sh,cp等？（A）

A、/bin/ B、/lib/ C、/etc/ D、/

96、U盘病毒依赖于哪个文件打到自我运行的目的？（A）

A、autoron.inf B、autoexec.bat C、config.sys D、system.ini

97、Windows nt/2k中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

98、Windows 2000目录服务的基本管理单位是（D）。

A、用户 B、计算机 C、用户组 D、域

99、Windows 2000系统中哪个文件可以查看端口与服务的对应？（D）

A、c:\winnt\system\drivers\etc\services B、c:\winnt\system32\services

C、c:\winnt\system32\config\services D、c:\winnt\system32\drivers\etc\services

100、Windows NT/2000 SAM存放在（D）。

A、WINNT B、WINNT/SYSTEM32

C、WINNT/SYSTEM D、WINNT/SYSTEM32/config

101、 Windows NT/2000中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

102、Windows NT的安全标识（SID）串是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是什么？（C）

A、击键速度 B、用户网络地址 C、处理当前用户模式线程所花费CPU的时间 D、PING的响应时间

103、Windows NT和Windows 2000系统能设置为在几次无效登录后锁定账号，可以防止：（B）。

A、木马 B、暴力破解 C、IP欺骗 D、缓冲区溢出攻击

104、Windows主机推荐使用（A）格式。

A、NTFS B、FAT32 C、FAT D、Linux

105、XP当前的最新补丁是（C）。

A、SP1 B、SP2 C、SP3 D、SP4

106、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

107、当你感觉到你的Win2003运行速度明显减慢，当打开任务管理器后发现CPU使用率达到了100%，你认为你最有可能受到了（D）攻击。

A、缓冲区溢出攻击 B、木马攻击 C、暗门攻击 D、DOS攻击

108、档案权限755，对档案拥有者而言，是什么含义？（A）

A、可读，可执行，可写入 B、可读

C、可读，可执行 D、可写入

109、如何配置，使得用户从服务器A访问服务器B而无需输入密码（D）。

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhosts文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/et/hosts.equiv文件

110、要求关机后不重新启动，shutdown后面参数应该跟（C）。

A、–k B、–r C、-h D、 –c

111、一般来说，通过web运行http服务的子进程时，我们会选择（D）的用户用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

112、以下哪项技术不属于预防病毒技术的范畴？（A）

A、加密可执行程序 B、引导区保护

C、系统监控与读写控制 D、校验文件

113、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？（B）

A、缓冲区溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDos攻击

114、与另一台机器建立IPC$会话连接的命令是（D）。

A、net user [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

B、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$) user:Administrator / passwd:aaa

C、net user \192.168.0.1IPC$ D、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

115、在NT中，如果config.pol已经禁止了对注册表的访问，那么黑客能够绕过这个限制吗？怎样实现？（B）

A、不可以 B、可以通过时间服务来启动注册表编辑器

C、可以通过在本地计算机删除config.pol文件 D、可以通过poledit命令

116、在NT中，怎样使用注册表编辑器来严格限制对注册表的访问？（C）

A、HKEY\_CURRENT\_CONFIG,连接网络注册、登录密码、插入用户ID

B、HKEY\_CURRENT\_MACHINE,浏览用户的轮廓目录，选择NTUser.dat

C、HKEY\_USERS,浏览用户的轮廓目录，选择NTUser.dat

D、HKEY\_USERS,连接网络注册，登录密码，插入用户ID

117、在Solaris 8下，对于/etc/shadow文件中的一行内容如下“root:3vd4NTwk5UnLC:9038::::::”,以下说法正确的是：（E）。

A、这里的3vd4NTwk5UnLC是可逆的加密后的密码

B、这里的9038是指从1970年1月1日到现在的天数

C、这里的9038是指从1980年1月1日到现在的天数

D、这里的9038是指从1980年1月1日到最后一次修改密码的天数

E-以上都不正确

118、在Solaris 8下，对于/etc/shadow文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（A）。

A、是/etc/passwd文件格式 B、是/etc/shadow文件格式

C、既不是/etc/passwd也不是/etc/shadow文件格式

D、这个root用户没有SHELL，不可登录

E、这个用户不可登录，并不是因为没有SHELL

119、在Solaris系统中，终端会话的失败登录尝试记录在下列哪个文件里面?(D)

A、-/etc/default/login B、/etc/nologin

C、/etc/shadow D、var/adm/loginlog

120、在Windows 2000中，以下哪个进程不是基本的系统进程:(D)

A、smss. exe B、csrss. Exe C、winlogon. exe D、-conime.exe

121、在Windows 2000中可以察看开放端口情况的是:(D)。

A、nbtstat B、net C、net show D、netstat

122、在Windows 2003下netstat的哪个参数可以看到打开该端口的PID?(C)（格式到此）

A、a B、n C、o D 、p

123、在使用影子口令文件(shadowedpasswords)的Linux系统中，/etc/passwd文件和/etc/shadow文件的正确权限分别是(C)。

A、rw-r-----,-r-------- B、rw-r--r--,-r--r--r—

C、rw-r--r--,-r-------- Drw-r--rw-,-r-----r--

124、制定数据备份方案时，需要重要考虑的两个因素为适合的备份时间和(B)。

A、备份介质 B、备份的存储位置

C、备份数据量 D、恢复备份的最大允许时间

125、周期性行为，如扫描，会产生哪种处理器负荷?(A)

A、Idle Ioad B、Usage Ioad C、Traffic load D、以上都不对

126、主要由于(D)原因，使Unix易于移植

A、Unix是由机器指令书写的 B、Unix大部分由汇编少部分用C语言编写

C、Unix是用汇编语言编写的 D、Unix小部分由汇编大部分用C语言编写

127、HP-UX系统中，使用(A)命令查看系统版本、硬件配置等信息。

A、uname -a B、ifconfig C、netstat D、ps -ef

128、Linux文件权限一共10位长度，分成四段，第三段表示的内容是(C)。

A、文件类型 B、文件所有者的权限

C、文件所有者所在组的权限 D、其他用户的权限

129、在云计算虚拟化应用中，VXLAN技术处于OS工网络模型中2-3层间，它综合了2层交换的简单性与3层路由的跨域连接性。它是通过在UDP/IP上封装Mac地址而实现这一点的。在简单应用场合，vxLAN可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?(C)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

130、Linux中，什么命令可以控制口令的存活时间了(A)。

A、chage B、passwd C、chmod D、umask

131、Qfabric技术是使用市场上现成的计算和存储网元并利用行业标准的网络接口将它们连接后组建大规模的数据中心，以满足未来云计算的要求。该技术概念是哪个厂家主推的概念?(B)

A、惠普 B、uniper C、Cisco与Vmware D、博科Brocade

132、为了检测Windows系统是否有木马入侵，可以先通过(B)命令来查看当前的活动连接端口。

A、ipconfig B、netstat -rn C、tracert –d D、netstat -an

133、网络营业厅提供相关服务的可用性应不低于（A）。

A、99.99% B、99.9% C、99% D、98.9%

134、IRF(Intelligent Resilient Framework)是在该厂家所有数据中心交换机中实现的私有技术，是应用在网络设备控制平面的多虚拟技术。该技术属于哪个厂家?(A)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

135、Windows NT的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:(D)。

A、击键速度 B、当前用户名

C、用户网络地址 D、处理当前用户模式线程所花费CPU的时间

136、脆弱性扫描，可由系统管理员自行进行检查，原则上应不少于(B)。

A、每周一次 B、每月一次 C、每季度一次 D、每半年一次

137、下面哪一个情景属于身份验证(Authentication)过程?(A)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

138、下面哪一个情景属于授权(Authorization)过程?(B)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

139、下列哪一条与操作系统安全配置的原则不符合?(D)

A、关闭没必要的服务 B、不安装多余的组件

C、安装最新的补丁程序 D、开放更多的服务

140、关于DDoS技术，下列哪一项描述是错误的(D)。

A、一些DDoS攻击是利用系统的漏洞进行攻击的

B、黑客攻击前对目标网络进行扫描是发功DDoS攻击的一项主要攻击信息来源

C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的DDoS攻击入侵

D、DDoS攻击不对系统或网络造成任何影响

141、关于PPP协议下列说法正确的是:(C)。

A、PPP协议是物理层协议

B、PPP协议是在HDLC协议的基础上发展起来的

C、PPP协议支持的物理层可以是同步电路或异步电路

D、PPP主要由两类协议组成:链路控制协议族CLCP)和网络安全方面的验证协议族(PAP和CHAP)

142、接口被绑定在2层的zone，这个接口的接口模式是（C）。

A、NAT mode B、Route mode

C、-Transparent mode D、NAT或Route mode

143、接入控制方面，路由器对于接口的要求包括：（D）。

A、串口接入 B、局域网方式接入 C、Internet方式接入 D、VPN接入

144、局域网络标准对应OSI模型的哪几层？（C）。

A、上三层 B、只对应网络层 C、下三层 D、只对应物理层

145、拒绝服务不包括以下哪一项？（D）。

A、DDoS B、畸形报文攻击 C、Land攻击 D、ARP攻击

146、抗DDoS防护设备提供的基本安全防护功能不包括（A）。

A、对主机系统漏洞的补丁升级 B、检测DDoS攻击

C、DDoS攻击警告 D、DDoS攻击防护

147、路由器产品提供完备的安全架构以及相应的安全模块，在软、硬件层面设置重重过滤，保护路由器业务安全。其中不对的说法是：（C）。--》缺少D选项

A、路由器产品支持URPF，可以过滤大多数虚假IP泛洪攻击

B、路由器产品支持CAR功能，可以有效限制泛洪攻击

C、路由器产品不支持ACL配置功能，不能定制过滤规则

D、

148、路由器对于接入权限控制，包括：（D）。

A、根据用户账号划分使用权限 B、根据用户接口划分使用权限

C、禁止使用匿名账号 D、以上都是

149、路由器启动时默认开启了一些服务，有些服务在当前局点里并没有作用，对于这些服务：（C）。缺少D选项

A、就让他开着，也耗费不了多少资源 B、就让他开着，不会有业务去访问

C、必须关闭，防止可能的安全隐患 D、

150、设置Cisco设备的管理员账号时，应（C）。

A、多人共用一个账号 B、多人共用多个账号

C、一人对应单独账号 D、一人对应多个账号

151、什么命令关闭路由器的finger服务？（C）

A、disable finger B、no finger C、no finger service D、no service finger

152、什么是IDS？（A）

A、入侵检测系统 B、入侵防御系统 C、网络审计系统 D、主机扫描系统

153、实现资源内的细粒度授权，边界权限定义为：（B）。

A、账户 B、角色 C、权限 D、操作

154、使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）

A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

155、使用TCP 79端口的服务是：（D）。

A、telnet B、SSH C、Web D、Finger

156、使用一对一或者多对多方式的NAT转换，当所有外部IP地址均被使用后，后续的内网用户如需上网，NAT转换设备会执行什么样的动作？（C）

A、挤掉前一个用户，强制进行NAT转换 B、直接进行路由转发

C、不做NAT转换 D、将报文转移到其他NAT转换设备进行地址转换

157、私网地址用于配置本地网络、下列地址中属于私网地址的是？（C）

A、100.0.0.0 B、172.15.0.0 C、192.168.0.0 D、244.0.0.0

158、随着Internet发展的势头和防火墙的更新，防火墙的哪些功能将被取代。（D）

A、使用IP加密技术 B、日志分析工作

C、攻击检测和报警 D、对访问行为实施静态、固定的控制

159、随着安全要求的提高、技术的演进，（D）应逐步实现物理隔离，或者通过采用相当于物理隔离的技术（如MPLSVPN）实现隔离。

A、局域网 B、广域网及局域网 C、终端 D、广域网

160、通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出现崩溃，请问这种攻击属于何种攻击？（D）

A、拒绝服务（DoS）攻击 B、扫描窥探攻击

C、系统漏洞攻击 D、畸形报文攻击

161、通信领域一般要求3面隔离，即转发面、控制面、用户面实现物理隔离，或者是逻辑隔离，主要目的是在某一面受到攻击的时候，不能影响其他面。路由器的安全架构在实现上就支持：（D）

A、转发面和控制面物理隔离 B、控制面和用户面逻辑隔离

C、转发面和用户面逻辑隔离 D、以上都支持

162、网管人员常用的各种网络工具包括telnet、ftp、ssh等，分别使用的TCP端口号是（B）。

A、21、22、23 B、23、21、22 C、23、22、21 D、21、23、22

163、网络安全工作的目标包括：（D）。

A、信息机密性 B、信息完整性 C、服务可用性 D、以上都是

164、网络安全在多网合一时代的脆弱性体现在（C）。

A、网络的脆弱性 B、软件的脆弱性 C、管理的脆弱性 D、应用的脆弱性

165、应限制Juniper路由器的SSH（A），以防护通过SSH端口的DoS攻击。

A、并发连接数和1分钟内的尝试连接数 B、并发连接数

C、1分钟内的尝试连接数 D、并发连接数和3分钟内的尝试连接数

166、应用网关防火墙的逻辑位置处在OSI中的哪一层？（C）

A、传输层 B、链路层 C、应用层 D、物理层

167、应用网关防火墙在物理形式上表现为？（B）

A、网关 B、堡垒主机 C、路由 D、交换机

168、用来追踪DDoS流量的命令式：（C）

A、ip source-route B、ip cef C、ip source-track D、ip finger

169、用于保护整个网络IPS系统通常不会部署在什么位置？（D）

A、网络边界 B、网络核心 C、边界防火墙内 D、业务终端上

170、用于实现交换机端口镜像的交换机功能是：（D）

A、PERMIT LIST B、PVLAN C、VTP D、SPAN

171、有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（D）。

A、L2TP是由PPTV协议和Cisco公司的L2F组合而成

B、L2TP可用于基于Internet的远程拨号访问

C、为PPP协议的客户建立拨号连接的VPN连接

D、L2TP只能通过TCP/IP连接

172、有关PPTP（Point-to-Point Tunnel Protocol）说法正确的是（C）。

A、PPTP是Netscape提出的 B、微软从NT3.5以后对PPTP开始支持

C、PPTP可用在微软的路由和远程访问服务上 D、它是传输层上的协议

173、有一些应用，如微软Out look或MSN。它们的外观会在转化为基于Web界面的过程中丢失，此时要用到以下哪项技术：（B）

A、Web代理 B、端口转发 C、文件共享 D、网络扩展

174、预防信息篡改的主要方法不包括以下哪一项？（A）

A、使用VPN技术 B、明文加密 C、数据摘要 D、数字签名

175、域名服务系统（DNS）的功能是（A）。

A、完成域名和IP地址之间的转换 B、完成域名和网卡地址之间的转换

C、完成主机名和IP地址之间的转换 D、完成域名和电子邮件地址之间的转换

176、源IP为100.1.1.1，目的IP为100.1.1.255，这个报文属于什么攻击？（B）（假设该网段掩码为255.255.255.0）

A、LAND攻击 B、SMURF攻击 C、FRAGGLE攻击 D、WINNUKE攻击

177、在AH安全协议隧道模式中，新IP头内哪个字段无需进行数据完整性校验？（A）

A、TTL B、源IP地址 C、目的IP地址 D、源IP地址+目的IP地址

178、在C/S环境中，以下哪个是建立一个完整TCP连接的正确顺序？（D）

A、SYN，SYN/ACK，ACK B、Passive Open,Active Open,ACK,ACK

C、SYN,ACK/SYN,ACK D、Active Open/Passive Open,ACK,ACK

179、在L2TP应用场景中，用户的私有地址分配是由以下哪个组建完成？（B）

A、LAC B、LNS C、VPN Client D、用户自行配置

180、在OSI模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（A）

A、应用层 B、物理层 C、会话层 D、网络层

181、在OSI参考模型中有7个层次，提供了相应的安全服务来加强信息系统的安全性。以下哪一层提供了抗抵赖性？（B）

A、表示层 B、应用层 C、传输层 D、数据链路层

182、在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（B）

A、产生日志的数量 B、攻击减少的速度

C、较低的价格 D、假阳性的减少量

183、在安全审计的风险评估阶段，通常是按什么顺序来进行的？（A）

A、侦查阶段、渗透阶段、控制阶段 B、渗透阶段、侦查阶段、控制阶段

C、控制阶段、侦查阶段、渗透阶段 D、侦查阶段、控制阶段、渗透阶段

184、在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（D）

A、IETF 因特网工程工作小组 B、ISO 国际标准组织

C、IANA 因特网地址指派机构 D、OSI 开放系统互联

185、在传输模式IPSec应用情况中，以下哪个区域数据报文可受到加密安全保护？（D）

A、整个数据报文 B、原IP头 C、新IP头 D、传输层及上层数据报文

186、在点到点链路中，OSPF的Hello包发往以下哪个地址？（B）

A、127.0.0.1 B、224.0.0.5 C、233.0.0.1 D、255.255.255.255

187、在建立堡垒主机时，（A）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

188、在进行Sniffer监听时，系统将本地网络接口卡设置成何种侦听模式？（D）

A、unicast单播模式 B、Broadcast广播模式

C、Multicast组播模式 D、Promiscuous混杂模式

189、在零传输（Zone transfers）中DNS服务使用哪个端口？（A）

A、TCP 53 B、UDP 53 C、UDP 23 D、TCP23

190、在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（C）

A、入网访问控制 B、权限控制 C、网络检测控制 D、防火墙控制

191、在思科设备上，若要查看所有访问表的内容，可以使用的命令式（B）

A、show all access-lists B、show access-lists

C、show ip interface D、show interface

192、在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的这是对（A）。

A、可用性的攻击 B、保密性的攻击 C、完整性的攻击 D、真实性的攻击

193、在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（C）

A、报文服务拒绝 B、假冒 C、数据流分析 D、报文服务更改

194、在以下OSI七层模型中，synflooding攻击发生在哪层？（C）

A、数据链路层 B、网络层 C、传输层 D、应用层

195、在以下哪类场景中，移动用户不需要安装额外功能（L2TP）的VPDN软件？（B）

A、基于用户发起的L2TP VPN B、基于NAS发起的L2TP VPN

C、基于LNS发起的L2TP VPN D、以上都是

196、账户口令管理中4A的认证管理的英文单词为：（B）

A、Account B、Authentication C、Authorization D、Audit

197、只具有（A）和FIN标志集的数据包是公认的恶意行为迹象。

A、SYN B、date C、head D、标志位

198、主从账户在4A系统的对应关系包含：（D）

A、1 -N B、1 -1 C、N -1 D、以上全是

199、主动方式FTP服务器要使用的端口包括（A）。

A、TCP 21 TCP 20 B、TCP21 TCP大于1024的端口

C、TCP 20、TCP 大于1024端口 D、都不对

200、下列（D）因素不是影响IP电话语音质量的技术因素。

A、时延 B、抖动 C、回波 D、GK性能

201、下列安全协议中使用包括过滤技术，适合用于可信的LAN到LAN之间的VPN（内部VPN）的是（D）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

202、下列不是抵御DDoS攻击的方法有（D）。

A、加强骨干网设备监控 B、关闭不必要的服务

C、限制同时打开的Syn半连接数目 D、延长Syn半连接的time out时间

203、下列措施不能增强DNS安全的是（C）。

A、使用最新的BIND工具 B、双反向查找

C、更改DNS的端口号 D、不要让HINFO记录被外界看到

204、下列各种安全协议中使用包过滤技术，适合用于可信的LAN到LAN之间的VPN，即内部网VPN的是（D）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

205、下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适？（D）

A、回应的比例 B、被动的防御 C、主动的防御 D、都不对

206、下列哪项是私有IP地址？（A）

A、10.5.42.5 B、172.76.42.5 C、172.90.42.5 D、241.16.42.5

207、下列哪一项能够提高网络的可用性？（B）

A、数据冗余 B、链路冗余 C、软件冗余 D、电源冗余

208、下列哪一种攻击方式不属于拒绝服务攻击：（A）。

A、LOphtCrack B、Synflood C、Smurf D、Ping of Death

209、下列哪一项是arp协议的基本功能？（A）

A、通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行

B、对局域网内的其他机器广播路由地址

C、过滤信息，将信息传递个数据链路层 D、将信息传递给网络层

210、最早的计算机网络与传统的通信网络最大的区别是什么？（A）

A、计算机网络采用了分组交换技术 B、计算机网络采用了电路交换技术

C、计算机网络的可靠性大大提高 D、计算机网络带宽和速度大大提高

211、以下哪个属于IPS的功能？（A）

A、检测网络攻击 B、网络流量检测 C、实时异常告警 D、以上都是

212、以下说法错误的是（C）。

A、安全是一个可用性与安全性之间的平衡过程 B、安全的三要素中包含完整性

C、可以做到绝对的安全 D、网络安全是信息安全的子集

213、以下属于4A策略管理模块可以管理的为（C）。

A、访问控制策略 B、信息加密策略 C、密码策略 D、防火墙策略

214、最早研究计算机网络的目的是什么？（B）

A、共享硬盘空间、打印机等设备 B、共享计算资源

C、直接的个人通信 D、大量的数据交换

215、防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为（C）。

A、内容过滤 B、地址转换 C、透明代理 D、内容中转

216、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）。

A、防火墙 B、CA中心 C、加密机 D、防病毒产品

217、网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（D）。

A、多重安全网关 B、防火墙 C、Vlan隔离 D、物理隔离

218、下列哪项不是Tacacs+协议的特性。（A）

A、扩展记账 B、加密整个数据包 C、使用TCP D、支持多协议

219、一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（A）

A、最小特权 B、阻塞点 C、失效保护状态 D、防御多样化

220、包过滤防火墙工作的好坏关键在于？（C）

A、防火墙的质量 B、防火墙的功能 C、防火墙的过滤规则设计 D、防火墙的日志

221、对于日常维护工作，连接路由器的协议通常使用：（B）。缺少D选项

A、TELNET，简单，容易配置 B、SSH &SSHv2 加密算法强劲，安全性好

C、TELNET配置16位长的密码，加密传输，十分安全 D、

222、BOTNET是（C）。

A、普通病毒 B、木马程序 C、僵尸网络 D、蠕虫病毒

223、监听的可能性比较低的是（B）数据链路。

A、Ethernet B、电话线 C、有线电视频道 D、无线电

224、当IPS遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（B）。

A、pass B、bypass C、watchdog D、HA

225、网络环境下的security是指（A）。

A、防黑客入侵，防病毒，窃取和敌对势力攻击

B、网络具有可靠性，可防病毒，窃密和敌对势力攻击

C、网络具有可靠性，容灾性，鲁棒性

D、网络的具有防止敌对势力攻击的能力

226、某一案例中，使用者已将无线AP的SSID广播设置为禁止，并修改了默认SSID值，但仍有未经授权的客户端接入该无线网络，这是因为（D）

A、禁止SSID广播仅在点对点的无线网络中有效

B、未经授权客户端使用了默认SSID接入

C、无线AP开启了DHCP服务

D、封装了SSID的数据包仍然会在无线AP与客户端之间传递

227、为了保护DNS的区域传送（zone transfer），应该配置防火墙以阻止（B）。

1.UDP

2.TCP

3.53

4.52

A、1,3 B、2,3 C、1,4 D、2,4

228、以下不属于代理服务技术优点的是（D）。

A、可以实现身份认证 B、内部地址的屏蔽盒转换功能

C、可以实现访问控制 D、可以防范数据驱动侵袭

229、应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（C）。

A、60% B、70% C、80% D、90%

230、TCP协议与UDP协议相比，TCP是（B），UDP是（）。

A、设置起来麻烦；很好设置 B、容易；困难

C、面向连接的；非连接的 D、不可靠的；可靠的

231、交换机转发以太网的数据基于：（B）。

A、交换机端口号 B、MAC地址 C、IP地址 D、数据类别

232、HTTP，FTP，SMTP建立在OSI模型的哪一层？（D）

A、2层-数据链路层 B、3层-网络层 C、4层-传输层 D、7层-应用层

233、网络安全的基本属性是（D）。

A、机密性 B、可用性 C、完整性 D、以上都是

234、网络安全的主要目的是保护一个组织的信息资产的（A）。

A、机密性、完整性、可用性 B、参照性、可用性、机密性、

C、可用性、完整性、参照性 D、完整性、机密性、参照性

235、DBS是采用了数据库技术的计算机系统。DBS是一个集合体，包含数据库、计算机硬件、软件和（C）。

A、系统分析员 B、程序员 C、数据库管理员 D、操作员

236、MySQL -h host -u user -p password命令的含义如下，哪些事正确的？（D）

A、-h后为host为对方主机名或IP地址 B、-u后为数据库用户名

C、-p后为密码 D、以上都对

237、Oracle当连接远程数据库或其它服务时，可以指定网络服务名，Oracle9i支持5中命名方法，请选择错误的选项。（D）

A、本地命名和目录命名 B、Oracle名称（Oracle Names）

C、主机命名和外部命名 D、DNS和内部命名

238、Oracle的数据库监听器（LISTENER）的默认通讯端口是？（A）

A、TCP 1521 B、TCP 1025 C、TCP 1251 D、TCP 1433

239、Oracle默认的用户名密码为（A）。

A、Scote/tiger B、root C、null D、rootroot

240、Oracle数据库中，物理磁盘资源包括哪些（D）。

A、控制文件 B、重做日志文件 C、数据文件 D、以上都是

241、Oracle中启用审计后，查看审计信息的语句是下面哪一个？（C）

A、select \* from SYS.AUDIT$ B、select \* from syslogins

C、select \* from SYS.AUD$ D、AUDIT SESSION

242、SMTP的端口？（A）

A、25 B、23 C、22 D、21

243、SQL Server的登录账户信息保存在哪个数据库中？（C）

A、model B、msdb C、master D、tempdb

244、SQL Sever的默认DBA账号是什么？（B）

A、administrator B、sa C、root D、SYSTEM

245、SQL Sever的默认通讯端口有哪些？（B）

A、TCP 1025 B、TCP 1433 C、UDP 1434 D、TCP 14333 E、TCP 445

246、SQL Sever中可以使用哪个存储过程调用操作系统命令，添加系统账号？（B）

A、xp\_dirtree B、xp\_cmdshell C、xp\_cmdshell D、xpdeletekey

247、SQL Sever中下面哪个存储过程可以执行系统命令？（C）

A、xp\_regread B、xp\_command C、xp\_cmdshell D、sp\_password

248、SQL的全局约束是指基于元祖的检查子句和（C）。

A、非空值约束 B、域约束子句 C、断言 D、外键子句

249、SQL数据库使用以下哪种组件来保存真实的数据？（C）

A、Schemas B、Subschemas C、Tables D、Views

250、SQL语句中，彻底删除一个表的命令是（B）。

A、delete B、drop C、clear D、remore

251、SQL语言可以（B）在宿主语言中使用，也可以独立地交互式使用。

A、-极速 B、-嵌入 C、-混合 D、-并行

252、SSL安全套接字协议所用的端口是（B）。

A、80 B、443 C、1433 D、3389

253、不属于数据库加密方式的是（D）。

A、库外加密 B、库内加密 C、硬件/软件加密 D、专用加密中间件

254、测试数据库一个月程序主要应对的风险是（B）。

A、非授权用户执行“ROLLBACK”命令 B、非授权用户执行“COMMIT”命令

C、非授权用户执行“ROLLRORWARD”命令 D、非授权用户修改数据库中的行

**255、查看Oracle 8i及更高版本数据库的版本信息的命令是（C）。----缺少CD选项**

**A、cd $Oracle\_HOME/orainst B、C-cd $Oracle\_HIME/orainst C、 D、**

256、从安全的角度来看，运行哪一项起到第一道防线的作用？（C）

A、远端服务器 B、WEB服务器 C、防火墙 D、使用安全shell程序

257、从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（B）。

A、每个分割区G有g=|G|记录，其中g=0或g>=n，且g为偶数，

B、记录必须成对地加入G或从G中删除

C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从m各分割区G1，G2，… …Gm中每一个分割区而来的，则统计信息g（G1VG2V… …VGm）是允许发布

D、记录必须不对地加入G或从G中删除

258、单个用户使用的数据库视图的描述为（A）。

A、外模式 B、概念模式 C、内模式 D、存储模式

259、对于IIS日志记录，推荐使用什么文件格式？（D）

A、Microsoft IIS日志文件格式 B、NCSA公用日志文件格式

C、ODBC日志记录格式 D、W3C扩展日志文件格式

**260、对于IIS日志文件的存放目录，下列哪项设置是最好的？（D）----缺少D选型**

**A、%WinDir%\System32\LogFiles B、C:\Inetpub\wwwroot\LogFiles**

**C、C:\LogFiles..)-F:\LogFiles D、**

261、对于IIS日志文件的访问权限，下列哪些设置是正确的？（D）

A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）

B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）

C、SYSTEM（完全控制）Administrator（完全控制）Inernet来宾账户（读取和运行） D、SYSTEM（完全控制）Administrator（完全控制）

262、对于数据库的描述一下哪项说法是正确的？（A）

A、数据和一系列规则的集合 B、一种存储数据的软件

C、一种存储数据的硬件 D、是存放人量数据的软件

263、攻击者可能利用不必要的extproc外部程序调用功能获取对系统的控制权，威胁系统安全。关闭Extproc功能需要修改TNSNAMES.ORA和LISTENER.ORA文件删除一下条目，其中有一个错误的请选择出来（A）。

A、sys\_ertproc B、icache\_extproc

C、PLSExtproc D、extproc

264、关系数据库中，实现实体之间的联系是通过表与表之间的（D）。

A、公共索引 B、公共存储

C、公共元组 D、公共属性

265、关系型数据库技术的特征由一下哪些元素确定的？（A）

A、行和列 B、节点和分支

C、Blocks和Arrows D、父类和子类

266、关于WEB应用软件系统安全，说法正确的是（D）？

A、Web应用软件的安全性仅仅与WEB应用软件本身的开发有关

B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C、黑客的攻击主要是利用黑客本身发现的新漏洞

D、以任何违反安全规定的方式使用系统都属于入侵

267、目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（D）？

A、数据库系统庞大会提供管理成本 B、数据库系统庞大会降低管理效率

C、数据的集中会降低风险的可控性 D、数据的集中会造成风险的集中

268、哪一个是PKI体系中用以对证书进行访问的协议（B）？

A、SSL B、LDAP C、CA D、IKE

269、如果一个SQL Server数据库维护人员，需要具有建立测试性的数据库的权限，那么应该指派给他哪个权限（A）？

A、Database Creators B、System Administrators

C、Server Administrators D、Security Adiministrators

270、如果以Apache 为WWW服务器，（C）是最重要的配置文件。

A、access.conf B、srm.cong C、httpd.conf D、mime.types

271、若有多个Oracle数据需要进行集中管理，那么对sysdba的管理最好选择哪种认证方式（B）？

A、系统认证 B、password文件认证方式 C、域认证方式 D、以上三种都可

272、数据库管理系统DBMS主要由哪两种部分组成？（A）

A、文件管理器和查询处理器 B、事务处理器和存储管理器

C、存储管理器和查询处理器 D、文件管理器和存储管理器

273、数据库系统与文件系统的最主要区别是（B）。

A、数据库系统复杂，而文件系统简单

B、文件系统不能解决数据冗余和数据独立性问题，而数据库系统可以解决

C、文件系统只能管理程序文件，而数据库系统能够管理各宗类型的文件

D、文件系统管理的数据量较少，而数据库系统可以管理庞大的数据量

274、为了防止电子邮件中的恶意代码，应该由（A）方式阅读电子邮件。

A、纯文本 B、网页 C、程序 D、会话

275、为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机（D）？

A、SMTP身份认证 B、逆向名字解析 C、黑名单过滤 D、内容过滤

276、为什么要对数据库进行“非规范化”处理（B）？

A、确保数据完整性 B、增加处理效率 C、防止数据重复 D、节省存储空间

277、下列不属于WEB安全性测试的范畴的是（A）？

A、数据库内容安全性 B、客户端内容安全性

C、服务器端内容安全性 D、日志功能

278、下列操作中，哪个不是SQL Server服务管理器功能（A）？

A、执行SQL查询命令 B、停止SQL Server 服务

C、暂停SQL Server服务 D、启动SQL Server服务

279、下列关于IIS的安全配置，哪些是不正确的（C）？

A、将网站内容移动到非系统驱动程序 B、重命名IUSR账户

C、禁用所有WEB服务扩展 D、创建应用程序池

280、下列哪些不是广泛使用http服务器？（D）

A、W3C B、Apache C、IIS D、IE

281、下列哪些属于WEB脚本程序编写不当造成的（C）？

A、IIS5.0 Webdav Ntdll.dll远程缓冲区一处漏洞

B、apache可以通过../../../../../../../etc/passwd方位系统文件

C、登陆页面可以用password=’a’or’a’=’a’绕过

D、数据库中的口令信息明文存放

282、下列哪种方法不能有效的防范SQL进入攻击（C）？

A、对来自客户端的输入进行完备的输入检查

B、把SQL语句替换为存储过程、预编译语句或者使用ADO命令对象

C、使用SiteKey技术

D、关掉数据库服务器或者不使用数据库

283、下列哪种工具不是WEB服务器漏洞扫描工具（B）？

A、Nikto B、Web Dumper C、paros Proxy D、Nessus

284、下列哪种攻击不是针对统计数据库的（D）？

A、小查询集合大查询集攻击 B、中值攻击 C、跟踪攻击 D、资源解析攻击

285、下列哪项中是数据库中涉及安全保密的主要问题（A）？

A、访问控制问题 B、数据的准确性问题

C、数据库的完整性问题 D、数据库的安全性问题

286、下列应用服务器中，不遵循J2EE规范的是（C）？

A、MTS B、WebLogic C、Oracle 9iApplication Server D、WebSpere

287、下面关于IIS报错信息含义的描述正确的是（B）？

A、401-找不到文件 B、403-禁止访问 C、404-权限问题 D、500-系统错误

288、下面关于Oracle进程的描述，哪项是错误的（B）？

A、运行在Windows平台上的Oracle能让每个用户组程序化地打开新的进程，这是一个安全隐患

B、在Windows平台，除了Oracle.exe进程外还有其他的独立进程

C、unix平台上有多个独立运行的进程，包括数据写进程、日志写进程、存档进程、系统监控进程、进程监控进程

D、有一个特殊的内存区域被映射为\*nix平台上的所有进程，此区域时系统全局去

289、下面哪一项是与数据库管理员（DBA）职责不相容的（C）？

A、数据管理 B、信息系统管理 C、系统安全 D、信息系统规划

290、下面选型中不属于数据库安全控制的有（D）。

A、信息流控制 B、推论控制 C、访问控制 D、隐通道控制

291、下面选型中不属于数据库安全模型的是（D）。

A、自主型安全模型 B、强制型安全模型 C、基于角色的模型 D、访问控制矩阵

292、一般来说，通过WEB运行http服务的子进程时，我们会选择（D）的用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

293、一下不是数据库的加密技术的是（D）。

A、库外加密 B、库内加密 C、硬件加密 D、固件加密

294、一下对于Oracle文件系统描述错误的是（B）？

A、\*nix下Oracle的可执行文件在$Oracle\_HOME/bin/Oracle,$Oracle\_HOME/bin也应该包含在路径环境变量内

B、Windows下Oracle的可执行文件在%Oracle\_HOME%\bin\Oracle.exe,其他

C、硬件加密 D、固件加密

295、以下几种功能中，哪个是DBMS的控制功能（A）？

A、数据定义 B、数据恢复 C、数据修改 D、数据查询

296、以下哪个安全特征和机制是SQL数据库所特有的（B）？

A、标识和鉴别 B、数据恢复 C、数据修改 D、数据查询

297、以下哪个是数据库管理员（DBA）可以行使的职责（A）？

A、系统容量规划 B、交易管理 C、审计 D、故障承受机制

298、以下哪条命令能利用“SQL注入”漏洞动用XP\_cmdshell存储过程，获得某个子目的清单？（A）

A、http://localhost/script?’:EXEC+master..XP\_cmdshell+’dir’:--

B、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’:--

C、http://localhost/script?0’:EXEC+master..XP\_cmdshell+’ dir’:--

D、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’--

299、以下哪条命令能利用“SQL”漏洞动用XP\_cmdshell存储过程，启动或停止某项服务？（B）

A、http://localhost/script?’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;-

B、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;--

C、http://localhost/script?1’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ; --

D、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ --

300、以下哪项不属于访问控制策略的实施方式？（D）

A、子模式法 B、修改查询法 C、集合法 D、验证法

301、以下哪一项是和电子邮件系统无关的？（）

A、PEM(Privacy enhanced mail) B、PGP(Pretty good privacy)

C、X.500 D、X.400

302、以下哪种方法可以用于对付数据库的统计推论？（C）

A、信息流控制 B、共享资源矩阵 C、查询控制 D、间接存取

303、以下是对层次数据库结构的描述，请选择错误描述的选项。（C）

A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来

B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据

C、它的优点是用户不需要十分熟悉数据库结构

D、层次数据库模型的结构就像是一棵倒转的树

304、以下是对单用户数据库系统的描述，请选择错误描述的选项（C）。

A、单用户数据库系统是一种早期的最简单的数据库系统

B、在单用户系统中，整个数据库系统，包括应用程序、DBMS、数据，都装在一台计算机之间不能共享数据

C、在单用户系统中，由多个用户共用，不同计算机之间能共享数据

D、单用户数据库系统已经不适用于现在的使用，被逐步淘汰了

305、以下是对分布式结构数据库系统的描述，请选择错误描述的选项。（D）

A、分布式结构的数据库系统的数据在逻辑上是一个整体，但物理地分布在计算机网络的不同节点上，每个节点上的主机又带有多个终端用户

B、网络中的每个节点都可以独立的处理数据库中的数据，执行全局应用

C、分布式结构的数据库系统的数据分布存放给数据的处理、管理和维护带来困难

D、分布式结构的数据库系统的数据只在存放在服务器端，其他节点只进行处理和执行

306、以下是对关系数据库结构的描述，请选择错误描述的选项。（D）

A、数据存储的主要载体是表，或相关数据组

B、有一对一、一对多、多对多三种表关系

C、表关联是通过引用完整性定义的，这是通过主码和外码（主键或外键约束条件实现的）

D、缺点是不支持SQL语言

307、以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（A）

A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力

B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行DBMS功能又执行应用程序

C、在网络中把某些节点的计算机专门用于执行DBMS核心功能，这台计算机就成为数据库服务器

D、其他节点上的计算机安装DBMS外围应用开发工具和应用程序，支持用户的应用，称为客户机

308、以下是对面向对象数据库结构的描述，请选择错误描述的选项。（C）

A、它允许用对象的概念来定义与关系数据库交互

B、面向对象数据库中有两个基本的结构：对象和字面量

C、优点是程序员需要掌握与面向对象概念以及关系数据库有关的存储

D、缺点是用户必须理解面向对象概念，目前还没有统一的标准，稳定性还是一个值得关注的焦点

309、以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（D）

A、主从式结构是指一个主机带多个终端的多用户结构

B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上

C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源

D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈

311、在GRUB的配置文件grub.conf中，“timeout=-1”的含义是（C）。

A、不等待用户选择，直接启动默认的系统

B、在10秒钟内，等待用户选择要启动的系统

C、一直等待用户选择要启动的系统

D、无效

312、在Oracle中，quota可以限制用户在某个表空间上最多可使用多少字节，如果要限制data\_ts表500K，以下哪个是正确的命令？（B）

A、quo 500k in data\_ts B、quota 500K on data\_ts

C、quota data\_ts ,imit 500K D、quota data\_ts on 500K

313、在Oracle中，建表约束包括引用完整性约束、check完整性约束，还有以下三项是正确的，请排除一个错误选项。（D）

A、非空完整性约束 B、唯一完整性约束

C、主码完整性约束 D、数据角色性约束

314、在Oracle中，将scott的缺省表空间改为data2\_ts，下列哪个是正确的？（A）

A、ALTER USER scott DEFAULT TABLESPACE data2\_ts

B、ALTER DEFAULT TABLESPACE data2\_ts USER scott

C、ALTER USER scott TABLESPACE DEFAULT data2\_ts D、ALTER scott USER DEFAULT TABLESPACE data2\_ts

315、在Oracle中，将scott的资源文件改为otherprofile，下列哪个是正确的？（C）

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

316、在Oracle中，将当前系统所有角色都授予scott，除Payroll外，下列哪个是正确的？（D）

A、ALTER DEFAULT ROLLE USER　　scott ALL EXCEPT Payroll

B、ALTER USER DEFAULT ROLLE ALL EXCEPT Payroll

C、ALTER DEFAULT ROLLE ALL EXCEPT USER scott

D、ALTER USER scott DEFAULT ROLLE ALL EXCEPT Payroll

317、在Oracle中，用ALTER将scott的口令改为hello，下列哪个是正确的？（A）

A、ALTER USER scott IDENTIFIED BY hello

B、ALTER scott USER IDENTIFIED BY hello

C、ALTER USER scott IDENTIFIED AS hello

D、ALTER USER hello IDENTIFIED BY scott

318、在WEB应用软件的基本结构中，客户端的基础是（A）。

A、HTML文档 B、客户端程序

C、HTML协议 D、浏览器

319、在WEB应用软件的系统测试技术中，下面不属于安全性测试内容的是（C）。

A、客户端的内容安全性 B、服务器的内容安全性

C、数据库的内容安全性 D、Cookie安全性

320、在典型的WEB应用站点的层次结构中，“中间件”是在哪里运行的？（C）

A、浏览器客户端 B、web服务器

C、应用服务器 D、数据库服务器

321、在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（C）

A、对话管理服务 B、事务管理服务

C、资源管理服务 D、控制管理服务

322、主要用于加密机制的协议时（D）。

A、HTTP B、FTP C、TELNETD D、SSL

323、分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？（D）

A、自主性 B、可靠性 C、灵活性 D、数据备份

324、下面对Oracle的密码规则描述，哪个是错误的？（D）

A、Oracle密码必须由英文字母，数值，#，下划线(\_)，美元字符（$）构成，密码的最大长度为30字符，并不能以“$”，“#”，“\_”或任何数字卡头；密码不能包含像“SELECT”，“DELETE”，“CREATE”这类的ORACLE/SQL关键字

B、Oracle的若算法加密机制（）两个相同的用户名和密码在两台不同的ORACLE数据库机器中，将具有相同的哈希值。这些哈希值存储在SYS.USER表中，可以通过像DBA\_USE这类的试图来访问

C、Oracle默认配置下，每个中户如果有10此的失败登录，此账户将会被锁定

D、SYS账户在Oracle数据库中有最高权限，能够做任何事情，包括启动/关闭Oracle数据库，如果SYS被锁定，将不能访问数据库

325、无论是哪一种Web服务器，都会受到HTTP协议本身安全问题的困扰，这样的信息系统安全漏洞属于（C）。

A、设计型漏洞 B、开发型漏洞 C、运行型漏洞 D、以上都不是

326、SSL加密的过程包括以下步骤：（1）通过验证以后，所有数据通过密钥进行加密，使用DEC和RC4加密进行加密；（2）随后客户端随机生成一个对称密钥；（3）信息通过HASH加密，或者一次性加密（MD5SHA）进行完整性确认；（4）客户端和服务器协商建立加密通道的特定算法。正确的顺序的是（D）

A、（4）（3）（1）（2） B、（4）（1）（3）（2） C、（4）（2）（3）（1） D、（4）（2）（3）（1）

327、影响WEB系统安全的因素，不包括？（C）

A、复杂应用系统代码量大、开发人员多、难免出现疏忽

B、系统屡次升级、人员频繁变更，导致代码不一致

C、历史遗留系统、试运行系统等对个WEB系统运行于不同的服务器上

D、开发人员未经安全编码培训

328、Oracle通过修改用户密码策略可提高密码强度，以下哪个密码策略参数中文描述是错误的？（A）

A、PASSWORD\_MAX 登录超过有效次数锁定时间

B、FAILED\_LOGIN\_ATTEMPTS 最大错误登录次数

C、PASSWORD\_GRACE\_TIME 密码失效后锁定时间

D、PASSWORD\_LIFE\_TIME 口令有效时间

329、SQL Server服务有一个启动账号，默认账号是属于administrators组，现在为了安全需要创建一个新的服务启动账号，它需要哪些权限既能兼顾安全又能保证启动数据库成功，请排除一个错误的。（D）

A、数据库本地目录的读写权限 B、启动本地服务的权限

C、读取注册表的权限 D、通过API访问Windows Resource

330、作为一台运行IIS 在Internet发布站点的Windows Web服务器，下面哪项服务不是必需的？（B）

A、IIS Admin B、Net Logon

C、Performance Logs and Alerts D、World Wide Web Publishing

331、数据库中超级账户不能被锁定，其中Oracle的是（），mysql的是（），SQLServer的是（C）。

A、sa，root，sys B、admin，root，sa

C、sys，root，sa D、sys，admin，sa

332，Oracle的安全机制，是由（A）、实体权限和角色权限这三级体系结构组成的。

A、系统权限 B、索引权限 C、操作权限 D、命令控制

333、对SQL数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（B）

A、-- B、- C、-= D、-+

334、在Web页面中增加验证码功能后，下面说法正确的是（A）。

A、可以增加账号破解等自动化软件的攻击难度 B、可以防止文件包含漏洞 C、可以防止缓冲溢出 D、可以防止 浏览

335、以下破解Oracle密码哈希值的步棸，其中哪个描述是错误的？（B）

A、用Sqlplus直接登录到Oracle数据库，使用select username，password form dba\_users命令查看数据库中的用户名和密码，此时看到的密码是哈希值

B、在Cain的Cracker菜单点击导入用户名和哈希值，可直接显示用户密码明文

C、在Cain的Cracker菜单点解导入用户名和哈希值，只能通过字典破解 D、在Cain的Rainbow生成的表会占用大量的硬盘空间和内存，可是破解速度和效率很高

336、在数据库向因特网开放前，哪个步棸是可以忽略的？（B）

A、安全安装和配置操作系统和数据库系统

B、应用系统应该在内网试运行3个月

C、对应用软件如Web也没、ASP脚本等进行安全性检查

D、网络安全策略已经生效

337、如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf文件，查看是否包含如下设置，选出一个正确的（D）。

A、audit=filename B、sys=filename C、event=filename D、log=filename

338、针对一台对外提供Web服务的Windows服务器，下列关于账户权限控制，哪些项是不合理的？（C）

A、限制匿名账户对Web内容的目录写权限

B、从Everyone组中删除“从网络访问此计算机” 用户权限

C、禁用IUSR-MACHE和IWAN\_MACHINE账户

D、本地登录时必须使用Administrators账户

339、网上营业中间件如果启用了SSl，应采用不低于（C）版本的SSL，采用经国家密码管理局认可的密码算法。

A、2.0 B、2.5 C、3.0 D、3.1

340、SQL Server默认的具有DBA权限的账号是什么？（C）

A、root B、admin C、sa D、system

341、（A）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

342、（C）是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

343、《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（B）。

A、GA 163-1997 B、GA 267-2000

C、GA 243-2000 D、GB 17859-1999

344、安装了合格防雷保安器的计算机信息系统，还必须在（C）雷雨季节前对防雷保安器、保护接地装置进行一次年度检查，发现不合格时，应及时修复或更换。

A、第三年 B、第二年 C、每年 D、当年

345、使用IIalon灭火的工作原理是什么？（C）

A、降低温度 B、隔绝氧气和可燃物

C、破坏氧气和可燃物之间的化学反应 D、减少氧气

346、白炽灯、高压汞灯与可燃物、可燃结构之间的距离不应小于（C）cm。

A、30 B、40 C、50 D、60

347、被电击的人能否获救，关键在于（D）。

A、触电的方式 B、人体电阻的大小

C、触电电压的高底 D、能否尽快脱离电源和施行紧急救护

348、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）。

A、可以随意弯折 B、转弯是，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

349、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

350、长期在高频电磁场作用下，操作者会有什么不良反应？（B）

A、呼吸困难 B、神经失常 C、疲劳无力

351、触电事故中，绝大部分是由于（A）导致人身伤亡的。

A、人体接受电流遭到电击 B、烧伤 C、触电休克

352、从业人员发现直接危及人身安全的紧急情况时，例如气体灭火系统开始开启时，应（A）。

A、停止作业，立即撤离危险现场 B、继续作业

C、向上级汇报，等待上级指令

353、从业人员既是安全生产的保护对象，又是实现安全生产的（C）。

A、关键 B、保证 C、基本要素

354、低压验电笔一般适用于交、直流电压未（C）伏以下。

A、220 B、380 C、500

355、电流为（B）毫安是，称为致命电流。

A、50 B、100 C、120 D、150

356、电器的保险丝只能装在（B）上。

A、零线 B、火线 C、底线

357、电器着火是不能用（C）灭火。

A、四氧化碳或1211灭火 B、沙土 C、水

358、对不符合防雷标准、规范防雷工程专业设计方案，以下（B）应当按照审核结论进行修改并重新报批。

A、建设单位 B、防雷工程专业设计单位 C、工程施工单位

359、发现人员触电时，应（B），使之脱离电源。

A、立即用手拉开触电人员 B、用绝缘物体拨开电源或触电者 C、用铁棍拨开电源线

360、凡设在年平均雷电日大于（C）的地区的计算机信息系统，原则上均应装设计算机信息系统防雷保安器，以防止雷电电磁脉冲过电压和过电流侵入计算机信息系统设备。

A、40 B、45 C、5 D、15

361、废电池随处丢弃会造成（B）的污染。

A、白色污染 B、重金属污染 C、酸雨

362、干粉灭火器多长时间检查一次？（A）

A、半年 B、一年 C、三个月 D、两年

363、根据国家相关规定，电压（D）以下不必考虑防止电击的安全？

A、48伏 B、36伏 C、65伏 D、25伏

364、根据作业环境的不同，安全帽的颜色也不同，如在爆炸性作业场所工作宜戴（A）安全帽。

A、红色 B、黄色 C、白色

365、关于空气的正向压力，下面哪项描述是正确的？（B）

A、当门打开时，空气向内流动 B、当门打开，空气向外流动

C、当发生火灾，系统自动切断电源 D、当发生火灾，烟雾向另外一间房间流动

366、国家颁布的《安全色》标准中，表示警告、主要的颜色为（C）。

A、红色 B、蓝色 C、黄色

367、火灾中对人员威胁最大的是（B）。

A、火 B、烟气 C、可燃物

368、机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（B）m。

A、0.1 B、0.6 C、1.2 D、0.3

369、计算机电源系统的所有节点均应镀铅锡处理（B）连接。

A、热压 B、冷压 C、焊锡 D、直接

370、计算机系统接地应采用（A）。

A、专用底线 B、和大楼的钢筋专用网相连

C、大楼的各种金属管道相连 D、没必要

371、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

372、计算机系统应选用（A）电缆。

A、铜芯 B、铅芯

C、铁芯 D、没有要求

373、进行腐蚀品的装卸作业应戴（B）手套。

A、帆布 B、橡胶 C、棉布

374、人体在电磁场作用下，由于（C）将使人体受到不同程度的伤害。

A、电流 B、电压 C、棉布

375、身上着火后，下列哪种灭火方法是错误的（C）。

A、就地打滚 B、用厚重衣物覆盖压灭火苗 C、迎风快跑

376、生产经营单位必须为从业人员提供符合国家标准或（C）标准的劳动防护用品。

A、当地 B、本单位 C、行业

377、使用新设备，必须了解、掌握其安全技术特征，采取有效的安全防护措施，并对从业人员进行专门的安全生产。（B）

A、当地 B、本单位 C、行业

378.实验地点相对湿度大于75%时，则此实验环境属于易触电的环境：（A）

A、危险 B、特别危险 C、一般

379、通过人身的安全交流电流规定在(A)以下。

A、10mA B、30mA C、50mA

380、下列不属于对物理层信息窃取的是(D)

A、对存储介质的盗取 B、对监视器的窃听

C、对网络线路的窃听 D、对设备屏蔽电磁干扰

381、新、改、扩建项目的安全设施投资应当纳入(C)。

A、企业成本 B、安措经费 C、建设项目概算

382、液体表面的蒸汽与空气形成可燃气体，遇到点火源时，发生一闪即灭的现象称为(C)

A、爆炸 B、蒸发 C、闪燃

383、防雷保安器：防止(B)破坏计算机信息系统的保安装置，可分为两大类：电源

线防雷保安器（简称电源防雷保安器）和信号传输线防雷保安器（简称通道防雷保安器）。

A、直击雷 B、感应雷 C、雷暴 D、雷电电磁脉冲

384、EMC标准是为了保证(D)正常工作而制走的。

A、网络 B、媒体 C、信息 D、系统和设备

385、以下不符合防静电要求的是(B)。

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

386、以下哪些属于系统的物理故障？(A)

A、硬件故障与软件故障 B、计算机病毒

C、人为的失误 D、网络故障和设备环境故障

387、用灭火器灭火时，灭火器的喷射口应该对准火焰的(C)。

A、上部 B、中部 C、根部

388、运输、携带、邮寄计算机信息媒体进出靖的，应当如实向(A)申报。

A、海关 B、工商

C、税务 D、边防

389、在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ (B)

A、产生静电 B、计算机部件腐蚀

C、有污染物 D、B+A

390、在空气不流通的狭小地方使用二氧化碳灭火器可能造成的危险是(B)。

A中毒 B缺氧 C爆炸

391、在雷雨天不要走近高压电杆、铁塔、避雷针、远离至少(C)米以外。

A、IO米 B、15米 C、20米

392、在易燃易爆场所穿(C)最危险。

A、布鞋 B、胶鞋 C、带钉鞋

393、在遇到高压电线断落地面时，导线断落点(B)m内，禁止人员进入。

A、IO B、20 C、30

394、数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？(C)

A、30%-40% B、40%-50% C、45%-60% D、50%-70%

395、计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所

以防雷保安器必须有合理的(B)。

A、屏蔽配置 B、接地配置

C、分流配置 D、均压配置

396、计算站场地宜采用(A)蓄电池。

A、封闭式 B、半封闭式

C、开启式 D、普通任意的

397、多层的楼房中，最适合做数据中心的位置是(D)。

A、楼 B、地下室

C、顶楼 D、除以上外的任何楼层

398、计算机机房是安装计算机信息系统主体的关键场所，是(A)工作的重点，所以

对计算机机房要加强安全管理。

A、实体安全保护 B、人员管理

C、媒体安全保护 D、设备安全保护

399、区域安全，首先应考虑（B），用来识别来访问的用户的身份，并对其合法性进行验证，主要通过特殊标示符、口令、指纹等来实现。

A、来访者所持物 B、物理访问控制 C、来访者所具有的特征 D、来访者所知信息

400、在计算机房出入口处或值班室，应设置（D）和应急断电装置。

A、 电视 B、电扇 C、报警器 D、应急电话

401、下列（A）灭火器是扑救精密仪器火灾的最佳选择。

A、二氧化碳灭火剂 B、干粉灭火剂 C、泡沫灭火剂

402、电气安全主要包括人身安全、（B）安全。

A、照明 B、设备 C、电器 D、空调

403、（C）基于IDEA算法。

A、S/MIME B、SET C、PGP D、SSL

404、

405、(C)是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

406、(D)是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。

A、认证机构 B、密码 C、票据 D、数字证书

407、（D）协议主要用于加密机制。

A、HTTP B、FTP C、TELNET D、SSL

408、（A）原则保证只有发送方与接收方能访问消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

409、（D）原则允许某些用户进行特定访问。

A、保密性 B、鉴别 C、完整性 D、访问控制

410、（B）增加明文冗余度。

A、混淆 B、扩散 C、混淆与扩散 D、都不是

411、3DES加密算法的密钥长度是：（A）。

A、168 B、128 C、56 D、256

412、AES密钥长度不能是（D）。

A、128位 B、192位 C、256位 D、512位

413、AES算法是哪种算法？（A）。

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

414、AES属于哪种加密方式？（B）。

A、流加密 B、分组加密 C、异或加密 D、认证加密

415、CA指的是（A）。

A、证书授权 B、加密认证 C、虚拟专用网 D、安全套接层

416、DES经过（A）轮运算后，左右两部分合在一起经过一个末置换，输出一个64位的密文。（A）

A、16 B、8 C、32 D、4

417、DES算法是哪种算法？（A）

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

418、DES属于哪种加密方式？（B）

A、流加密 B、块加密 C、异或加密 D、认证加密

419、DNSSec中并未采用（C）。

A、数字签名技术 B、公钥加密技术 C、地址绑定技术 D、报文摘要技术

420、ECB指的是（D）。

A、密文链接模式 B、密文反馈模式 C、输出反馈模式 D、电码本模式

421、EC-DSA复杂性的程度是（D）。

A、简单 B、最简单 C、困难 D、最困难

422、EFS可以用在什么文件系统下（C）。

A、FAT16 B、FAT32 C、NTFS D、以上都可以

423、IDEA的密钥长度是多少bit？（D）。

A、56 B、64 C、96 D、128

424、Kerberos是80年代中期，麻省理工学院为Athena项目开发的一个认证服务系统，其目标是把认证、记账和（B）的功能扩展到网络环境。

A、访问控制 B、审计 C、授权 D、监控

425、Kerberos是为TCP/IP网络设计的基于（B）的可信第三方鉴别协议，负责在网络上进行仲裁及会话密钥的分配。

A、非对称密钥体系 B、对称密钥体系 C、公钥体系 D、私钥体系

426、Kerberos是一种网络认证协议。它采用的加密算法是（C）。

A、RSA B、PGP C、DES D、MD5

427、Kerberos算法是一个（B）。

A、面向访问的保护系统 B、面向票据的保护系统

C、面向列表的保护系统 D、面向门与锁的保护系统

428、Kerberos提供的最重要的安全服务是？（A）。

A、鉴别 B、机密性 C、完整性 D、可用性

429、MD5产生的散列值是多少位？（C）。

A、56 B、64 C、128 D、160

430、MD5是按每组512位为一组来处理输入的信息，经过一系列变换后，生成一个（B）为散列值。

A、64 B、128 C、256 D、512

431、MD5是以512位分组来处理输入的信息，每一分组又被划分为（A）32位子分组。

A、16个 B、32个 C、64个 D、128个

432、MD5算法将输入信息M按顺序每组（D）长度分组，即：M1，M2，...，Mn-1，Mn。

A、64位 B、128位 C、256位 D、512位

433、PKI（公共密钥基础结构）中应用的加密方式为（B）。

A、对称加密 B、非对称加密 C、HASH加密 D、单向加密

434、PKI的全称是（D）。

A、Private Key Intrusion B、Public Key Intrusion

C、Private Key Infrastructure D、Public Key Infrastructure

435、PKI无法实现（D）。

A、身份认证 B、数据的完整性 C、数据的机密性 D、权限分配

436、RC4是由RIVEST在1987年开发的一种流式的密文，就是实时地把信息加密成一个整体，它在美国一般密钥长度是128位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）。

A、64位 B、56位 C、40位 D、32位

437、RSA公钥加密系统中，他想给她发送一份邮件，并让她知道是他发出，应选用的加密秘钥是（C）。

A、他的公钥 B、她的公钥 C、他的私钥 D、她的私钥

438、RSA使用不方便的最大问题是（A）。

A、产生密钥需要强大的计算能力 B、算法中需要大数

C、算法中需要素数 D、被攻击过很多次

439、RSA算法建立的理论基础是（C）。

A、DES B、替代想组合 C、大数分解和素数检测 D、哈希函数

440、SHA-1产生的散列值是多少位？（D）。

A、56 B、64 C、128 D、160

441、按密钥的使用个数，密码系统可以分为（C）。

A、置换密码系统和易位密码系统 B、分组密码系统和序列密码系统

C、对称密码系统和非对称密码系统 D、密码系统和密码分析系统

442、充分发挥了DES和RSA两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是：（C）。

A、数字签名 B、数字指纹 C、数字信封 D、数字时间戳

443、从技术角度上看数据安全的技术特征主要包含哪几个方面？（B）。

A、数据完整性、数据的方便性、数据的可用性 B、数据的完整性、数据的保密性、数据的可用性 C、数据的稳定性、数据的保密性、数据的可用性 D、数据的方便性、数据的稳定性、数据的完整性

444、单项散列函数的安全性来自于他的（A）。

A、单向性 B、算法复杂性 C、算法的保密性 D、离散性

445、电路网关防火墙工作在OSI协议的哪一层？（A）。

A、传输层 B、链路层 C、应用层 D、物理层

446、电子邮件的机密性与真实性是通过下列哪一项实现的？（A）

A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密

B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密

C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密

D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

447、端对端加密只需要保证消息都在哪里进行加密？（A）

A、源点和目的地节点 B、经过的每一个节点

C、源点和中间经过的每一个节点 D、所有节点

448、对明文字母重新排列，并不隐藏他们的加密方法属于（C）。

A、置换密码 B、分组密码 C、易位密码 D、序列密码

449、对网络中两个相邻节点之间传输的数据进行加密保护的是（A）。

A、节点加密 B、链路加密 C、端到端加密 D、DES加密

450、发送消息和用发送方私钥加密哈希加密信息将确保消息的：（A）。

A、真实性和完整性 B、真实性和隐私 C、隐私和不可否认性 D。隐私和不可否性

451、高级加密标准AES算法中，加密回合数不可能是（D）。

A、10 B、12 C、14 D、16

452、公钥机制利用一对互相匹配的（B）进行加密，解密。

A、私钥 B、密钥 C、数字签名 D、数字证书

453、公钥加密体制中，没有公开的是（A）。

A、明文 B、密文 C、公钥 D、算法

454、公钥证书提供了一种系统的、可扩展的、统一的（A）。

A、公钥分发方案 B、实现不可否认方案

C、对称密钥分发方案 D、保证数据完整性方案

455、关于CA和数字证书的关系，以下说法不正确的是（B）。

A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由CA签发

B、数字证书一般依靠CA中心的对称密钥机制来实现

C、在电子交易中，数字证书可以用于表明参与方的身份

D、数字证书能以一种不能被假冒的方式证明证书持有人身份

456、关于数字签名说法正确的是（A）。

A、数字签名的加密方法以目前的计算机的运算能力来破解是不现实的

B、采用数字签名，不能够保证信息自签发后到收到为止没有做过任何修改（能保证信息收到后没做个任何修改）

C、采用数字签名，能够保证信息是有签名者自己签名发送的，但由于不是真实的签名，签名者容易否认（签名不容易否认）

D、用户可以采用公钥对信息加以处理，形成数字签名（需使用私钥对信息加以处理）

457、基于私有密钥体制的信息认证方法采用的算法是（D）。

A、素数检测 B、非对称算法 C、RSA算法 D、对称加密算法

458、加密技术不能实现（D）。

A、数据信息的完整性 B、基于密码技术的身份认证 C、机密文件加密 D基于IP头信息的包过滤

459、加密技术不能提供以下哪种安全服务？（D）。

A、鉴别 B、机密性 C、完整性 D可用性

460、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）。

A、对称密钥加密 B、非对称密钥加密 C、 D

461、假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（A）。

A、对称加密技术 B、分组加密技术 C、公钥加密技术 D、单项函数密码技术

462、就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。（C）

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

463、利用非对称密钥体制实现加密通信时，若A要向B发送加密信息，则该加密信息应该使用（B）。

A、A的公钥加密 B、B的公钥加密 C、A的私钥加密 D、B的私钥加密

464、利用物理设备将各类型的无法预测的输入集中起来生成随机数的设备是（A）。

A、随机数生成器 B、伪随机数生成器 C、中央处理 D、非易失存储

465、链路加密要求必须先对链路两端的加密设备进行（C）。

A、异步 B、重传 C、同步 D、备份

466、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？（C）

A、对称的公钥算法 B、非对称私钥算法 C、对称密钥算法 D、非对称密钥算法

467、密码分析的目的是什么？（A）

A、确定加密算法的强度 B、增加加密算法的代替功能

C、减少加密算法的换为功能 D、确定所使用的换位

468、请从下列各项中选出不是HASH函数算法的一项。（D）

A、MD5 B、SHA C、HMAC D、MMAC

469、如今，DES加密算法面临的问题是（A）。

A、密钥太短，已经能被现代计算机暴力破解 B、加密算法有漏洞，在数学上已被破解 C、留有后门，可能泄露部分信息 D、算法过于陈旧，已经有更好的替代方案

470、若单项散列函数的输入串有很小的变化，则输出串（A）。

A、可能有很大的变化 B、一定有很大的变化 C、可能有很小的变化 D、一定有很小的变化

471、散列算法可以做哪些事？（C）。

A、碰撞约束 B、入侵检测 C、组合散列 D、随机数生成器

472、身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（B）。

A、可信性 B、访问控制 C、完整性 D、保密性

473、数字签名常用的算法有（B）。

A、DES算法 B、RSA算法 C、Hash函数 D、AES算法

474、数字签名和随机数挑战不能防范以下哪种攻击或恶意行为？（D）。

A、伪装欺骗 B、重放攻击 C、抵赖 D、DOS攻击

475、数字签名可以解决（D）。

A、数据被泄露 B、数据被篡改 C、未经授权擅自访问 D、冒名发送数据或发送后抵赖

476、数字签名通常使用（B）方式。

A、公钥密码体系中的私钥 B、公钥密码系统中的私钥对数字摘要进行加密

C、密钥密码体系 D、公钥密码体系中公钥对数字摘要进行加密

477、数字信封是用来解决（C）。

A、公钥分发问题 B、私钥分发问题 C、对称密钥分发问题 D、数据完整性问题

478、数字证书不包括（B）。

A、签名算法 B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号 D、颁发数字证书单位的数字签名

479、数字证书的应用阶段不包括（D）。

A、证书检索 B、证书验证 C、密钥恢复 D、证书撤销

480、下列说法中错误的是（D）。

A、非对称算法也叫公开密钥算法 B、非对称算法的加密密钥和解密密钥是分离的 C、非对称算法不需要对密钥通信进行保密 D、非对称算法典型的有RSA算法、AES算法等

481、下列算法中，哪种不是对称加密算法？（C）

A、AES B、DES C、RSA D、RC5

482、下列算法中属于Hash算法的是（C）。

A、DES B、IDEA C、SHA D、RSA

483、以下对于链路加密哪项是正确的？（B）

A、消息只在源点加密，目的节点解密 B、消息在源点加密，在每一个经过的节点解密并加密 C、消息在所有经过的节点中都是加密的，但只在目的节点解密 D、消息以明文形式在节点之间传输

484、以下各种加密算法中属于单钥制加密算法的是（A）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密算法

485、以下各种加密算法中属于双钥制加密算法的是（D）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密486、以下各种算法中属于古典加密算法的是（B）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密487、以下关于CA认证中心说法正确的是（C）。

A、CA认证时使用对称密钥机制的认证方法 B、CA认证中心支负责签名，不负责证书的产生 C、CA认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份 D、CA认证中心不用保持中立，可以随便找一个用户来作为CA认证中心

488、以下关于VPN说法正确的是（B）。

A、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B、VPN指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接

C、VPN不能做到信息认证和身份认证 D、VPN只能提供身份认证、不能提供加密数据的功能

489、以下关于数字签名说法正确的是（D）。

A、数字签名是在所传输的数据后附上一段和传输数据毫无关系的数字信息

B、数字签名能够解决数据的加密传输，即安全传输问题

C、数字签名一般采用对称加密机制 D、数字签名能够解决篡改、伪造等安全性问题

490、以下密码使用方法中正确的是（D）。

A、将密码记录在日记本上以避免忘记 B、任何情况下均不得使用临时性密码

C、密码中的字母不得重复 D、不要使用全部由字母组成的密码

491、以下哪个不包含在证书中？（C）

A、密钥采取的算法 B、公钥及其参数 C、私钥及其参数 D、签发证书的CA名称

492、以下哪个选项不会破坏数据库的完整性？（A）

A、对数据库中的数据执行删除操作 B、用户操作过程中出错

C、操作系统的应用程序错误 D、DBMS或操作系统程序出错

493、以下哪项不属于数据库系统实体安全？（B）

A、环境安全 B、线路安全 C、设备安全 D、媒体安全

494、以下哪一种算法产生最长的密钥？（D）

A、Diffe-Hellman B、DES C、IDEA D、RSA

495、以下认证方式中，最为安全的是（D）。

A、用户名+密码 B、卡+密码 C、用户名+密码+验证码 D、卡+指纹

496、远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（B）

A、知道什么 B、拥有什么 C、是谁 D、双因素认证

497、在3DES算法中，密钥最高可达到多少位？（C）

A、96 B、128 C、168 D、200

498、在IPSec中，（C）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的IPSec协议、密码算法、密钥等信息。

A、ESP B、SPI C、SA D、SP

499、在IPSec中，IKE提供（B）方法供两台计算机建立。

A、解释域 B、安全关联 C、安全关系 D、选择关系

500、在RIP的MD5认证报文中，经过加密的密钥是放在哪里的？（B）

A、保温的第一个表项里 B、报文的最后一个表项里

C、报文的第二个表项里 D、报文头里

501、在非对称加密算法中，涉及到的密钥个数是？（B）

A、一个 B、两个 C、三个 D、三个以上

502、在高级加密标准AES算法中，区块大小为（A）。

A、128位 B、192位 C、256位 D、512位

503、在给定的密钥体制中，密钥与密码算法可以看成是（A）。

A、前者是可变的，后者是固定的 B、前者是固定的，后者是可变的

C、两者都是可变的 D、两者都是固定的

504、在公钥体制中，不公开的是（B）。

A、公钥 B、私钥 C、公钥和私钥 D、私钥和加密算法

505、在密码学中，需要被交换的原消息被称为什么？（D）

A、密文 B、算法 C、密码 D、明文

506、一般证书采用哪个标准？（D）

A、ISO/IEC 15408 B、ISO/IEC 17799 C、BS 7799 D、X. 509V3

507、一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（D）

A、信息的数据和时间戳 B、识别发信的计算机

C、对信息内容进行加密 D、对发送者的身份进行识别

508、在数据库中，下列哪些数据不能加密？（A）

A、索引字段 B、存放日期字段

C、存放密码的 D、存放名称字段

509、在一个网络节点中，链路加密仅在以下哪项中提供安全性？（D）

A、数据链路层 B、物理层

C、通信层 D、通信链路

510、在以下隧道协议中，属于三层隧道协议的是（D）。

A、L2F B、PPTP C、L2TP D、IPSec

511、以下哪一项是基于一个大的整数很难分解成两个素数因数？（B）

A、ECC B、RSA C、DES D、D-H

512、以下哪种数据加密技术可以在基础架构层面进行？（A）

A、IPSec B、Secure Sockets Layer

C、Transport Layer Securit D、RSA

513、目前最安全的身份认证机制是（A）。

A、一次口令机制 B、双因素法

C、基于智能卡的用户身价认证 D、身价认证的单因素法

514、当数据库由于各种原因而使其完整性遭到破坏时，必须采取以下哪项措施来恢复数据库？（C）

A、重新安装数据库 B、换一种数据库

C、使用数据库备份 D、将数据库中的数据利用工具导出，并保存

515、PGP加密算法是混合使用（B）算法和IDEA算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES B、RSA C、IDEA D、AES

516、以下哪些软件是用于加密的软件？（A）

A、PGP B、SHA C、EFS D、DES

517、如果消息接受方要确定发送方身价，则要使用（B）原则。

A、保密性 B、鉴别 C、完整性 D、访问控制

518、对于现代密码破解，（D）是最常的方法。

A、攻破算法 B、监听截获 C、信息猜测 D、暴力破解

519、非对称密码技术的缺点有哪些？（B）

A、密钥持有量减少 B、加/解密速度慢 C、耗用资源较少 D、以上都是

520、CA不能提供下列哪种证书？（D）

A、个人数字证书 B、SSL服务器证书

C、安全电子邮件证书 D、SET服务器证书

521、以下关于混合加密方式说法正确的是（B）。

A、采用公开密钥体制进行通信过程中的加解密处理

B、采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C、采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D、采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密

处理速度快的双重优点

522、果要保证（C）原则，则不能在中途修改消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

523、口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（D）

A、长期没有修改的口令 B、过短的口令

C、两个人共用的口令 D、设备供应商提供的默认的口令

524.非对称密钥的密码技术具有很多优点，其中不包括：（B）。

A、可提供数字签名、零知识证明等额外服务

B、加密/解密速度快，不需占用较多资源

C、通信双方事先不需要通过保密信道交换密钥

D、密钥持有量大大减少

525．DES是一种block（块）密文的加密算法，是把数据加密成多大的块？（B）

A、32位 B、64位 C、128位 D、256位

526．CA数字证书中不包含的信息有（C）。

A、CA的数字签名 B、证书申请者的个人信息

C、证书申请者的私钥 D、证书申请者的公钥信息

527．以下关于对称密钥加密说法正确的是（C）。

A、加密方和解密可以使用不同的算法 B、加密密钥和解密密钥可以是不同的

C、加密密钥和解密密钥必须是相同的 D、密钥的管理非常简单

528、在为计算机设置使用密码时，下面（D）密码是最安全的。

A、12345678 B、66666666

C、20061001 D、72aB@#41

529、（C）的攻击者发生在Web应用层？

A、25% B、50%

C、75% D、90%

530、“U盘破坏者”病毒（Worm.vhy）采用（B）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。

A、网上邻居 B、我的电脑

C、我的文档 D、收藏夹

531、“冲击波”病毒运行时会将自身复制到Windows目录下，并命名为（C）

A、Gsrss.exe B、msbast.exe

C、msblast.exe D、lsass.exe

532、Code Red 爆发于2001年7月，利用微软的IIS漏洞在Web服务器之间传播。针对这一漏洞，微软早在2001年三月就发布了相关的补丁。如果今天服务器仍然感染Code Red，那么属于哪个阶段的问题？（A）

A、系统管理员维护阶段的失误 B、微软公司软件的设计阶段的失误

C、最终用户使用阶段的失误 D、微软公司软件的实现阶段的失误

533、病毒的传播机制主要有哪些？（D）

A、移动存储 B、电子邮件 C、网络共享 D、以上均是

534、病毒的反静态反汇编技术都有（D）。

A、数据压缩 B、数据加密 C、感染代码 D、以上均是

535、病毒在感染计算机系统时，一般（B）感染系统的。

A、病毒程序都会在屏幕上提示，待操作者确认（允许）后

B、实在操作者不觉察的情况下

C、病毒程序会要求操作者制定存储的磁盘和文件夹后

D、在操作者为病毒制定存储的文件名以后

536、杀毒软件时提示“重新启动计算机后删除文件”其主要原因是（A）

A、文件插入了系统关键进程，杀毒时无法处理

B、文件是病毒文件，无法处理

C、由于病毒的加壳形式不同，杀毒时无法正确处理

D、文件正在运行且无法安全的结束，需要其他处理方法

537、蠕虫的目标选择算法有（D）。

A、随机性扫描 B、基于目标列表的扫描

C、顺序扫描 D、以上均是

538、网络钓鱼是指（A）

A、通过大量发送声来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息。

B、网上进行钓鱼活动

C、通过网络组织钓鱼活动，从而获得利益 D、以上都不是

539、不属于常见把入侵主机的信息发送给攻击者的方法是（D）。

A、E-MAIL B、UDP C、ICMP D、连接入侵主机

540、不属于黑客被动攻击的是（A）

A、缓冲区溢出 B、运行恶意软件 C、浏览恶意代码网页 D、打开病毒附件

541、不属于黑客前期收集信息的工具是（D）

A、Nmap B、Xscan C、Nslookup D、LC

542、常见Web攻击方法，不包括？（D）

A、利用服务器配置漏洞 B、恶意代码上传下载

C、构造恶意输入（SQL注入攻击、命令注入攻击、跨站脚本攻击）

D、业务测试

543、常用的抓包软件有（A）。

A、ethereal B、MS office C、fluxay D、netscan

544.网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（A）

A、密码加密后，不会被窃听 B、Cookie字段可以被窃听

C、报文和帧可以窃听 D、高级窃听者还可以进行ARPSpoof，中间人攻击

545、除了在代码设计开发阶段预防SQL注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（C）

A、禁止将任何高权限账号（例如sa,dba等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户

B、拒绝用户访问敏感的系统存储过程

C、禁止用户访问的数据库表 D、限制用户所能够访问的数据库表

546、防止用户被冒名所欺骗的方法是（A）。

A、对信息源发放进行身份验证 B、进行数据加密

C、对访问网络的流量进行过滤和保护 D、采用防火墙

547、给电脑设置多道口令，其中进入电脑的第一道口令是（B）。

A、系统口令 B、CMOS口令

C、文件夹口令 D、文档密码

548、攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息重新发往B称为（D）。

A、中间人攻击 B、口令猜测器和字典攻击

C、强力攻击 D、回放攻击

549、故意制作、传播计算机病毒，造成计算机信息系统不能正常运行，但如果后果不严重就无罪，可以原谅，这种说法（C）。

A、不对，对这种蓄意破坏行为不能原谅 B、即使不是故意的，后果也不很严重

C、对。我国实行成文法，根据《中华人民共和国刑法》第286条的规定，只有造成严重后果者才有罪

D、无法断定

550、关于80年代Mirros蠕虫危害的描述，哪句话是错误的？（B）

A、占用了大量的计算机处理器的时间，导致拒绝股务

B、窃取用户的机密信息，破坏计算机数据文件

C、该蠕虫利用Unix系统上的漏洞传播

D、大量的流量堵塞了网络，导致网络瘫痪

551、关于黑客注入攻击说法错误的是： (D)

A、它的主要原因是程序对用户的输入缺乏过滤

B、一般情况下防火墙对它无法防范

C、对它进行防范时要关注操作系统的版本和安全补丁

D、注入成功后可以获取部分权限

552、基于主机评估报告对主机进行加固时，第一步是（B）。

A、账号、口令策略修改 B、补丁安装

C、文件系统加固 D、日志审核增强

553、计算机病毒会对下列计算机服务造成威胁，除了（C）。

A、完整性 B、有效性

C、保密性 D、可用性

554、计算机病毒是一段可运行的程序，它一般（C）保存在磁盘中。

A、作为一个文件 B、作为一段数据

C、不作为单独文件 D、作为一段资料

555、什么方式能够从远程绕过防火墙去入侵一个网络？(D)

A、IP services\_ B、Active ports

C、Identified network topology D、Modem banks

556、输入法漏洞通过（D）端口实现的。

A、21 B、23 C、445 D、3389

557、特洛伊木马攻击的威胁类型属于（B）。

A、授权侵犯威胁 B、植入威胁

C、渗入威胁 D、旁路控制威胁

558、通常黑客扫描目标机的445端口是为了(B)。

A、利用NETBIOS SMB服务发起DOS攻击

B、发现并获得目标机上的文件及打印机共享

C、利用SMB服务确认Windows系统版本

D、利用NETBIOS服务确认Windows系统版本

559、网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？(A)

A、残余风险评估阶段 B、检查阶段

C、入侵检测系统监控阶段 D、网络异常流量临控阶段

560、网络病毒预防范阶段的主要措施是什么？(A)

A、强制补丁、网络异常流量的发现 B、强制补丁、入侵检测系统监控

C、网络异常流量的发现、入侵检测系统的监控阶段 D、缺少D选项

561、下列除了(B)以外，都是防范计算机病毒侵害的有效方法。

A、使用防病毒软件 B、机房保持卫生，经常进行消毒

C、避免外来的磁盘接触系统 D、网络使用防病毒网关设备

562、下列除了(A)以外，都是计算机病毒传

A、通过操作员接触传播 B、通过U盘接触传播

C、通过网络传播 D、通过电子播的途径邮件传播

563、下列措施中，(C)不是减少病毒的传染

和造成的损失的好办法。

A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B、外来的文件要经过病毒检测才能使用，不要使用盗版软件

C、不与外界进行任何交流，所有软件都自行开发

D、定期用抗病毒软件对系统进行查毒、杀毒

564、下列哪项是跨站脚本Cross Site Scripting攻击具体事例？（B）

A、搜索用户 B、发帖子，发消息 C、上传附件 D、下载文件

565、下列哪项为信息泄露与错误处理不当Information Leakage and Improper

Error Handlina攻击具体实例？(D)

A、不明邮件中隐藏的html链接 B、发帖子，发消息

C、上传附件 D、错误信息揭示路径

566、下面哪一项是黑客用来实施DDoS攻击的工具？(D)

A、LC5 B、Rootkit C、Icesword D、Trinoo

567、以下哪个工具可以抹去所有NT/2K配置，并将其还原到初始状态？(A)

A、Rollback. exe B、Recover. exe C、Zap. exe D、Reset. exe

568、以下哪个工具通常是系统自带任务管理器的替代？(D)

A、Regmon B、Filemon C、Autoruns D、Process explorer

569、以下哪个针对访问控制的安全措施是最容易使用和管理的？(C)

A、密码 B、加密标志 C、硬件加密 D、加密数据文件

570、以下哪项不是分布式拒绝服务攻击常用的工具？(D)

A、Trinoo B、Trinoo C、TFN D、synkill

571、以下哪项不属于针对数据库的攻击？(D)

A、特权提升 B、强力破解弱口令或默认的用户名及口令

C、SQL注入 D、利用xss漏洞攻击

572、以下哪项工具不适合用来做网络监听？(B)

A、sniffer B、Webscan C、 Windump D、 D-Iris

573、以下哪项是SYN变种攻击经常用到的工具？(B)

A、sessionIE B、synkill C、TFN D、Webscan

574、以下哪一项不是流氓软件的特征？(D)

A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装

B、通常添加驱动保护使用户难以卸载

C、通常会启动无用的程序浪费计算机的资源

D、通常会显示下流的言论

575、一个数据仓库中发生了安全性破坏。以下哪一项有助于安全调查的进行？(B)

A、访问路径 B、时戳 C、数据定义 D、数据分类

576、以下哪一项不属于恶意代码？(C)

A、病毒 B、蠕虫 C、宏 D、特洛伊木马

577、以下哪一项不属于计算机病毒的防治策略？(D)

A、防毒能力 B、查毒能力 C、杀毒能力 D、禁毒能力

578、以下哪一项是常见Web站点脆弱性扫描工具？(A)

A、Appscan B、Nmap C、Sniffer D、LC

579、以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？(A)

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将臀陆信息写入记事本

580、以下哪种符号在SQL注入攻击中经常用到？(D)

A、$\_ B、1 C、@ D、;

581、以下哪种工具能从网络上检测出网络监听软件(A)

A、sniffdet, , B、purify, , C、Dsniff D、WireShark

582、以下哪种攻击可能导致某些系统在重组IP分片的过程中宕机或者重新启动？(B)

A、分布式拒绝服务攻击 B、Ping of Death

C、NFS攻击 D、DNS缓存毒化攻击

583、下面哪部分不属于入侵的过程？(B)

A、数据采集 B、数据存储 C、数据检测 D、数据分析

584、以下对木马阐述不正确的是(A)。

A、木马可以自我复制和传播

B、有些木马可以查看目标主机的屏幕

C、有些木马可以对目标主机上的文件进行任意揉作

D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。

585、由于攻击者可以借助某种手段，避开DBMS以及应用程序而直接进入系统访问

数据，我们通常采取以下哪种方式来防范？(A)

A、数据库加密

B、修改数据库用户的密码，将之改得更为复杂

C、使用修改查询法，使用户在查询数据库时需要满足更多的条件

D、使用集合法

586、在大多数情况下，病毒侵入计算机系统以后，(D)。

A、病毒程序将立即破坏整个计算机软件系统

B、计算机系统将立即不能执行我们的各项任务

C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

587、在确定威胁的可能性时，可以不考虑以下哪项？(D)

A、威胁源 B、潜在弱点

C、现有控制措施 D、攻击所产生的负面影响

588、在以下人为的恶意攻击行为中，属于主动攻击的是(A)。

A、身份假冒 B、数据GG C、数据流分析 D、非法访问

589、下面哪一种攻击方式最常用于破解口 令？(B)

A、哄骗( spoofing) B、字典攻击(dictionary attack)

C、拒绝服务(DoS) D、WinNuk

590、针对DNS服务器发起的查询DoS攻击，属于下列哪种攻击类型？(C)

A、syn flood B、ack flood C、 udpflood D、Connection flood

591、下列哪项不是安全编码中输入验证的控制项？(D)

A、数字型的输入必须是合法的数字

B、字符型的输入中对’进行特殊处理

C、验证所有的输入点，包括Get，Post，Cookie以及其他HTTP头

D、正确使用静态查询语句，如PreDaredStatement

592、以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？(C)

A、早期的SMTP协议没有发件人认证的功能

B、网络上存在大量开放式的邮件中转服务器，导致垃圾邮件的来源难于追查

C、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因

D、Internet分布式管理的性质，导致很难控制和管理

593、以下哪种方法是防止便携式计算机机密信息泄露的最有效方法？（A）

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将登录信息写入记事本

594、以下哪种攻击属于DDoS类攻击？（A）

A、SYN变种攻击 B、smurf攻击 C、arp攻击 D、Fraggle攻击

595、URL访问控制不当不包括（D）

A、Web应用对页面权限控制不严 B、缺乏统一规范的权限控制框架

C、部分页面可以直接从URL中访问 D、使用分散登录认证

596、Web应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（A）

A、静态密码 B、短信挑战 C、指纹认证 D、图片认证

597、Web应用漏洞按类别进行排名，由多到少正确的顺序为？（A）

A、跨站脚本、注入、恶意代码、引用不当

B、注入、跨站脚本、恶意代码、引用不当

C、恶意代码、跨站脚本、注入、引用不当

D、引用不当、跨站脚本、注入、恶意代码

598、从技术角度，以下不是漏洞来源的是（D）

A、软件或协议设计时候的瑕疵 B、软件或协议实现中的弱点

C、软件本身的瑕疵 D、显示卡内存容量过低

599、（C）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A、身份假冒 B、数据篡改 C、信息窃取 D、越权访问

600、有关密码学分支的定义，下列说法中错误的是（D）

A、密码学是研究信息系统安全保密的科学，由两个相互对立、相互斗争、而且又相辅相成、相互渗透的分支科学所组成的、分别称为密码编码学和密码分析学

B、密码编码学是对密码体制、密码体制的输入输出关系进行分析、以便推出机密变量、包括明文在内的敏感数据

C、密码分析学主要研究加密信息的破译或信息的伪造

D、密码编码学主要研究对信息进行编码，实现信息的隐藏

601、与RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（C）

A、数字签名 B、鉴别机制 C、加密机制 D、数据完整性

602、以下哪项是数据库加密方法中的库外加密的缺点？（A）

A、即使访问一条数据也要对整个数据库解密 B、密钥管理比较复杂

C、加密之后不能完整的查询数据 D、密钥过于简单，容易被破解

603、以下哪项数据中涉及安全保密的最主要问题？（A）

A、访问控制问题 B、数据完整性 C、数据正确性 D、数据安全性

604、以下哪一个最好的描述了数字证书？（A）

A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，它使得黑客不能得知用户的身份

C、网站要求用户使用用户名和密码登陆的安全机制

D、伴随在线交易证明购买的收据

605、TCP SYN Flood网络攻击时利用了TCP建立连接过程需要（C）次握手的特点而完成对目标进行攻击的。

A、1 B、2 C、3 D、6

二、多项选择题（606-789）

606、COBIT度量过程的三个纬度分别是（ABC）。

A、能力 B、绩效 C、控制度 D、能力成熟度

607、IT系统内网与互联网连接检查手段有哪些？（BCD）

A、工具扫描 B、人员访谈 C、人工检查 D、文档检查

608、公司应该采取以下措施，对第三方访问进行控制。（ABCD）

A、公司应于第三发公司法人签署保密协议，并要求其第三方个人签署保密承诺，此项工作应在第三方获得网络与信息资产的访问权限之前完成

B、实行访问授权管理，未经授权，第三方不得进行任何形式的访问

C、公司应加强第三方访问的过程控制，监督其活动及操作，对其进行适当的安全宣传与培训

D、第三方人员应佩戴易于识别的标志，并在访问公司重要场所时有专人陪同

609、计算机信息系统安全的三个相辅相成，互补互通的有机组成部分是（ABD）

A、安全策略 B、安全法规 C、安全技术 D、安全管理

610、劳动合同中应包含网络与信息安全条款，这些条款规定（ACD）。

A、员工的安全责任和违约罚则

B、安全责任不可延伸至公司场所以外和正常工作时间以外

C、安全责任可延伸至公司场所以外和正常工作时间以外

D、如必要，一些安全责任应在雇佣结束后延续一段特定的时间

611、审核是网络安全工作的核心，下列应用属于主动审核的是：（CD）

A、Windows事件日志记录 B、数据库的事务日志记录

C、防火墙对访问站点的过滤 D、系统对非法链接的拒绝

612、通用准则CC实现的目标有（ABC）

A、成为统一的国际通用安全产品、系统的安全标准

B、在不同国家达成协议，相互承认产品安全等级评估

C、概述IT产品的国际通用性 D、都不是

613、系统用户账号登记表应包括（ABCD）。

A、使用者姓名、部门、职务、联系电话 B、账号权限

C、批准人、开通人 D、开通时间、到期日

614、下列情况哪些是对公司经营管理的影响为“一般”级别的互联网网络安全事件？（ABD）

A、发生未到达“预警”的一般性安全事件

B、出现新的漏洞，尚未发现利用方法或利用迹象

C、有来自境外的网络性能明显下降的报警，并且其技术原因普遍适用于我国互联网 D、出现新的蠕虫/病毒或其它恶意代码，尚未证明可能造成严重危害

615、信息安全的主要原则有（BCD）

A、认证性 B、保密性 C、可用性 D、完整性

**616、针对支撑系统，除业务关联性、对业务网络的影响，资产价值主要体现在（ACD）几个方面。 缺少D选项**

**A、业务收益的影响 B、设备购买成本 C、面向客户的重要程度 D、**

617、IT系统病毒泛滥的主要原因有哪些？（ABCD）

A、主机和终端防病毒软件缺乏统一管理

B、主机和终端防病毒软件没有设置为自动更新或更新周期较长

C、防病毒服务器没有及时更新放病毒库

D、缺乏防病毒应急处理流程和方案

618、IT系统病毒防护评估检查对象包括哪些内容？（ABCD）

A、防病毒服务器 B、重要应用Windows主机

C、Windows终端 D、主机管理员

619、互联网连接防火墙设备的安全策略配置要求包括哪几点（ABCD）。

A、远程登录是否禁止telnet方式 B、最后一条策略是否是拒绝一切流量

C、是否存在允许any to any的策略

D、是否设置了管理IP，设备只能从管理IP登录维护

620、《安全基线标准》在安全管理层面主要围绕哪几部分考评安全基线？（ABC）

A、组织架构管理 B、人员安全管理 C、运维安全管理 D、制度安全管理

621、IT系统维护人员权限原则包括（ACD）。

A、工作相关 B、最大授权 C、最小授权 D、权限制约

622、安全系统加固手册中关于造成系统异常中断的各方面因素，主要包括哪三方面（ABD）

A、人为原因 B、环境原因 C、生产原因 D、设备原因

623、IT系统维护人员权限原则包括（ACD）

A、工作相关 B、最大授权 C、最小授权 D、权限制约

624、计算当前Linux系统中所有用户的数量，可以使用（ABC）命令

A、wc -l /etc/passwd B、wc -l</etc/passwd

C、cat/etc/passwd|wc -l D、cat/etc/passwd>wc -l

625、Solarid系统中，攻击者在系统中增加账户会改变哪些文件？（AB）

A、shadow B、passwd C、inetd,conf D、hosts

626、Syn Flood攻击的现象有以下哪些？（ABC）

A、大量连接处于SYN\_RCVD状态 B、正常网络访问受阻

C、系统资源使用率高

627、UNIX安全审计的主要技术手段有哪些？（ABCDEF）

A、文件完整性审计 B、用户、弱口令审计 C、安全补丁审计

D、端口审计 E、进程审计 F、系统日志审计

628、Unix系统提供备份工具有（ABCD）

A、cp：可以完成把某一目录内容拷贝到另一目录

B、tar：可以创建、把文件添加到或从一个tar档案中解开文件

C、cpio：把文件拷贝进或拷贝出一个cpio档案或tar档案

D、dump：用来恢复整个文件系统或提取单个文件

629、操作系统应利用安全工具提供以下哪些访问控制功能？（ABC）

A、验证用户身份，必要的话，还应进行终端或物理地点识别

B、记录所有系统访问日志

C、必要时，应能限制用户连接时间 D、都不对

630、从哪些地方可以看到遗留痕迹？（ABCD）

A、回收站 B、最近使用过的文件 C、注册表 D、文件最后更改的时间戳631、

632、关于Windows活动目录说法正确的是（ABD）。

A、活动目录是采用分层结构来存储网络对象信息的一种网络管理体系

B、活动目录可以提供存储目录数据和网络用户级管理员使用这些数据的方法

C、利用活动目录来实现域内计算机的分布式管理

D、活动目录与域紧密结合构成与目录林和域目录树，使大型网络中庞大、复杂的网络管理、控制、访问变得简单，使网络管理效率更高

633、建立堡垒主机的一般原则是（AC）。

A、最简化原则 B、复杂化原则 C、预防原则 D、网络隔离原则

634、逻辑空间主要包括哪些部分？（ABDE）

A、TABLESPACES B、SEGMENTS C、DATAFILE

D、EXTENTS E、BLOCK

635、哪些属于Windows日志？（ABCD）

A、AppEvent.Evt B、SecEvent.Evt C、SysEvent.Evt D、W3C扩展日志

636、如何设置listener口令？（ACDE）

A、以Oracle用户运行lsnrctl命令 B、set log\_file

C、change\_password D、set password E、save\_config

637、审计启动其日志有哪两种存放方式？（BD）

A、NONE B、OS C、TRUE D、SYS.AUD$

638、生产服务器通常都是UNIX平台，资产价值最高，不直接连接外部网络，主要的安全需求是（ABD）

A、访问控制 B、账号口令 C、数据过滤 D、权限管理和补丁管理

639、使用md5sum工具对文件签名，以下说法正确的是？（ADE）

A、md5sum对任何签名结果是定长的16字节

B、md5sum对文件签名具有不可抵赖性

C、md5sum是对文件进行加密运算得出签名，不同文件结果几乎不相同

D、md5sum是对文件进行哈希运算得出签名，不同文件结果几乎不相同

E、md5sum对文件签名时，与文件的日期和时间无关

640、为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有（ABCD）

A、口令/账号加密 B、定期更换口令

C、限制对口令文件的访问 D、设置复杂的、具有一定位数的口令

641、文件系统是构成Linux基础，Linux中常用文件系统有（ABD）？

A、ext3 B、ext2 C、hfs D、reiserfs

642、下列关于UNIX下日志说法正确的是（AC）

A、wtmp记录每一次用户登录和注销的历史信息

B、acct记录每个用户使用过的命令

C、sulog记录su命令的使用情况

D、acct记录当前登录的每个用户

643、下列哪些操作可以看到自启动项目？（ABD）

A、注册表 B、开始菜单 C、任务管理器 D、msconfig

644、下列哪些命令行可用于查看当前进程？（ABC）

A、Ps -ef B、Strings -f/proc/[0-9]\*/cmdline

C、Ls -al /proc/[0-9]\*/exe D、Cat/etc/inetd.conf

645、下面操作系统中，哪些是UNIX操作系统？（CD）

A、Red-hat Linux B、Novell Netware C、Free BSD D、SCO Unix

646、严格的口令策略应当包含哪些要素（ABC）

A、满足一定的长度，比如8位以上 B、同时包含数字，字母和特殊字符

C、系统强制要求定期更改口令 D、用户可以设置空口令

647、在Solaris 8 下，使用ps -ef命令列出进程中有一行如下“root 1331 0 00:01:00? 0:00 /usr/sbin/inetd -s -t”，以下说法正确的是（ABE）

A、参数-t是trace，记录包括IP和PORT等信息

B、参数-t对于UDP服务无效 C、进程启动的时间不能确定

D、进程已经运行了1分钟 E、进程的父进程号是1

648、在Solaris 8 下，以下说法正确的是：（AB）

A、/etc/rc2.d里S开头的文件在系统缺省安装的缺省级别会自动运行

B、/etc/rc3.d里S开头的文件在系统缺省安装的缺省级别会自动运行

C、/etc/init.d里的文件在系统启动任何级别时会自动运行

D、init 0是进入单用户级别 E、init 6命令会运行所有级别的rc目录下以S开头的文件

649、在Solaris 8 下，以下说法正确的是：（BC）

A、PATH环境变量最后带有“.”，会使当前目录的命令比其他目录的命令有限执行

B、可以修改/etc/inittab里ttymon的参数，使得登录的SHELL在无输入时自动退出

C、在使用/bin/ksh时，可以设置TMOUT值，使得登录的SHELL在无输入时自动退出

D、在/etc/login中，可以设置TIMEOUT值，使得登录的SHELL在无输入时自动退出

E、tar xvf命令的意思是以tar格式解开输入，并且保持文件属性等参数不变

650、在配置Apache访问控制时，Allow和Deny指令可以允许或拒绝来自特定主机名或主机名地址的访问。那么下列哪些配置是不正确的？（AD）

A、Order allow,deny Allow from 192.101.205

B、B、Order deny,allow Deny from all Allow from example

C、C、Order deny,allow Deny from 192.101.205

D、D、Order allow,deny Deny from 192.101.205 Allow from all

651、造成操作系统安全漏洞的原因是（ABC）。

A、不安全的编程语言 B、不安全的编程习惯

C、考虑不周的架构设计 D、人为的恶意破坏

652、针对Linux主机，一般的加固手段包括（ABC）。

A、打补丁 B、关闭不必要的服务 C、限制访问主机 D、切断网络

653、做系统快照，查看端口信息的方式有（AD）。

A、netstat -an B、net share C、net use D、用taskinfo来查看连接情况

654、网厅安全解决方案主要从哪几个方面对网厅安全进行建议和指导？（ABCD）

A、安全管理 B、安全防护 C、安全运维 D、灾备/恢复

655、IT系统软件设计中应当考虑并执行安全审计功能，详细记录访问信息的活动，包括（ABCD）。

A、记录的活动以是否有数据的修改、应用程序的异常关闭、异常删除触发

B、应用系统应当配置单独的审计数据库，审计记录应单独存放，并设置严格的边界访问控制，只有安全管理人员才能够看到审计记录

C、信息系统的审计功能包括：事件日期、时间、发起者信息、类型、描述和结果

D、应用系统的审计进程为后台处理，与应用系统运行同步进行，并且对于审计进程应当涉及相应的守护进程，一旦出现异常停止系统可重新启动审计进程，从而保障审计的“完整性”

656、IPSec的配置步骤包括：（ABCD）

A、防火墙基本配置 B、定义保护数据流和域间规则

C、配置IPSec安全提议 D、配置IKEPeer

657、Juniper路由器在配置SSH访问时应注意如下（ABCD）细节。

A、建立允许访问的SSH-ADDRESSES过滤器

B、确保只允许来自内部接口的授权用户访问

C、针对SSH进行限速以保护路由引擎

D、过滤器应用在loopback接口

658、对于使用RPF反向地址验证，以下说法错误的是：（BCD）。

A、对称路由可以使用 B、非对称路由可以使用

C、有些情况不可以使用，但与对称或非对称路由无关

D、在任何情况下都可以使用

659、防病毒服务升级检查包括如下几项内容？（ABC）

A、检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决

B、在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本

C、对重要的服务器，定期抽查防病毒客户端的病毒库升级情况

660、防范DOS攻击的方法主要有（ABCD）。

A、安装Dos检测系统 B、对黑洞路由表里的地址进行过滤

C、及时打好补丁 D、正确配置TCP/IP参数

661、防火墙trust域中的客户机通过nat访问untrust中的服务器的ftp服务，已经允许客户机访问服务器的tcp21端口，但只能登陆到服务器，却无法下载文件，以下解决办法中可能的是：（ABC）

A、修改trust untrust域间双向的默认访问策略为允许

B、FTP工作方式为port模式时，修改untrust trust域间in方向的默认访问策略为允许 C、在trust untrust域间配置中启用detect ftp

D、FTP工作方式为passive模式时，修改untrust trust域间in方向的默认访问策略为允许

662、防火墙不能防止以下哪些攻击？（ABD）

A、内部网络用户的攻击 B、传送已感染病毒的软件和文件

C、外部网络用户的IP地址欺骗 D、数据驱动型的攻击

663、防火墙常见的集中工作模式有（ABC）。

A、路由 B、NAT C、透明 D、旁路

664、防火墙的缺陷主要有（ABCD）。

A、限制有用的网络服务 B、无法防护内部网络用户的攻击

C、不能防备新的网络安全问题 D、不能完全防止传送已感染病毒的软件或文件

665、防火墙的日志管理应遵循如下原则：（BC）

A、本地保存日志 B、本地保存日志并把日志保存到日志服务器上

C、保持时钟的同步 D、在日志服务器保存日志

666、防火墙的特征是（ABCD）。

A、保护脆弱和有缺陷的网络服务 B、加强对网络系统的访问控制

C、加强隐私，隐藏内部网络结构 D、对网络存取和访问进行监控审计

667、防火墙的主要功能有哪些？（ABCD）

A、过滤进、出网络的数据 B、管理进、出网络的访问行为

C、封堵某些禁止的业务，对网络攻击进行检测和报警

D、记录通过防火墙的信息内容和活动

668、防火墙的作用主要有（ABCD）。

A、实现一个公司的安全策略 B、创建一个阻塞点

C、记录Internet活动 D、限制网络暴露

669、防火墙技术，涉及到（ABCD）。

A、计算机网络技术 B、密码技术 C、软件技术 D、安全操作系统

670、防火墙可以部署在下列位置：（ABCD）。

A、安全域边界 B、服务器区域边界

C、可信网络区域和不可信网络区域之间 D、根据网络特点设计方案

671、防火墙配置时应确保（ABCD）服务不开放。

A、Rlogin B、NNTP C、Finger D、NFS

672、启用Cisco设备的访问控制列表，可以起到如下作用（ABC）。

A、过滤恶意和垃圾路由信息 B、控制网络的垃圾信息流

C、控制未授权的远程访问 D、防止DDoS攻击

673、如果Cisco设备的VTY需要远程访问，则需要配置（ABCD）。

A、至少8位含数字、大小写、特写字符的密码 B、远程连接的并发数目

C、访问控制列表 D、超市退出

674、如果需要配置Cisco路由器禁止从网络启动和自动从网络下载初始配置文件，配置命令包括（AB）。

A、no boot network B、no service config C、no boot config D、no service network

675、入侵检测的内容主要包括：（BC）。

A、独占资源、恶意使用 B、试图闯入或成功闯入、冒充其他用户

C、安全审计 D、违反安全策略、合法用户的泄露

676、入侵检测系统包括以下哪些类型？（AC）

A、主机入侵检测系统 B、链路状态入侵检测系统

C、网络入侵检测系统 D、数据包过滤入侵检测系统

677、随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器（sniffer）来监听整个子网的办法不再可行。可选择解决的办法有（ABCD）。

A、使用交换机的核心芯片上的一个调试的端口

B、把入侵检测系统放在交换机内部或防火墙等数据流的关键入口

C、采用分解器（tap）

D、使用以透明网桥模式接入的入侵检测系统

678、通常要求把路由器的日志存储在专用日志服务器上，假设把Cisco路由器日志存储在192.168.0.100的syslog服务器上，需要在路由器侧配置的操作时：（ABCD）。

A、使用Router(config)# logging on启用日志：使用Router(config)# logging trap information将记录日志级别设定为“information”

B、使用Routee(config)# logging192.168.0.100将记录日志类型设定为“local6”

C、使用(config)# logging facility local6将日志发送到192.168.0.100

D、使用(config)# logging sourceinterface loopback0设定日志发送源loopback0

679、通过SSL VPN接入企业内部的应用，其优势体现在哪些方面：（ABCD）。

A、应用代理 B、穿越NAT和防火墙设备

C、完善的资源访问控制 D、抵御外部攻击

680、网络地址端口转换（NAPT）与普通地址转换有什么区别？（AD）

A、经过NAPT转换后，对于外网用户，所有报文都来自于同一个IP地址

B、NAT只支持应用层的协议地址转换

C、NAPT只支持网络层的协议地址转换

D、NAT支持网络层的协议地址转换

681、网络攻击的类型包括以下哪几种？（ABCD）

A、窃取口令 B、系统漏洞和后门 C、协议缺陷 D、拒绝服务

682、网络面临的典型威胁包括（ABCD）。

A、未经授权的访问 B、信息在传送过程中被截获、篡改

C、黑客攻击 D、滥用和误用

683、网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，该类病毒程序大规模爆发后，会对相关网络造成拒绝服务攻击，为了防止受到网络蠕虫的侵害，应当注意对（ACD）及时进行升级更新。

A、计算机操作系统 B、计算机硬件 C、文字处理软件 D、应用软件

684、下列关于NAT地址转换的说法中哪些事正确的：（ABCD）。

A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

B、地址转换可以按照用户的需要，在局域网内向外提供FTP、WWW、Telnet等服务

C、有些应用层协议在数据中携带IP地址信息，对它们作NAT时还要修改上层数据中的IP地址信息

D、对于某些非TCP、UDP的协议（如ICMP、PPTP），作上层NAT时，会对它们的特征参数（如ICMP的id参数）进行转换。

685、下列哪两项正确描述了由WPA定义的无线安全标准？（BC）

A、使用公开密钥的认证方法 B、当客户端连接的时候都要进行动态密钥交换

C、包含PSK认证 D、定制了一个经常更换的静态的加密密钥来增强安全性

686、下列配置中，可以增强无线AP（access point）安全性的有（ABCD）。

A、禁止SSID广播 B、禁用DHCP服务

C、采用WPA2-PSK加密认证 D、启用MAC地址接入过滤

687、下面可以攻击状态检测的防火墙方法有：（ABD）

A、协议隧道攻击 B、利用FTP-pasv绕过防火墙认证的攻击

C、ip欺骗攻击 D、反弹木马攻击

688、下面什么路由协议不可以为HSRP的扩充：（ABC）

A、SNMP B、CDP C、HTTP D、VRRP

689、下面什么协议有MD5认证：（ABC）

A、BGP B、OSPF C、EIGER D、RIPversion 1

690、下面是网络安全技术的有：（ABC）

A、防火墙 B、防病毒 C、PKI D、UPS

691、选购一个防火墙时应该考虑的因素有：（ABCD）

A、网络受威胁的程度 B、可能受到的潜在损失

C、站点是否有经验丰富的管理员 D、未来扩展的需要

692、一台路由器的安全快照需要保存如下哪些信息？（AB）

A、当前的配置--running-config B、当前的开放端口列表

C、当前的路由表 D、当前的CPU状态

693、以下对于包过滤防火墙的描述正确的有（ACD）。

A、难以防范黑客攻击 B、处理速度非常慢

C、不支持应用层协议 D、不能处理新的安全威胁

694、以下对于代理防火墙的描述正确的有（ABCD）。

A、能够理解应用层上的协议 B、时延较高，吞吐量低

C、能做复杂一些的访问控制，并做精细的认证和审核 D、可伸缩性较差

695、以下关于L2TP VPN配置注意事项的说法中正确的有：（ABC）

A、L2TP的LNS端必须配置虚拟接口模板（Virtual-Template）的IP地址，该虚拟接口模板需要加入域

B、防火墙缺省需要进行隧道的认证。如果不配置认证，需要undo tunnel authentication命令

C、为了使L2TP拨号上来的用户分配的地址不能喝内网用户的地址在同一个网段

D、LNS端不允许配置多个L2TP-Group

1. 以下哪几项关于安全审计和安全审计系统的描述是正确的？（CD）

A、对入侵和攻击行为只能起到威慑作用

B、安全审计不能有助于提高系统的抗抵赖性

C、安全审计是对系统记录和活动的独立审查和检验

D、安全审计系统可提供侦破辅助和取证功能

697、以下哪些属于网络欺骗方式？（ABCD）

A、IP欺骗 B、ARP欺骗 C、DNS欺骗 D、Web欺骗

698、以下哪些是防火墙规范管理需要的？（ABCD）

A、需要配置两个防火墙管理员 B、物理访问防火墙必须严密地控制

C、系统软件、配置数据文件在更改后必须进行备份

D、通过厂商指导发布的硬件和软件的bug和防火墙软件升级版

699、以下硬件安装维护重要安全提示正确的有：（ABCD）

A、不要在雷雨天气进行故障处理 B、保持故障处理区域的干净、干燥

C、上防静电手套或防静电腕带再执行安装和更换操作

D、在使用和操作设备时，需要按照正确的操作流程来操作

700、以下属于DTE(Data Terminal Equipment)数据终端设备的有（AB）

A、路由器 B、PC C、交换机 D、HUB

701、在防火墙的“访问控制”应用中，内网、外网、DMZ三者的访问关系为：（ABD）

A、内网可以访问外网 B、内网可以访问DMZ区

C、DMZ区可以访问内网 D、外网可以访问DMZ区

702、关于GRE校验和验证技术，当本端配置了校验和而对端没有配置校验和时，以下叙述正确的有（BC）。

A、本端对接收报文检查校验和 B、对端对接收报文检查校验和

C、本端对发送报文计算校验和 D、对端对发送报文计算校验和

703、配置PPP链路层协议时，链路层协议状态始终不能转为Up状态的处理建议：（ABCD）

A、PPP链路两端的接口上配置的参数和验证方式都必须一致，LCP检查才能成功

B、如果LCP协商失败，请检查LCP配置协商参数

C、请检查验证方式配置是否正确。因为LCP协商中，包含验证方式的协商。因为LCP协商中，包含验证方式的协商。验证方式协商失败也会导致LCP协商失败

D、接口试图下先执行shutdown命令将接口关闭，再执行undo shutdown命令重启接口

704、对DNSSEC的描述正确的有（AC）。

A、为DNS数据提供来源验证，即保证数据来自正确的名称服务器

B、DNSSEC可防御DNS Query Flood攻击

C、为域名数据提供完整性验证，即保证数据在传输的过程中没有被篡改

D、实施DNSSEC后，只需升级软件系统，对网络、服务器等硬件设备不需考虑

705、MySQL安装程序会给出三种选择，用户可以根据自身的需要选择一种适合的安装方式，以下哪些是正确的？（ABD）

A、Typical（典型安装） B、Compact(最小安装)

C、Full(全部安装) D、Custom(选择安装)

706、MySQL中用DROP语句可删除数据库和数据表，以下哪句是正确的语法？（ABCD）

A、DROP TABLE table\_name1 B、DROP TABLE table\_name1,table\_name2

C、DROP TABLE IF EXISTS table\_name1 D、DROP DATABASE DB name1

707、Oracle 7.2之前的数据库连接用户名和密码在网络传输时是不进行加密的，为了要和旧版本兼容Oracle数据库9.02存在DBLINK\_ENCRYPT\_LOGIN参数用来调节数据库连接时用户名和密码的加密特性，以下说法正确的是：（ACD）。

A、DBLINK\_ENCRYPT\_LOGIN为TRUE时，数据库连接加密用户名和密码

B、DBLINK\_ENCRYPT\_LOGIN时，数据库连接不加密用户名和密码

C、DBLINK\_ENCRYPT\_LOGIN为FALSE时，如果加密的数据库连接失败，会尝试不加密的连接

D、DBLINK\_ENCRYPT\_LOGIN为TRUE时，加密的数据库连接失败，也不会尝试不加密的连接

708、Oracle实例主要由哪两部分组成：（AC）

A、内存 B、Share pool buffer C、后台进程 D、pmon和smon

709、Oracle中如何设置audit trail审计，正确的说法是：（ABD）

A、在init.ora文件中设置“audit\_trail = true”或者“audit\_trail = db”

B、以SYSDBA身份使用AUDIT ALL ON SYS.AUD$ BY ACCESS，语句对audit trail审计

C、Oracle不支持对audit trail的审计

D、在设置audit trail审计前，要保证已经打开Oracle的审计机制

710、SQL Server的登录认证种类有以下哪些？（ACD）

A、Windows认证模式 B、双因子认证模式

C、混合认证模式 D、SQL Server认证

711、SQL Server的取消权限的操作有以下哪些？（ABC）

A、在“详细信息”窗格中右击要授予/拒绝/取消其权限的用户定义的角色

B、单击“属性”命令在“名称”下单击“权限”单击列出全部对象

C、选择在每个对象上授予拒绝或废除的权限，选中标志表示授予权限，X表示拒绝权限，空框表示废除权限，只列出适用于该对象的权限

D、回到“数据库用户属性”对话框中，再点击“确定”按钮，所有的设置就完成了

712、SQL Server中ALTER DATABASE可以提供以下哪些功能选项？（ABCD）

A、更改数据库名称 B、文件组名称 C、数据文件 D、日志文件的逻辑名称

713、SQL Server中关于实例的描述，请选择正确的答案。（ABD）

A、如果安装选择“默认”的实例名称。这时本SQL Server的名称将和Windows 2000服务器的名称相同

B、SQL Server可以在同一台服务器上安装多个实例

C、SQL Server只能在一台服务器上安装一个实例

D、实例各有一套不为其他实例共享的系统及用户数据库，所以各实例的运行是独立的。

714、SQL Server中使用企业管理器从数据库中删除数据或日志文件的步骤如下，正确的步骤是？（ABCD）

A、展开服务器组，然后展开服务器

B、展开“数据库”文件夹，右击要从中删除数据或日志文件的数据库，然后单击“属性”命令

C、若要删除数据文件，单击“常规”选项卡。若要删除日志文件，单击“事务日志”选项卡

D、在“文件名”列户，单击要删除的文件名旁边的箭头，再点DELETE键，文件名旁出现十字光标，表明将删除此文件

715、参数REMOTE\_LOGIN\_PASSWORDFILE在Oracle数据库实例的初始化参数文件中，此参数控制着密码文件的使用及其状态，以下说法正确的是：（ABCD）

A、NONE：只是Oracle系统不使用密码文件，不允许远程管理数据库

B、EXCLUSIVE：指示只有一个数据库实例可以使用密码文件

C、SHARED：指示可有多个数据库实例可以使用密码文件

D、以上说法都正确

716、关于SQL Server 2000中的SQL账号、角色，下面说法正确的是：（ABC）

A、PUBLIC,guest为缺省的账号 B、guest不能从master数据库清除

C、可以通过删除guest账号的角色，从而消弱guest可能带来的安全隐患

D、SQL Server角色的权限是不可以修改的

717、连接MySQL后选择需要的数据库DB\_NAME？以下哪些方法是对的（AC）

A、连接后用USE DB\_NAME选择数据库

B、连接后用SET DB\_NAME选择数据库

C、用mysql -h host -u user -p DB\_NAME连接数据库

D、用mysql -h host -u user -p -T DB\_NAME连接数据库

718、如果数据库不需要远程访问，可以禁止远程tcp/ip连接，以增强安全性。可选择的有效方法：（AC）

A、用防火墙封堵数据库侦听端口避免远程连接 B、禁止tcp/ip协议的使用

C、在mysqld服务器中参数中添加 --skip-networking启动参数来使mysql

D、在/etc/my.cnf下添加remoteConnnect=disable

719、以下哪些MySQL中GRANT语句的权限指定符？（ABCDEF）

A、ALTER B、CREATE C、DELETE

D、UPLOAD E、DROP F、INSERT

720、用THC组织的Oracle的工具，通过sniffer方式抓取数据库的认证信息可有效破解Oracle密码，以下哪些数据是必须获取的？（ABC）

A、AUTH\_SESSKEY B、AUTH\_PASSWORD C、用户名 D、实例名

721、在Oracle 9数据库可以通过配置$Oracle\_HOME\network\admin\sqlnet.ora文件实现数据库层次的基于TCP协议和地址的访问控制。下面说法正确的是：（ABCD）

A、首先需要配置TCP,VALIDNODE\_CHECKING=yes启用节点检查功能

B、其次配置TCP.INVITED\_NODES=192.168.0.12，192.168.0.33将会允许地址是192.168.0网段的12和33的主机访问

C、然后配置TCP.EXCLUDED\_NONES=192.168.0.123将会禁止地址是192.168.0网段的123的主机访问

D、要以上配置生效必须重启lsnrctl监听器

722、在SQL Server 2000中，如果想查询当前数据库服务器软件的版本，可以使用下面哪些方式（ABCD）

A、在查询分析器中通过如下语句查询SELECT ServerPROPERTY(‘productversion’),ServerPROPERTY(‘productlevel’),ServerPROPERTY(‘edition’)

B、在命令行下，用SQL Server自带的管理工具osql连接进入数据库，输入select@@version

C、企业管理器查看服务器属性 D、在SQL Server服务管理器里面查看“关于”

723、在SQL Server 2000中一些无用的存储过程，这些存储过程极容易被攻击者利用，攻击数据库系统。下面的存储过程哪些可以用来执行执行系统命令或修改注册表？（ABC）

A、xp\_cmdshell B、xp\_regwrite C、xp\_regdeletekey D、select \* from master

724、在SQL Server中创建数据库，如下哪些描述是正确的？（ABCD）

A、创建数据库的权限默认授权sysadmin和dbcreator固定服务器角色的成员，但是它仍可以授予其他用户

B、创建数据库的用户将成为该数据库的所有者

C、在一个服务器上，最多可以创建32,767个数据库

D、数据库名称必须遵循标示符规则

725、在对SQL Server 2000的相关文件、目录进行安全配置时，下面可以采用的措施是：（ABCD）

A、删除缺省安装时的例子样本库

B、将存放数据的库文件，配置权限为administrators组、system和启动SQL Server服务的用户账号及DBA组具有完全控制权限

C、对SQL Server安装目录，去除everyone的所有控制权限

D、将数据库数据相关的文件，保存在非系统盘的NTFS独立分区

726、sybase数据库文件系统需要哪些裸设备？（ABCD）

A、master B、proce C、data D、log

727、Oracle支持哪些加密方式？（ABCD）

A、DES B、RC4\_256 C、RC4\_40 D、DES40

728、SQL Server用事件探测器可以帮助排除故障和解决问题，创建跟踪的步骤如下哪些是正确的？（ABCD）

A、从“模板名称”下拉菜单为你创建跟踪选择一个模板

B、“事件探查器”主界面打开后，从“文件”菜单选择“新跟踪”

C、在“跟踪名称”文本框中输入你想要为这个跟踪创建的跟踪名称

D、修改这些默认的选项设置。通过点击“显示全部事件”和“显示全部列”复选框来查看其他的选项。

729、最重要的电磁场干扰源是：（BCD）

A、电源周波干扰 B、雷电电磁脉冲LEMP

C、电网操作过电压SEMP D、静电放电ESD

730、雷电侵入计算机信息系统的途径主要有：（ABD）

A、信息传输通道线侵入 B、电源馈线侵入 C、建筑物 D、地电位反击

731、电信生产其机房作业，是由专门的值机员、机务员来完成，作业内容是：固定电话、无线电话、电报、载波、短波、微波、卫星和电力等电信通信设备，使设备出去良好状态，保证其正常运行。（ABCD）

A、安装 B、值守 C、维护 D、检修

732、对计算机系统有影响的腐蚀性气体大体有如下几种：（ABCD）

A、二氧化硫 B、氢化硫 C、臭氧 D、一氧化碳

733、防火工作的基本措施有：（ABCD）

A、加强对人员的教育管理 B、加强对可燃物的管理

C、加强对物的管理 D、加强对火源、电源的管理

734、会导致电磁泄漏的有（ABCDE）

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

E、信号处理电

735、火灾自动报警、自动灭火系统部署应注意（ABCD）。

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、具有自动和手动两种触发装置

736、计算机场地安全测试包括（ABCD）。

A、温度，湿度，尘埃 B、照度，噪声，电磁场干扰环境场强

C、接地电阻，电压、频率 D、波形失真率，腐蚀性气体的分析方法

737、计算机信息系统设备处于不同雷电活动地区，其雷电电磁场强度有很大差异，根据这一差异，将被防护空间分为下列哪些防护区？（ABCD）

A、直击雷非防护区（LPZOA） B、直击雷防护区（LPZOB）

C、第一防护区（LPZI） D、后续防护区（LPZ2,3...等）

738、静电的危害有（ABCD）。

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

739、灭火的基本方法有（ABCD）。

A、冷却法 B、隔离法 C、窒息法 D、抑制

740、实体安全技术包括（ABD）。

A、环境安全 B、设备安全 C、人员安全 D、媒体安全

741、使用配有计算机的仪器设备时，不应该做的有：（ABCD）

A、更改登机密码和系统设置

B、自行安装软件

C、玩各种电脑游戏

D、将获得的图像、数据等资料存储在未予指定的硬盘分区上

742、硬件设备的使用管理包括（ABCD）。

A、严格按硬件设备的操作使用规程进行操作

B、建立设备使用情况日志，并登记使用过程

C、建立硬件设备故障情况登记表

D、坚持对设备进行例行维护和保养

743、预防静电的措施有（ABCD）。

A、接地 B、不使用或安装产生静电的设备

C、不在产生静电场所穿脱工作服 D、作业人员穿防静电鞋

744、在实验室中引起火灾的通常原因包括：（ABCD）

A、明火 B、电器保养不良

C、仪器设备在不使用时未关闭电源 D、使用易燃物品时粗心大意

745、直击雷：直接击在（ABCD）并产生电效应、热效应和机械力的雷电放电。

A、建筑物 B、构建物 C、地面突进物 D、大地或设备

746、员工区域安全守则包括：（ABCD）

A、非工作时间，员工进入或离开办公区域，应在值班人员处登记

B、外来人员进入办公区域或机房，相关员工必须全程陪同

C、将物品带入/带出公司，要遵守公司相关的规定及流程

D、参加会议时遵守会前、会中、会后的保密流程

747、机房出入控制措施包括：（ABCD）

A、机房接待前台须核查弄清业务系统安全区域的来访者的身份，并记录其进入和离开安全区域的日期与时间

B、机房须告知进入安全区的来访者，该区域的安全要求和紧急情况下的行动步骤

C、可采用强制性控制措施，对来访者的访问行为进行授权和验证

D、要求所有进出机房人员佩带易于辨识的标识

748、为了减小雷电损失，可以采取的措施有（ACD）

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

749、安全要求可以分解为（ABCDE）。

A、可控性 B、保密性 C、可用性 D、完整性 E、不可否认性

750、HASH加密使用复杂的数字算法来实现有效的加密，其算法包括（ABC）

A、MD2 B、MD4 C、MD5 D、Cost256

751、利用密码技术，可以实现网络安全所要求的。（ABCD）

A、数据保密性 B、数据完整性 C、数据可用性 D、身份验证

752、一个密码体系一般分为以下哪几个部分？（ABCD）

A、明文 B、加密密钥和解密密钥

C、密文 D、加密算法和解密算法

753、公钥密码体质的应用主要在于。（AC）

A、数字签名 B、加密 C、密钥管理 D、哈希函数

754、目前基于对称密钥体制的算法主要有。（BC）

A、RSA B、DES C、AES D、DSA

755、使用esp协议时，可以使用的加密运算是。（ABC）

A、DES B、3DES C、AES D、RSA

756、数字签名的作用是。（ACD）

A、确定一个人的身份 B、保密性

C、肯定是该人自己的签字 D、使该人与文件内容发生关系

757、以下属于对称加密算法的是：（ABD）

A、DES B、3DES C、SHA-1 D、RC4 E、MD5

758、在加密过程中，必须用到的三个主要元素是（ABC）

A、所传输的信息（明文） B、加密 钥匙（Encryption Key）

C、加密函数 D、传输信道

759、账号口令管理办法适用于所有和DSMP系统、智能网系统、彩铃平台相关的（ACD）

A、系统管理员 B、操作系统

C、操作维护人员 D、所有上述系统中存在的账号和口令

760、为保证密码安全，我们应采取的正确措施有（ABC）

A、不使用生日做密码 B、不使用少于5为的密码

C、不适应纯数字密码 D、将密码设的非常复杂并保证20位以上

761、公司在使用数据签名技术时，除充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名外，还应注意（ABCD）

A、采取保护公钥完整性的安全措施，例如使用公约证书

B、确定签名算法的类型、属性以及所用密钥长度

C、用于数字签名的密钥应不同于用来加密内容的密钥

D、符合有关数字签名的法律法规，必要时，应在合同或协议中规定使用数字签名的相 关事宜

762、相对于对称加密算法，非对称密钥加密算法（ACD）

A、加密数据的速率较低

B、更适合于现有网络中对所传输数据（明文）的加解密处理

C、安全性更好 D、加密和解密的密钥不同

763、一个典型的PKI应用系统包括（ABCD）实体

A、认证机构CA B、册机构RA C、证书及CRL目录库 D、用户端软件

764、加密的强度主要取决于（ABD）

A、算法的强度 B、密钥的保密性 C、明文的长度 D、密钥的强度

765、一下对于对称密钥加密说法正确的是（BCD）

A、对称加密算法的密钥易于管理 B、加解密双方使用同样的密钥

C、DES算法属于对称加密算法 D、相对于非对称加密算法，加解密处理速度比较快

766、在通信过程中，只采用数字签名可以解决（ABC）等问题

A、数据完整性 B、数据的抵抗赖性 C、数据的篡改 D、数据的保密性

767、对称密钥算法体系包括：（ABCDE）

A、明文(plaintext)：原始消息或数据，作为算法的输入

B、加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换

C、秘密密钥(secret key)：秘密密钥也是算法输入，算法进行的具体替换和转换取决于 这个密钥

D、密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对 于一个给定的消息，两个不同的密钥会产生两个不同的密文

、.解密算法(decryption algorithm)：本质上是加密算法的执行。它使用密文和统一密钥 产生原始明文

768、一下对于混合加密方式说法正确的是。（BCD）

A、 使用公开密钥密码体制对要传输的信息（明文）进行加解密处理

B、使用对称加密算法对要传输的信息（明文）进行加解密处理

C、使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信

D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的

769、电信的网页防篡改技术有（ABC）

A、外挂轮询技术 B、核心内嵌技术

C、时间触发技术 D、安装防病毒软件

770、病毒发展的趋势是？（ABC）

A、 范围更广 B、度更快 C、方式更多

771、病毒自启动方式一般有（ABC）

A、 修改注册表 B、将自身添加为服务

C、将自身添加到启动文件夹 D、修改系统配置文件

772、常见Web攻击方法有一下哪种？（ABCD）

A、SQL Injection B、Cookie欺骗 C、跨站脚本攻击

D、信息泄露漏洞 E、文件腹泻脚本存在的安全隐患

F、 GOOGLE HACKING

773、宏病毒感染一下哪些类型的文件？（ABCDEF）

A、DOC B、EXE C、XLS D、DOT

774、木马传播包括一下哪些途径：（ACD）

A、通过电子邮件的附件传播 B、通过下载文件传播

C、通过网页传播 D、通过聊天工具传播

775、目前最好的防病毒软件能做到的是（ABCD）

A、检查计算机是否感染病毒，消除已感染的任何病毒

B、杜绝病毒对计算的侵害

C、查出计算机已感染的已知病毒，消除其中的一部分

D、检查计算机是否染有已知病毒，并作相应处理

776、通用的DoS攻击手段有哪些？（CD）

A、 SYN Attack B、ICMP Flood C、UDP Flood

D、Ping of Death E、Tear Drop F、Ip Spoofing

777、以下关于蠕虫的描述正确的有：（ABCDEF）

A、 蠕虫具有自动利用网络传播的特点，在传播的同时，造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪

B、 隐藏式蠕虫的基本特征，通过在主机上隐藏，使得用户不容易发现它的存在

C、蠕虫需要传播受感染的宿主文件来进行复制

D、蠕虫的传染能力主要是针对计算机内的文件系统。

778、以下哪几种扫描检测技术属于被动式的检测技术？（AB）

A、 基于应用的检测技术 B、基于主动的检测技术

C、基于目标的漏洞检测技术 D、基于网络的检测技术

779、以下是检查磁盘与文件是否被病毒感染的有效方法：（BC）

A、 检查磁盘目录中是否有病毒文件 B、用抗病毒软件检查磁盘的各个文件

C、用放大镜检查磁盘编码是否有霉变现象 D、检查文件的长度是否无故变化

780、造成计算机不安全的因素有（BD）等多种。

A、 技术原因 B、自然原因 C、认为原因 D、管理原因

781、嗅探技术有哪些特点？（ABCD）

A、间接性 B、.直接性 C、隐蔽性 D、开放性

782、一个恶意的攻击者必须具备哪几点？（ABC）

A、 方法 B、机会 C、动机 D、运气

783、对于DOS网络攻击，可以采用以下哪些措施来缓解主机系统被攻击进程。（ACD）

A、缩短SYN Timeout时间和设置SYN Cookie B、增加网络带宽

C、在系统之前增加负载均衡设备 D、在防火墙上设置ACL或黑客路由

784、利用Bind/DNS漏洞攻击的分类主要有（ACD）

A、 拒绝服务 B、匿名登录 C、.缓冲区溢出

D、DNS缓存中毒 E、病毒或后门攻击

785、常见Web攻击方法有一下哪种？（ABCD）

A、 SQL Injection B、 Cookie欺骗 C、 跨站脚本攻击 D、信息泄露漏洞

786、黑客所使用的入侵技术主要包括（ABCDE）

A、协议漏洞渗透 B、密码分析还原 C、应用漏洞分析与渗透

D、拒绝服务攻击 E、病毒或后门攻击

787、主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有（ABC）

A、针对入侵者采取措施 B、修正系统

C、收集更详细的信息 D、入侵追踪

788、下面哪些漏洞属于网络服务类安全漏洞：（BC）

A、Windows 2000中文版输入法漏洞 B、IS Web服务存在的IDQ远程溢出漏洞

C、RPC DCOM服务漏洞 D、Web服务asp脚本漏洞

789、系统感染病毒后的现象有哪些？（ABCD）

A、系统错误或系统崩溃 B、系统反应慢，网络拥塞

C、陌生的进程或服务 D、陌生的自启动

**三、判断题：（790-1000）**

790、TCSEC将信息安全风机防护等级一共分为7个安全等级：D、C1、C2、B1、B2、B3、 A。(A)

A、正确 B、错误

791、通用标准v2版（CC）的安全等级是以EAL来表示的。（A）

A、正确 B、错误

792、一个企业的信息安全组织能否顺利开展工作（定期安全评估、日志安全巡检、定期安全审核、应急演练等），主要取决于公司领导对信息安全工作的认识程度和支持力度。（A）

A、正确 B、错误

793、在信息安全领域，CIA通常是指：保密性、完整性和可用性。（A）

A、正确 B、错误

794、信息安全是永远是相对的，并且需要不断持续关注和改进，永远没有一劳永逸的安全

防护措施。（A）

A、正确 B、错误

795、在信息安全领域，CIA通常是指：保密性、完整性和非抵赖性。（B）

A、正确 B、错误

796、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

797、信息安全的威胁主体包括内部人员、准内部人员、外部人员、系统自身等方面。（B）

A、正确 B、错误误

798、互联网网络安全事件根据危害和紧急程度分为一般、预警、报警、紧急、重大五种。 （B）

A、正确 B、错误

799、安全审计是从管理和技术两个方面检查公司的安全策略和控制措施的执行情况，发现安全隐患的过程。（A）

A、正确 B、错误

800、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

801、计算机系统安全是指应用系统具备访问控制机制，数据不被泄露、丢失、篡改等。（B）

A、正确 B、错误

802、主机加固完成后，一般可以有效保证主机的安全性增强。（A）

A、正确 B、错误

803、黑客在进行信息收集时，通常利用Windows的IPC漏洞可以获得系统用户的列表的信 息。（A）

A、正确 B、错误

804、Solaris系统中一般需要确认ROOT账号只能本地登录，这样有助于安全增强。（A）

A、正确 B、错误

805、HP-UX系统加固中在设置ROOT环境变量不能有相对路径设置。（A）

A、正确 B、错误

806、屏幕保护的木马是需要分大小写。（B）

A、正确 B、错误

807、安全审计就是日志的记录。（B）

A、正确 B、错误误

808、HP-UX系统加固中在设置通用用户环境变量不能有相对路径设置。（A）

A、正确 B、错误

809、AIX系统加固时，对系统配置一般需要自编脚本完成。（A）

A、正确 B、错误

810、Windows NT中用户登录域的口令是以明文方式传输的。（B）

A、正确 B、错误

811、操作系统普通用户账号审批记录应编号、留档。（A）

A、正确 B、错误

812、计算机病毒是计算机系统中自动产生的。（B）

A、正确 B、错误

813、主机系统加固时根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。（A）

A、正确 B、错误

814、4A系统的建设能够减轻账户管理员的维护工作。（A）

A、正确 B、错误

815、4A系统的接入管理可以管理到用户无力访问的接入。（B）

A、正确 B、错误

816、Cisco路由器可以使用enable password命令为特权模式的进入设置强壮的密码。（B）

A、正确 B、错误

817、Cisco设备的AUX端口默认是启用的。（A）

A、正确 B、错误

818、DHCP可以向终端提供IP地址、网关、DNS服务器地址等参数。（A）

A、正确 B、错误误

819、Inbound方向的NAT使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际IP地址。（B）

A、正确 B、错误

820、IPS设备即使不出现故障，它仍然是一个潜在的网络瓶颈，需要强大的网络结构来配合。（A）

A、正确 B、错误

821、IPS的过滤器规则不能自由定义。（B）

A、正确 B、错误

822、IPS的某些功能和防火墙类似。（A）

A、正确 B、错误

823、IPS和IDS都是主动防御系统。（B）

A、正确 B、错误

824、NAT是一种网络地址翻译的技术，它能是的多台没有合法地址的计算机共享一个合法的IP地址访问Internet。（A）

A、正确 B、错误

825、Netscreen的ROOT管理员具有的最高权限，为了避免ROOT管理员密码被窃取后造成威胁，应该限制ROOT只能通过CONSOLE接口访问设备，而不能远程登录。(A)

A、正确 B、错误

826、Netscreen防火墙的外网口应禁止PING测试，内网口可以不限制。（B）

A、正确 B、错误

827、OSI是开放的信息安全的缩写。（B）

A、正确 B、错误

828、OSI七层模型中，传输层数据成为段（Segment），主要是用来建立主机端到端连接，包括TCP和UDP连接。（A）

A、正确 B、错误

829、OSI中会话层不提供机密性服务。（A）

A、正确 B、错误

830、SSH使用TCP 79端口的服务。（B）

A、正确 B、错误

831、TCP/IP模型从下至上分为四层：物理层，数据链路层，网络层和应用层。（B）

A、正确 B、错误

832、TCP/IP模型与OSI参考模型的不同点在于TCP/IP把表示层和会话层都归于应用层，所以TCP/IP模型从下至上分为五层：物理层，数据链路层，网络层，传输层和应用层。 （A）

A、正确 B、错误

833、TCP/IP协议体系结构中，IP层对应OSI/RM模型的网络层。（A）

A、正确 B、错误

834、默认情况下需要关闭Cisco设备的Small TCP/UDP服务。（A）

A、正确 B、错误

835、缺省情况下，防火墙工作模式为路由模式，切换工作模式后可直接进行进一步配置。（B）

A、正确 B、错误

836、入侵检测具有对操作系统的校验管理，判断是否有破坏安全的用户活动。（A）

A、正确 B、错误

837、入侵检测可以处理数据包级的攻击。（B）

A、正确 B、错误

838、入侵检测系统不能弥补由于系统提供信息的质量或完整性的问题。（A）

A、正确 B、错误

839、入侵检测系统能够检测到用户的对主机、数据库的网络操作行为。（B）

A、正确 B、错误

840、入侵检测系统是一种对计算机系统或网络事件进行检测并分析这个入侵事件特征的过程。（A）

A、正确 B、错误

841、统计分析的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。（B）

A、正确 B、错误

842、统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。（A）

A、正确 B、错误

843、透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决IP地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的IP的地址。（A）

A、正确 B、错误

844、完整性分析的缺点是一般以批处理方式实现，不用于实时响应。（A）

A、正确 B、错误

845、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（B）

A、正确 B、错误

846、网络边界的Cisco路由器应关闭CDP服务。（A）

A、正确 B、错误

847、网络边界Cisco设备的CDP协议可以开放。（B）

A、正确 B、错误

848、网络层的防护手段（防火墙，SSL，IDS，加固）可以组织或检测到应用层攻击。（B）

A、正确 B、错误

849、针对不同的攻击行为，IPS只需要一个过滤器就足够了。（B）

A、正确 B、错误

850、主机型IDS其数据采集部分当然位于其所检测的网络上。（B）

A、正确 B、错误

851、状态检测防火墙检测每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。（B）

A、正确 B、错误

852、IPS虽然能主动防御，但是不能坚挺网络流量。（B）

A、正确 B、错误

853、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。（B）

A、正确 B、错误

854、审计系统进行关联分析时不需要关注日志时间。（B）

A、正确 B、错误

855、垃圾邮件一般包括商业广告、政治邮件、病毒邮件、而已欺诈邮件（网络钓鱼）等几个方面。（A）

A、正确 B、错误

856、防止网络窃听最好的方法就是给网上的信息加密，是的侦听程序无法识别这些信息模式。（A）

A、正确 B、错误

857、侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。（A）

A、正确 B、错误

858、模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。（A）

A、正确 B、错误

859、入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。（A）

A、正确 B、错误

860、VPN的主要特点是通过加密是信息安全的通过Internet传递。（A）

A、正确 B、错误

861、传输层协议使用端口号（Port）来标示和区分上层应用程序，如：Telnet协议用的是23号端口、DNS协议使用69号端口。（B）

A、正确 B、错误

862、如果Web应用对URL访问控制不当，可能造成用户直接在浏览器中输入URL，访问不该访问的页面。（A）

A、正确 B、错误

863、如果Web应用没有对攻击者的输入进行适当的编码和过滤，就用于构造数据库查询或操作系统命令时，可能导致注入漏洞。（A）

A、正确 B、错误

864、HTTP协议定义了Web浏览器向Web服务器发生Web页面请求的格式及Web页面在Internet上传输的方式。（A）

A、正确 B、错误

865、HTTP协议是文本协议，可利用回车换行做边界干扰。（A）

A、正确 B、错误

866、Init<sid>.ora文件是Oracle启动文件，任何参数的配置错误都会造成Oracle不能启动，任何参数的不合理配置都可能造成系统故障。（A）

A、正确 B、错误

867、Mysqldump是采用SQL级别的备份机制，它将数据表导成SQL脚本文件，在不同的MySQL版本之间升级时相对比较合适，这也是最常见的备份方法。（A）

A、正确 B、错误

868、Orabrute是进行远程破解Oracle密码的工具，要猜解的密码可以在password.txt中设置。（A）

A、正确 B、错误

869、Oracle的SYS账户在数据库中具有最高权限，能够做任何事情，包括启动/关闭Oracle数据库。即使SYS被锁定，也已然能够访问数据库。（A）

A、正确 B、错误

870、Oracle的若算法加密机制：两个相同的用户名和密码在两个不同的Oracle数据库机器中，将具有相同的哈希值。（A）

A、正确 B、错误

871、Oracle密码允许包含像“SELECT”，“DELETE”，“CREATE”这类的Oracle/SQL关键字。（B）

A、正确 B、错误

872、Oracle的HTTP的基本验证可选择SYS破解，因为它始终存在和有效。（A）

A、正确 B、错误

873、Oracle默认情况下，口令的传输方式是加密。（B）

A、正确 B、错误

874、Oracle数据库的归档日志不是在线日志的备份。（B）

A、正确 B、错误

875、OSI网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。（A）

A、正确 B、错误

876、OSI网络安全体系结构的五类安全服务是鉴别、访问控制、保密性、完整性、抗否认。（A）

A、正确 B、错误

877、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因。（A）

A、正确 B、错误

878、SQL Server如果设置了不恰当的数据库文件权限，可能导致敏感文件被非法删除或读取，威胁系统安全。（A）

A、正确 B、错误

879、SQL Server数据库应禁止使用除tcp/ip以外的协议，保护数据库通信安全。（A）

A、正确 B、错误

880、SQL Server应该社会自日志审核无法追踪回溯安全事件。（A）

A、正确 B、错误

881、Web服务器一般省缺不允许攻击者访问Web根目录以外的内容，内容资源不可以任意访问。(A)

882、Web攻击面不仅仅是浏览器中可见的内容。（A）

A、正确 B、错误

883、Web应用对网络通讯中包含的敏感信息进行加密，就不会被窃听。（B）

A、正确 B、错误

884、暴力猜解不能对Web应用进行攻击。（B）

A、正确 B、错误

885、在Oracle自身的配置上做限定方法是：修改$Oracle\_HOME\network\admin目录下面的SQLNET..ORA文件，类似设置如下：

Tcp\_validnode\_checking=YES

Tcp\_invited\_nodes=

(192.168.0.1,ip2,ip3•••...)。

( A )

A、正确 B、错误

886、不设置必要的日志审核，就无法追踪回溯安全事件，Oracle中若果要审计记录成功的登陆语句”SQL>audit session whenever successful;”. ( A )

A、正确 B、错误

887、对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是DNS服务器。（B）

A、正确 B、错误

888、防止XSS各种方法都有优劣之处，防范XSS的真正挑战不在于全免，而在于细致。（B）

A、正确 B、错误

889、访问控制、强制登陆、自动安全更新都属于Window2000的安全组件（B）

A、正确 B、错误

890、复杂的系统存在大量的相互引用访问，如果开发者不能有效的进行权限控制，就可能被恶意引用。（A）

A、正确 B、错误

891、攻击者可以通过SQL注入手段获取其他用户的密码。（A）

A、正确 B、错误

892、几乎所有的关系数据库系统和相应的SQL语言都面临SQL注入的潜在威胁。（A)

A、正确 B、错误

893、简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架（B）

A、正确 B、错误

894、默认可通过Web程序来远程管理Oracle10g数据库，端口是8080.（A）

A、正确 B、错误

895、如果sa是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。（A）

A、正确 B、错误

896、如果在SQL Server等领域成功并不意味这该用户已经可以访问SQL Server上的数据库。（A）

A、正确 B、错误

897、如果知道Oracle密码长度，用Rainbow表生成器来破解其密码哈希值是绝对成功的。（A）

A、正确 B、错误

898、所有操作系统、数据库、网络设备，包括一部分业务系统，均需要支持基于账号的访问控制功能。（B）

A、正确 B、错误

899、网络拓扑分析为检查是否有配置错误项泄露内部IP地址，从而推断网站系统拓扑。（A）

A、正确 B、错误

900、为Oracle数据库安全考虑，在对人共同对数据库进行维护时应依赖数据库预定义的传统角色。（B）

A、正确 B、错误

901、为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。(A)

A、正确 B、错误

902、系统类型鉴别为检查主机系统与开放服务是否存在安全漏点。（B）

A、正确 B、错误

903、系统漏洞扫描为检查目标的操作系统与应用系统信息。（B）

A、正确 B、错误

904、选择远程破解Oracle的最好账户是SYS，因为此账户永远有效。（A）

A、正确 B、错误

905、一封电子邮件可以拆分成对个IP包，每个IP包可以沿不同的路径到达目的地。（A）

A、正确 B、错误

906、一个共享文件夹。将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有读取的权限。（A）

A、正确 B、错误

907、用Sqlplus登陆到Oracle数据库，使用slesct username, password form dba\_users命令可查看数据库中的用户名和密码明文。（B）

A、正确 B、错误

908、有的Web应用登陆界面允许攻击者暴力猜解口令，在自动工具与字典表的帮助下，可以迅速找到弱密码用户。（A）

A、正确 B、错误

909、在Oracle所有版本在安装的时候都没有提示修改SYS的默认密码。（B）

A、正确 B、错误

910、在ORacle数据库安装补丁时，不需要关闭所有与数据库有关的服务。（B）

A、正确 B、错误

911、在SQL Server安装SP3补丁时不需要系统中已经安装了SP1或SP2。（B）

A、正确 B、错误

912、在SQL Server中具有sysadmin权限的用户可以通过xp\_cmdshell存储扩展以system的权限执行任意系统命令。（A）

A、正确 B、错误

913、Oracle默认配置下，每个账户如果有30次的失败登陆，此账户将被锁定。（B）

A、正确 B、错误

914、定制开发Web系统的安全度不如标准的产品。（A）

A、正确 B、错误

915、对MySQL注入攻击时，经常用到注释符号#来屏蔽剩下的内置SQL语句。（A）

A、正确 B、错误

916、一个登录名只能进入服务器，但是不能让用户访问服务器中的数据库资源。每个登录名的定义存放在msater数据库的syslogins表中。（A）

A、正确 B、错误

917、Web错误信息可能泄露服务器型号版本、数据库型号、路径、代码。（A）

A、正确 B、错误

918、Oracle的密码哈希值存储在SYS.USER$表中。可以通过像DBA USERS这类的视图来访问。（A）

A、正确 B、错误

919、产品的定制开发是应用安全中最薄弱的一环。（A）

A、正确 B、错误

920、Oracle限制了密码由英文字母，数字，#，下划线（\_），美元字符（$）构成，密码的最大长度为30字符；并不能以”$”,”#”,”\_”或任何数字开头。（A）

A、正确 B、错误

921、网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。（B）

A、正确 B、错误

922、计算机场地可以选择在公共区域人流量比较大的地方。（B）

A、正确 B、错误

923、EMC测试盒约束用户关心的信息信号的电磁发射、TEMPEST只测试盒约束系统和设备的所有电磁发射。（B）

A、正确 B、错误

924、加密传输是一种非常有效并经常使用的方法，也能解决输入和输出端的电磁信息泄露问题。（B）

A、正确 B、错误

925、出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。（B）

A、正确 B、错误

926、红区：红新号的传输通道或单元电路称为红区，反之为黑区。（A）

A、正确 B、错误

927、机房应设置相应的活在报警和灭火系统。（A）

A、正确 B、错误

928、计算机机房的建设应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。（A）

A、正确 B、错误

929、计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。（B）

A、正确 B、错误

930、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。（A）

A、正确 B、错误

931、提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。（A）

A、正确 B、错误

932、在计算机机房附近施工，不负有维护计算机信息系统安全的责任和义务。（B）

A、正确 B、错误

933、只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。（B）

A、正确 B、错误

934、主管计算机信息系统安全的公安机关和城建及规划部门，应与设施单位进行协调，在不危害用户利益的大前提下，制定措施。合理施工，做好计算机信息系统安全保护工作。（B）

A、正确 B、错误

935、防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。（A）

A、正确 B、错误

936、对于公司机密信息必须根据公司的相关规定予以适当的标识。（A）

A、正确 B、错误

937、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。（A）

A、正确 B、错误

938、如果在电话、电视会议中涉及讨论工伤机密信息，会议主持人或组织人在会议全过程中一定要确认每一个与会者是经授权参与的。（A）

A、正确 B、错误

939、为防止信息非法泄露，需要销毁存储介质时，应该批准后自行销毁。（B）

A、正确 B、错误

940、将公司的机密信息通过互联网络传送时，必须予以加密。（A）

A、正确 B、错误

941、机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。（A）

A、正确 B、错误

942、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式进行保密。（A）

A、正确 B、错误

943、“一次一密”属于序列密码的一种。（A）

A、正确 B、错误

944、3DES算法的加密过程就是用一个秘钥对待加密的数据执行三次DES算法的加密操作。（B）

A、正确 B、错误

945、AES加密算法的秘钥长度为128、192或256位。（A）

A、正确 B、错误

946、AES是一种非对称算法。（B）

A、正确 B、错误

947、DES3和RSA是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。（A）

A、正确 B、错误

948、Diffie-Hellman算法的安全性取决于离散对数计算的困难性，可以实现秘钥交换。（A）

A、正确 B、错误

949、DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。（A）

A、正确 B、错误

950、MD5是一种加密算法。（B）

A、正确 B、错误

951、PGP协议缺省的压缩算法是ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。（A）

A、正确 B、错误

952、PKI是一个用对称密码算法和技术来实现并提供安全服务的具有通用性的安全基础设施。（B）

A、正确 B、错误

953、RC4是典型的的序列密码算法。（A）

A、正确 B、错误

954、RSA算法作为主要的非对称算法，使用公钥加密的秘闻一定要采用公钥来街。（B）

A、正确 B、错误

955、安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。（A）

A、正确 B、错误

956、常见的公钥密码算法有RSA算法、Diffie-Hellman算法和EIGamal算法。（A）

A、正确 B、错误

957、当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（A）

A、正确 B、错误

958、发送方使用AH协议处理数据包，需要对整个IP的数据包计算MAC，包括IP头的所有字段和数据。（B）

A、正确 B、错误

959、分组密码的优点是错误扩展小、速度快、安全程度高。（B）

A、正确 B、错误

960、公共迷药密码体制在秘钥管理上比对称秘钥密码体制更安全。（A）

A、正确 B、错误

961、古典加密主要采用的主要方法是置换，代换。（A）

A、正确 B、错误

962、古典加密主要是对加密算法的保密，现代加密算法是公开的，主要是针对秘钥进行保密。（A）

A、正确 B、错误

963、基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。（A）

A、正确 B、错误

964、口令应在120天至少更换一次。（B）

A、正确 B、错误

965、链路加密方式适用于在广域网系统中应用。（B）

A、正确 B、错误

966、密码保管不善属于操作失误的安全隐患。（B）

A、正确 B、错误

967、日常所见的校园饭卡是利用身份认证的单因素法。（A）

A、正确 B、错误

968、身份认证要求对数据和信息来源进行验证，以确保发信人的身份。（B）

A、正确 B、错误

969、身份认证与权限控制是网络社会的管理基础。（A）

A、正确 B、错误

970、数据在传输过程中用哈希算法保证其完整性后，非法用户无法无法对数据进行任何修改。（B）

A、正确 B、错误

971、数字签名比较的是摘要结果长度是否都是128位。（B）

A、正确 B、错误

972、通信数据与文件加密是同一个概念。（B）

A、正确 B、错误

973、为AES开发的Rijndae1算法的秘钥长度是128位，分组长度也为128位。（B）

A、正确 B、错误

974、为了保证安全性，密码算法应该进行保密。（B）

A、正确 B、错误

975、文件压缩变换是一个单向加密过程。（B）

A、正确 B、错误

976、我的公钥证书不能在网络上公开，否则其他人可能冒充我的身份或伪造我的数字签名。（B）

A、正确 B、错误

977、现代加密算法可以分为对称加密算法和非对称加密。（A）

A、正确 B、错误

978、虚拟专用网VPN的关键技术主要是隧道技术、加解密技术、秘钥管理技术以及使用者与设备身份认证技术。（A）

A、正确 B、错误

979、以当前的技术来说，RSA体制是无条件安全的。（B）

A、正确 B、错误

980、在4A系统的远期建设中，应用系统自身不需要保留系统从账户信息。（B）

A、正确 B、错误

981、在MD5算法中，要先将以初始化的A、B、C、D这四个变量分别复制到a、b、c、d中。（A）

A、正确 B、错误

982、在MD5算法中要用到4个变量，分别表示A、B、C、D，均为32位长。（A）

A、正确 B、错误

983、在PKI中，注册机构RA是必要的组件。（B）

A、正确 B、错误

984、在SSL握手协议过程中，需要服务器发送自己的证书。（A）

A、正确 B、错误

985、在非对称加密过程中，加密和解密使用的是不同的秘钥。（A）

A、正确 B、错误

986、在公钥加密系统中，用公钥加密的密文可以由私钥解密，但用公钥加密的密文，不能用公钥解密。 （B）

A、正确 B、错误

987、在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一种“破解”。 （A）

A、正确 B、错误

988、账户管理的Agent不适用于在网络设备中部署。 （A）

A、正确 B、错误

989、整个PKI系统有证书服务器AS、票据许可服务器TGS、客户机和应用服务器四部分组成。 （B）

A、正确 B、错误

990、最基本的认证方式选择证书是数字证书。（B）

A、正确 B、错误

991、最小特权、纵深防御是网络安全原则之一。（A）

A、正确 B、错误

992、数字证书是由权威机构CA发行的一种权威的电子文档，是网络环境中的一种身份证。（A）

A、正确 B、错误

993、数字证书是由权威机构PKI发行的一种权威性的电子文档，是网络环境中的一种身份证。 （B）

A、正确 B、错误

994、信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段。（A）

A、正确 B、错误

995、病毒能隐藏在电脑的CMOS存储器里。（B）

A、正确 B、错误

996、对感染病毒的软盘进行浏览会导致硬盘被感染。（B）

A、正确 B、错误

997、已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（B）

A、正确 B、错误

998、重新格式化硬盘可以清楚所有病毒。（B）

A、正确 B、错误

999、专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，并根据评估结果提供评估报告。 （A）

A、正确 B、错误

1000、冒充信件回复、假装纯文字ICON、冒充微软雅虎发信、下载电子贺卡同意书、是使用的叫做字典攻击法的方法。（B）

A、正确 B、错误

一、填空题。（每空1分，共15分）

1、保证计算机网络的安全，就是要保护网络信息在存储和传输过程中的可用性、机密性、完整性、可控性和不可抵赖性。

2、信息安全的大致内容包括三部分：物理安全、网络安全和操作系统安全。

3、网络攻击的步骤是：隐藏IP、信息收集、控制或破坏目标系统、种植后门和在网络中隐身。

4、防火墙一般部署在内部网络和外部网络之间。

5、入侵检测系统一般由数据收集器、检测器、知识库和控制器构成。

二、单项选择题。（每题2分，共30分）

1、网络攻击的发展趋势是（B）。

A、黑客技术与网络病毒日益融合 B、攻击工具日益先进

C、病毒攻击 D、黑客攻击

2、拒绝服务攻击（A）。

A、用超出被攻击目标处理能力的海量数据包消耗可用系统、带宽资源等方法的攻击

B、全称是Distributed Denial Of Service

C、拒绝来自一个服务器所发送回应请求的指令

D、入侵控制一个服务器后远程关机

3、HTTP默认端口号为（B）。

A、21 B、80 C、8080 D、23

4、网络监听是（B）。

A、远程观察一个用户的计算机 B、监视网络的状态、传输的数据流

C、监视PC系统的运行情况 D、监视一个网站的发展方向

5、下面不是采用对称加密算法的是（D）。

A、DES B、AES C、IDEA D、RSA

6、在公开密钥体制中，加密密钥即（D）。

A、解密密钥 B、私密密钥 C、私有密钥 D、公开密钥

7、DES算法的入口参数有3个：Key、Data和Mode。其中Key的实际长度为（D）位，是DES算法的工作密钥。

A、64      B、7     C、8           D、56

8、计算机网络的安全是指（B）。

A、网络中设备设置环境的安全       B、网络中信息的安全

C、网络中使用者的安全               D、网络中财产的安全

9、打电话请求密码属于（B）攻击方式。

A、木马   B、社会工程学    C、电话系统漏洞    D、拒绝服务

10、安全套接层协议是（B）。

A、SET B、SSL C、HTTP D、S-HTTP

11、（B）是网络通信中标志通信各方身份信息的一系列数据，提供一种在Internet上验证身份的方式。

A、数字认证 B、数字证书 C、电子证书 D、电子认证

12、数字签名功能不包括（B）。

A．防止发送方的抵赖行为 B．接收方身份确认

C．发送方身份确认 D．保证数据的完整性

13、目前无线局域网主要以（B）作传输媒介。

A．短波　　 B．微波　　 C．激光　　 D．红外线

14、防火墙能够（A）。

A．防范通过它的恶意连接 B．防范恶意的知情者

C．防备新的网络安全问题 Ｄ．完全防止传送己被病毒感染的软件和文件

15、Windows Server 2003系统的安全日志通过（C）设置。

A、事件查看器 B、服务器管理 C、本地安全策略 D、网络适配器

三、多项选择题。（每题2分，共10分，错选或漏选不得分）

1、以下属于木马入侵的常见方法的是（ABCD）。

A、捆绑欺骗 B、邮件冒名欺骗 C、危险下载 D、打开邮件的附件

2、网络防火墙的作用是（ACD）。

A、防止内部信息外池B、防止系统感染病毒与非法访问

C、防止黑客访问D、建立内部信息和功能与外部信息和功能之间的屏障

3、计算机病毒的传播方式有（ABCD）。

A、通过共享资源传播 B、通过网页恶意脚本传播

C、通过网络文件传输传播 D、通过电子邮件传播

4、在保证密码安全中，应该采取的正确措施有（ABC）。

A、不用生日做密码 B、不要使用少于5位的密码

C、不要使用纯数字 D、将密码设得非常复杂并保证在20位以上

5、Windows Server 2003服务器的安全采取的安全措施包括（ABCD）。

A、使用NTFS格式的磁盘分区

B、及时对操作系统使用补丁程序堵塞安全漏洞

C、实行强有力的安全管理策略

D、借助防火墙对服务器提供保护

四、判断题。（每题1分，共10分，对的打“√”，错的打“×”）

1、常见的公钥密码算法有RSA算法、Diffie-Hellman算法和ElGamal算法。（√）

2、拒绝服务攻击属于被动攻击的一种。（×）

3、可以在局域网的网关处安装一个病毒防火墙，从而解决整个局域网的防病毒问题 。（×）

4、非军事化区DMZ是为了解决安全防火墙后外部网路不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。（√）

5、3DES算法的加密过程就是用同一个密钥对待加密的数据执行三次DES算法的加密操作。（×）

6、安全是永远是相对的，永远没有一劳永逸的安全防护措施。（√）

7、入侵检测系统是网络信息系统安全的第一道防线。（×）

8、我的公钥证书是不能在网络上公开的，否则其他人可能假冒我的身份或伪造我的数字签名。（×）

9、日常所见的校园饭卡是利用的身份认证的单因素法。（√）

10、公开密钥密码体制比对称密钥密码体制更为安全。（×）

五、简答题。（每题5分，共15分）

1、简述物理安全包括那些内容？

答：物理安全包括防盗、防火、防静电、防雷击和防电磁泄漏等方面的内容。

2、简述防火墙有哪些基本功能？（写出五个功能）

答：包过滤、远程管理、NAT技术、代理、MAC与IP地址的绑定、流量控制和统计分析、流量计费、VPN、限制同时上网人数、限制使用时间、限制特定使用者才能发送E-mail，限制FTP只能下载文件不能上传文件、阻塞Java、ActiveX控件等。

3、简述无线局域网由那些硬件组成？

答；无线局域网由无线网卡、AP、无线网桥、计算机和有关设备组成。

**《计算机网络安全》试卷及答案一**

1. **填空题（10分）**

1.MD-4散列算法中输入消息可以任意长度，但要进行分组，其分组的位数是( 512   )

2.SHA的含义是( 安全散列算法  )

3.对身份证明系统的要求之一是( 验证者正确识别示证者的概率极大化 )

4.阻止非法用户进入系统使用( 接入控制技术 )

5.以下不是数据库加密方法的是( 信息隐藏 )

**二、单项选择题（每小题2分，共30分）**

1.TCP/IP协议安全隐患不包括( D )

A.拒绝服务 B.顺序号预测攻击 C.TCP协议劫持入侵 D.设备的复杂性

2.IDEA密钥的长度为( D  )

A.56 B.64 C.124 D.128

3.在防火墙技术中，内网这一概念通常指的是( A )

A.受信网络 B.非受信网络 C.防火墙内的网络 D.互联网

4.《计算机场、地、站安全要求》的国家标准代码是( B )

A.GB57104-93 B.GB9361-88 C.GB50174-88 D.GB9361-93

5.在Kerberos中，Client向本Kerberos的认证域以内的Server申请服务的过程分为几个阶段?

( A )

A.三个 B.四个 C.五个 D.六个

6.信息安全技术的核心是( A )

A.PKI B.SET C.SSL D.ECC

7.Internet接入控制不能对付以下哪类入侵者? ( C  )

A.伪装者 B.违法者 C.内部用户 D.地下用户

8.CA不能提供以下哪种证书? ( D )

A.个人数字证书 B.SSL服务器证书 C.安全电子邮件证书 D.SET服务器证书

9.我国电子商务走向成熟的重要里程碑是( A )

A.CFCA B.CTCA C.SHECA D.RCA

10.通常为保证商务对象的认证性采用的手段是( C )

A.信息加密和解密 B.信息隐匿 C.数字签名和身份认证技术 D.数字水印

11.关于Diffie-Hellman算法描述正确的是( B  )

A.它是一个安全的接入控制协议 B.它是一个安全的密钥分配协议

C.中间人看不到任何交换的信息 D.它是由第三方来保证安全的

12.以下哪一项不在证书数据的组成中? ( D )

A.版本信息 B.有效使用期限 C.签名算法 D.版权信息

13.计算机病毒的特征之一是( B )

A.非授权不可执行性 B.非授权可执行性 C.授权不可执行性 D.授权可执行性

14.在Kerberos中，Client向本Kerberos认证域外的Server申请服务包含几个步骤? ( C )

A.6 B.7 C.8 D.9

15.属于PKI的功能是( C )

A.PAA，PAB，CA B.PAA，PAB，DRA C.PAA，CA，ORA D.PAB，CA，ORA

**三、多项选择题（每小题3分，共30分）**

1.电子商务系统可能遭受的攻击有( ABCDE )

A.系统穿透 B.植入 C.违反授权原则D.通信监视 E.计算机病毒

2.属于公钥加密体制的算法包括( CDE )

A.DES B.二重DES C.RSA D.ECC E.ELGamal

3.签名可以解决的鉴别问题有( BCDE )

A.发送者伪造 B.发送者否认 C.接收方篡改D.第三方冒充 E.接收方伪造

4.公钥证书的类型有( ABC )

A.客户证书 B.服务器证书 C.安全邮件证书D.密钥证书 E.机密证书

5.在SET中规范了商家服务器的核心功能是( ABC )

A.联系客户端的电子钱包 B.联系支付网关 C.处理SET的错误信息

D.处理客户的付款信息 E.查询客户帐号信息

6.从系统工程的角度，要求计算机信息网络具有(ABC )。

A．可用性、完整性、保密性B．真实性(不可抵赖性) C．可靠性、可控性D．稳定性

7.实施计算机信息系统安全保护的措施包括：(ABC )。

A．安全法规B、安全管理C．安全技术D．安全培训

8．OSI层的安全技术来考虑安全模型（ ABCD）。

A．物理层B．数据链路层C．网络层、传输层、会话层D．表示层、应用层

9．网络中所采用的安全机制主要有：（ BCD）。

A．区域防护 B．加密和隐蔽机制；认证和身份鉴别机制；审计；完整性保护

C．权力控制和存取控制；业务填充；路由控制 D．公证机制；冗余和备份

10．公开密钥基础设施(PKl)由以下部分组成：（ AD）。

A．认证中心；登记中心B．质检中心C．咨询服务D．证书持有者；用户；证书库

**四、判断（10分）**

1.安全法规、安全技术和安全管理，是计算机信息系统安全保护的三大组成部分。Y

2.计算机信息系统安全包括实体安全、信息安全、运行安全和人员安全等部分。Y

3.计算机信息系统的安全威胁同时来自内、外两个方面。Y

4.计算机信息网络脆弱性引发信息社会脆弱性和安全问题。Y

5.对全国公共信息网络安全监察工作是公安工作的一个重要组成部分。Y

**五、对安全的攻击可分为哪几种? （10分）**

答：网络窃听：监听局域网信道，窃取有用的数据分组，分析破解用户名、密码等；

IP 欺骗 ：在通信系统中主动插入和删除信息分组，发送一个来自被信任计算机的伪造信息分组，以使目的计算机信任并接收；

路由攻击：攻击者告诉网上的两个结点，它们之间最近的传输线路就是经过他这台计

算机的路径，这就使该台计算机的侦听变得更容易；（ARP病毒） 拒绝服务（DOS）攻击：

（1） 发送 SYN 信息分组：对网络上一台计算机提出大量的通信请求，使

该台计算机崩溃，且难以跟踪攻击源；

（2） 邮件炸弹：给某人发送过量的电子邮件可使他的系统满载直至崩溃；

拒绝服务攻击的对象不同，可以是邮件服务器、路由器或 Web 服务器等。

分布式拒绝服务（DDOS）攻击：这种攻击与传统的拒绝服务攻击一样，只不过进攻源

不只一个。

数据驱动攻击：数据驱动攻击是通过向某个程序发送数据，以产生非预期结果的攻击，

通常为攻击者给出访问目标系统的权限，数据驱动攻击分为缓冲区溢出攻

击、格式化字符串攻击、输入验证攻击、同步漏洞攻击、信任漏洞攻击等。

**六、 什么是理论安全(无条件安全)，什么是实际安全(计算上安全)？（10分）**

答：理论安全，或无条件安全： 攻击者无论截获多少密文，都无法得到足够的信息来唯一地决定明文。Shannon 用理论证明：欲达理论安全，加密密钥长度必须大于等于明文长度，密钥只用一次，用完即丢，即一次一密，One-time Pad，不实用。

实际安全，或计算上安全： 如果攻击者拥有无限资源，任何密码系统都是可以被破译的；但是，在有限的资源范围内，攻击者都不能通过系统地分析方法来破解系统，则称这个系统是计算上安全的或破译这个系统是计算上不可行。

一、单项选择题（本大题共15小题，每小题2分，共30分）

1．下列对计算机网络的攻击方式中，属于被动攻击的是(　A　　)

A．口令嗅探 B．重放C．拒绝服务 D．物理破坏

2．OSI安全体系结构中定义了五大类安全服务，其中，数据机密性服务主要针对的安全威胁是(　　B　)

A．拒绝服务 B．窃听攻击C．服务否认 D．硬件故障

3．为了提高电子设备的防电磁泄漏和抗干扰能力，可采取的主要措施是(　　B　)

A．对机房进行防潮处理 B．对机房或电子设备进行电磁屏蔽处理

C．对机房进行防静电处理 D．对机房进行防尘处理

4．为保证计算机网络系统的正常运行，对机房内的三度有明确的要求。其三度是指(　A　　)

A．温度、湿度和洁净度B．照明度、湿度和洁净度C．照明度、温度和湿度 D．温度、照明度和洁净度

5．下列加密算法中，属于双钥加密算法的是(　　D　)

A．DES B．IDEA C．Blowfish D．RSA

6．公钥基础设施(PKI)的核心组成部分是(　　A　)

A．认证机构CA B．X.509标准C．密钥备份和恢复 D．PKI应用接口系统

7．下面关于防火墙的说法中，正确的是(　C　　)

A．防火墙可以解决来自内部网络的攻击B．防火墙可以防止受病毒感染的文件的传输

C．防火墙会削弱计算机网络系统的性能D．防火墙可以防止错误配置引起的安全威胁

8．包过滤技术防火墙在过滤数据包时，一般不关心(　D　　)

A．数据包的源地址 B．数据包的目的地址C．数据包的协议类型 D．数据包的内容

9．不属于CIDF体系结构的组件是(　C　　)

A．事件产生器 B．事件分析器C．自我防护单元 D．事件数据库

10．阈值检验在入侵检测技术中属于(　　B　)

A．状态转换法 B．量化分析法C．免疫学方法 D．神经网络法

11．由于系统软件和应用软件的配置有误而产生的安全漏洞，属于(　C　　)

A．意外情况处置错误 B．设计错误C．配置错误 D．环境错误

12．采用模拟攻击漏洞探测技术的好处是(　　D　)

A．可以探测到所有漏洞 B．完全没有破坏性

C．对目标系统没有负面影响 D．探测结果准确率高

13．下列计算机病毒检测手段中，主要用于检测已知病毒的是(　　A　)

A．特征代码法 B．校验和法C．行为监测法 D．软件模拟法

14．在计算机病毒检测手段中，校验和法的优点是(　D　　)

A．不会误报 B．能识别病毒名称C．能检测出隐蔽性病毒 D．能发现未知病毒

15．一份好的计算机网络安全解决方案，不仅要考虑到技术，还要考虑的是(　C　　)

A．软件和硬件 B．机房和电源C．策略和管理 D．加密和认证

1.下面有关 DES 的描述，不正确的是（ A ）

A. 是由 IBM、Sun 等公司共同提出的 B. 其结构完全遵循 Feistel 密码结构

C. 其算法是完全公开的 D. 是目前应用最为广泛的一种分组密码算法

2． 下面有关 MD5 的描述，不正确的是（A ）

A. 是一种用于数字签名的算法 B. 得到的报文摘要长度为固定的 128 位

C. 输入以字节为单位 D. 用一个 8 字节的整数表示数据的原始长度

3. 在 PKI 系统中，负责签发和管理数字证书的是（A ）

A. CA B. RA C. LDAP D. CPS

4. 数字证书不包含（B ）

A. 颁发机构的名称 B. 证书持有者的私有密钥信息

C. 证书的有效期 D. CA 签发证书时所使用的签名算法

5. 套接字层（Socket Layer）位于（ B ）

A. 网络层与传输层之间 B. 传输层与应用层之间 C. 应用层 D. 传输层

6. 下面有关 SSL 的描述，不正确的是（D ）

A. 目前大部分 Web 浏览器都内置了 SSL 协议

B. SSL 协议分为 SSL 握手协议和 SSL 记录协议两部分

C. SSL 协议中的数据压缩功能是可选的

D. TLS 在功能和结构上与 SSL 完全相同

7. 在基于 IEEE 802.1x 与 Radius 组成的认证系统中，Radius 服务器的功能不包括（D ）

A. 验证用户身份的合法性 B. 授权用户访问网络资源

C. 对用户进行审计 D. 对客户端的 MAC 地址进行绑定

8. 在生物特征认证中，不适宜于作为认证特征的是（D ）

A. 指纹 B. 虹膜 C. 脸像 D. 体重

9. 防止重放攻击最有效的方法是（ B ）

A. 对用户账户和密码进行加密 B. 使用“一次一密”加密方式

C. 经常修改用户账户名称和密码 D. 使用复杂的账户名称和密码

10. 计算机病毒的危害性表现在（ B ）

A. 能造成计算机部分配置永久性失效 B. 影响程序的执行或破坏用户数据与程序

C. 不影响计算机的运行速度 D. 不影响计算机的运算结果

11. 下面有关计算机病毒的说法，描述正确的是（B ）

A. 计算机病毒是一个 MIS 程序

B. 计算机病毒是对人体有害的传染性疾病

C. 计算机病毒是一个能够通过自身传染，起破坏作用的计算机程序

D. 计算机病毒是一段程序，只会影响计算机系统，但不会影响计算机网络

13. 计算机病毒具有（A ）

A. 传播性、潜伏性、破坏性 B. 传播性、破坏性、易读性

C. 潜伏性、破坏性、易读性 D. 传播性、潜伏性、安全性

14. 目前使用的防杀病毒软件的作用是（C ）

A. 检查计算机是否感染病毒，并消除已感染的任何病毒

B. 杜绝病毒对计算机的侵害

C. 检查计算机是否感染病毒，并清除部分已感染的病毒

D. 查出已感染的任何病毒，清除部分已感染的病毒

15. 在 DDoS 攻击中，通过非法入侵并被控制，但并不向被攻击者直接发起攻击的计算机称为（B ）

A. 攻击者 B. 主控端 C. 代理服务器 D. 被攻击者

16. 对利用软件缺陷进行的网络攻击，最有效的防范方法是（A ）

A. 及时更新补丁程序 B. 安装防病毒软件并及时更新病毒库

C. 安装防火墙 D. 安装漏洞扫描软件

17. 在 IDS 中，将收集到的信息与数据库中已有的记录进行比较，从而发现违背安全策略的行为，

这类操作方法称为（A ）

A. 模式匹配 B. 统计分析 C. 完整性分析 D. 不确定

18. IPS 能够实时检查和阻止入侵的原理在于 IPS 拥有众多的（C ）

A. 主机传感器 B. 网络传感器 C. 过滤器 D. 管理控制台

19. 将利用虚假 IP 地址进行 ICMP 报文传输的攻击方法称为（D ）

A. ICMP 泛洪 B. LAND 攻击 C. 死亡之 ping D. Smurf 攻击

20. 以下哪一种方法无法防范口令攻击（C ）

A. 启用防火墙功能 B. 设置复杂的系统认证口令

C. 关闭不需要的网络服务 D. 修改系统默认的认证名称

21. 在分布式防火墙系统组成中不包括（D ）

A. 网络防火墙 B. 主机防火墙 C. 中心管理服务器 D. 传统防火墙

22. 下面对于个人防火墙未来的发展方向，描述不准确的是（D ）

A. 与 xDSL Modem、无线 AP 等网络设备集成

B. 与防病毒软件集成，并实现与防病毒软件之间的安全联动

C. 将个人防火墙作为企业防火墙的有机组成部分 D. 与集线器等物理层设备集成

23. 在以下各项功能中，不可能集成在防火墙上的是（D ）

A. 网络地址转换（NAT） B. 虚拟专用网（VPN）

C. 入侵检测和入侵防御 D. 过滤内部网络中设备的 MAC 地址

24. 当某一服务器需要同时为内网用户和外网用户提供安全可靠的服务时，该服务器一般要置于防

火墙的（C ） A. 内部 B. 外部 C. DMZ 区 D. 都可以

25. 以下关于状态检测防火墙的描述，不正确的是（ D ）

A. 所检查的数据包称为状态包，多个数据包之间存在一些关联

B. 能够自动打开和关闭防火墙上的通信端口

C. 其状态检测表由规则表和连接状态表两部分组成

D. 在每一次操作中，必须首先检测规则表，然后再检测连接状态表

26. 在以下的认证方式中，最不安全的是（A ）

A. PAP B. CHAP C. MS-CHAP D. SPAP

27. 以下有关 VPN 的描述，不正确的是（ C ）

A. 使用费用低廉 B. 为数据传输提供了机密性和完整性

C. 未改变原有网络的安全边界 D. 易于扩展

28. 目前计算机网络中广泛使用的加密方式为（C ）

A. 链路加密 B. 节点对节点加密 C. 端对端加密 D. 以上都是

29. 以下有关软件加密和硬件加密的比较，不正确的是（B ）

A. 硬件加密对用户是透明的，而软件加密需要在操作系统或软件中写入加密程序

B. 硬件加密的兼容性比软件加密好

C. 硬件加密的安全性比软件加密好 D. 硬件加密的速度比软件加密快

30. 对于一个组织，保障其信息安全并不能为其带来直接的经济效益，相反还会付出较大的成本，

那么组织为什么需要信息安全？ （D ）

A. 有多余的经费 B. 全社会都在重视信息安全，我们也应该关注

C. 上级或领导的要求 D. 组织自身业务需要和法律法规要求

二、填空题（本大题共10小题，每小题2分，共20分）

请在每小题的空格中填上正确答案。错填、不填均无分。

16．P2DR (PPDR)模型是一种常用的计算机网络安全模型，包含4个主要组成部分，分别是：\_\_安全策略\_\_\_\_\_\_\_\_、防护、检测和响应。

17．对计算机网络安全构成威胁的因素可以概括为：偶发因素、自然因素和\_\_人为因素\_\_\_\_\_\_\_\_三个方面。

18．物理安全技术主要是指对计算机及网络系统的环境、场地、\_\_\_设备\_\_\_\_和人员等采取的安全技术措施。

19．密码体制从原理上可分为两大类，即单钥密码体制和\_\_双密钥密码体制\_\_\_\_\_\_\_\_。

20．在加密系统中，作为输入的原始信息称为明文，加密变换后的结果称为\_\_\_密文\_\_\_\_\_\_\_。

21．防火墙的体系结构一般可分为：双重宿主主机体系机构、屏蔽主机体系结构和屏蔽\_\_\_子网体系结构\_\_\_\_\_\_\_。

22．就检测理论而言，入侵检测技术可以分为异常检测和\_误用检测\_\_\_\_\_\_\_\_\_。

23．从系统构成上看，入侵检测系统应包括数据提取、\_\_\_\_入侵分析\_\_\_\_\_\_、响应处理和远程管理四大部分。

24．按照计算机网络安全漏洞的可利用方式来划分，漏洞探测技术可以划分为信息型漏洞探测和\_\_攻击型漏洞探测\_\_

25．防范计算机病毒主要从管理和\_\_\_技术\_\_\_\_\_两方面着手。

三、简答题（本大题共6小题，每小题5分，共30分）

26．简述计算机网络安全的定义。

计算机网络安全是指利用管理控制和技术措施，保证在一个网络环境里，信息数据的机密性、完整性及可使用性受到保护。

27．简述物理安全在计算机网络安全中的地位，并说明其包含的主要内容。

物理安全是整个计算机网络系统安全的前提.

物理安全主要包括：①机房环境安全②通信线路安全③设备安全④电源安全

28．防火墙的五个主要功能是什么？

防火墙的主要功能：①过滤进、出网络的数据②管理进、出网络的访问行为③封堵某些禁止的业务④记录通过防火墙的信息和内容⑤对网络攻击检测和告警

29．基于数据源所处的位置，入侵检测系统可以分为哪5类？

基于数据源的分类：按数据源所处的位置，把入侵检测系统分为五类：即基于主机、基于网络、混合入侵检测、基于网关的入侵检测系统及文件完整性检查系统；

30．什么是计算机网络安全漏洞？

计算机网络安全漏洞是在硬件、软件和协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

31．简述恶意代码的主要防范措施。

恶意代码的防范措施（P228）：①及时更新系统，修补安全漏洞②设置安全策略，限制脚本程序的运行③开启防火墙，关闭不必要的服务和系统信息；④养成良好的上网习惯。

四、综合分析题（本大题共2小题，每小题10分，共20分）

32．某局域网如下图，其中：1号设备是路由器，4号设备是交换机，5和6号设备是DMZ区服务器，7、8和9号设备是个人计算机。

请回答下列问题：

(1)2和3号设备中，哪个设备是防火墙?哪个设备是交换机?

3号设备是防火墙；2设备是交换机

(2)3套个人防火墙软件最适合安装在哪3个设备上?(只能选3个设备)

7、8、9号设备

(3)5套防病毒软件应该安装在哪5个设备上?(只能选5个设备)

5套防病毒软件应该安装在5、6、7、7、8、9号设备

33．对给定二进制明文信息“0011010101000101001111010010101110010101”进行两次加密。第一次，采用8位分组异或算法，用密钥“01010101”对明文进行加密运算。第二次，采用“1→4(读作：位置l的数据移到位置4，以下类推)，2→8，3→1，4→5，5→7，6→2，7→6，8→3”对第一次加密后的密文进行8位分组换位加密运算。请写出两次加密的密文。

注：异或运算的规则如下表所示。

x y x COR y

0 0 0

0 1 1

1 0 1

1 1 0

第一次，采用8位分组异或算法，用密钥“01010101”对明文进行加密运算的密文：

01100000 00010000 01101000 01111110 11000000

第二次，对第一次加密后的密文进行8位分组换位加密运算的密文

10000001 00001000 10000011 11001111 00010001

一、 单项选择题（每小题 1 1 分，共 30 分）

1.下面有关 DES 的描述，不正确的是（ A ）

A. 是由 IBM、Sun 等公司共同提出的 B. 其结构完全遵循 Feistel 密码结构

C. 其算法是完全公开的 D. 是目前应用最为广泛的一种分组密码算法

2． 下面有关 MD5 的描述，不正确的是（A ）

A. 是一种用于数字签名的算法 B. 得到的报文摘要长度为固定的 128 位

C. 输入以字节为单位 D. 用一个 8 字节的整数表示数据的原始长度

3. 在 PKI 系统中，负责签发和管理数字证书的是（A ）

A. CA B. RA C. LDAP D. CPS

4. 数字证书不包含（B ）

A. 颁发机构的名称 B. 证书持有者的私有密钥信息

C. 证书的有效期 D. CA 签发证书时所使用的签名算法

5. 套接字层（Socket Layer）位于（ B ）

A. 网络层与传输层之间 B. 传输层与应用层之间 C. 应用层 D. 传输层

6. 下面有关 SSL 的描述，不正确的是（D ）

A. 目前大部分 Web 浏览器都内置了 SSL 协议

B. SSL 协议分为 SSL 握手协议和 SSL 记录协议两部分

C. SSL 协议中的数据压缩功能是可选的

D. TLS 在功能和结构上与 SSL 完全相同

7. 在基于 IEEE 802.1x 与 Radius 组成的认证系统中，Radius 服务器的功能不包括（D ）

A. 验证用户身份的合法性 B. 授权用户访问网络资源

C. 对用户进行审计 D. 对客户端的 MAC 地址进行绑定

8. 在生物特征认证中，不适宜于作为认证特征的是（D ）

A. 指纹 B. 虹膜 C. 脸像 D. 体重

9. 防止重放攻击最有效的方法是（ B ）

A. 对用户账户和密码进行加密 B. 使用“一次一密”加密方式

C. 经常修改用户账户名称和密码 D. 使用复杂的账户名称和密码

10. 计算机病毒的危害性表现在（ B ）

A. 能造成计算机部分配置永久性失效 B. 影响程序的执行或破坏用户数据与程序

C. 不影响计算机的运行速度 D. 不影响计算机的运算结果

11. 下面有关计算机病毒的说法，描述正确的是（B ）

A. 计算机病毒是一个 MIS 程序

B. 计算机病毒是对人体有害的传染性疾病

C. 计算机病毒是一个能够通过自身传染，起破坏作用的计算机程序

D. 计算机病毒是一段程序，只会影响计算机系统，但不会影响计算机网络

13. 计算机病毒具有（A ）

A. 传播性、潜伏性、破坏性 B. 传播性、破坏性、易读性

C. 潜伏性、破坏性、易读性 D. 传播性、潜伏性、安全性

14. 目前使用的防杀病毒软件的作用是（C ）

A. 检查计算机是否感染病毒，并消除已感染的任何病毒

B. 杜绝病毒对计算机的侵害

C. 检查计算机是否感染病毒，并清除部分已感染的病毒

D. 查出已感染的任何病毒，清除部分已感染的病毒

15. 在 DDoS 攻击中，通过非法入侵并被控制，但并不向被攻击者直接发起攻击的计算机称为（B ）

A. 攻击者 B. 主控端 C. 代理服务器 D. 被攻击者

16. 对利用软件缺陷进行的网络攻击，最有效的防范方法是（A ）

A. 及时更新补丁程序 B. 安装防病毒软件并及时更新病毒库

C. 安装防火墙 D. 安装漏洞扫描软件

17. 在 IDS 中，将收集到的信息与数据库中已有的记录进行比较，从而发现违背安全策略的行为，

这类操作方法称为（A ）

A. 模式匹配 B. 统计分析 C. 完整性分析 D. 不确定

18. IPS 能够实时检查和阻止入侵的原理在于 IPS 拥有众多的（C ）

A. 主机传感器 B. 网络传感器 C. 过滤器 D. 管理控制台

19. 将利用虚假 IP 地址进行 ICMP 报文传输的攻击方法称为（D ）

A. ICMP 泛洪 B. LAND 攻击 C. 死亡之 ping D. Smurf 攻击

20. 以下哪一种方法无法防范口令攻击（C ）

A. 启用防火墙功能 B. 设置复杂的系统认证口令

C. 关闭不需要的网络服务 D. 修改系统默认的认证名称

21. 在分布式防火墙系统组成中不包括（D ）

A. 网络防火墙 B. 主机防火墙 C. 中心管理服务器 D. 传统防火墙

22. 下面对于个人防火墙未来的发展方向，描述不准确的是（D ）

A. 与 xDSL Modem、无线 AP 等网络设备集成

B. 与防病毒软件集成，并实现与防病毒软件之间的安全联动

C. 将个人防火墙作为企业防火墙的有机组成部分

D. 与集线器等物理层设备集成

23. 在以下各项功能中，不可能集成在防火墙上的是（D ）

A. 网络地址转换（NAT） B. 虚拟专用网（VPN）

C. 入侵检测和入侵防御 D. 过滤内部网络中设备的 MAC 地址

24. 当某一服务器需要同时为内网用户和外网用户提供安全可靠的服务时，该服务器一般要置于防

火墙的（C ） A. 内部 B. 外部 C. DMZ 区 D. 都可以

25. 以下关于状态检测防火墙的描述，不正确的是（ D ）

A. 所检查的数据包称为状态包，多个数据包之间存在一些关联

B. 能够自动打开和关闭防火墙上的通信端口

C. 其状态检测表由规则表和连接状态表两部分组成

D. 在每一次操作中，必须首先检测规则表，然后再检测连接状态表

26. 在以下的认证方式中，最不安全的是（A ）

A. PAP B. CHAP C. MS-CHAP D. SPAP

27. 以下有关 VPN 的描述，不正确的是（ C ）

A. 使用费用低廉 B. 为数据传输提供了机密性和完整性

C. 未改变原有网络的安全边界 D. 易于扩展

28. 目前计算机网络中广泛使用的加密方式为（C ）

A. 链路加密 B. 节点对节点加密 C. 端对端加密 D. 以上都是

29. 以下有关软件加密和硬件加密的比较，不正确的是（B ）

A. 硬件加密对用户是透明的，而软件加密需要在操作系统或软件中写入加密程序

B. 硬件加密的兼容性比软件加密好

C. 硬件加密的安全性比软件加密好

D. 硬件加密的速度比软件加密快

30. 对于一个组织，保障其信息安全并不能为其带来直接的经济效益，相反还会付出较大的成本，

那么组织为什么需要信息安全？ （D ）

A. 有多余的经费 B. 全社会都在重视信息安全，我们也应该关注

C. 上级或领导的要求 D. 组织自身业务需要和法律法规要求

二、 填空 题 （每空 空 1 1 分，共 20 分）

31．利用公钥加密数据，然后用私钥解密数据的过程称为 加密 ；利用私钥加密数据，然后用公钥解密数据的过程称为 数字签名 。

32. 在 PKI/PMI 系统中，一个合法用户只拥有一个唯一的 公钥证书 ，但可能会同时拥有多个不同的 属性证书 。

33. 计算机网络安全领域的 3A 是指 认证、 授权 和 审计 。

34. SSL 是一种综合利用 对称密钥 和 非对称密钥 技术进行安全通信的工业标准。

35. 扫描技术主要分为 主机安全扫描 和 网络安全扫描 两种类型。

36. 在 IDS 的报警中，可以分为错误报警和正确的报警两种类型。其中错误报警中，将 IDS 工于正常状态下产生的报警称为 误报 ；而将 IDS 对已知的入侵活动未产生报警的现象称为 漏报 。

37. 状态检测防火墙是在传统包过滤防火墙的基础上发展而来的，所以将传统的包过滤防火墙称为

静态包过滤 防火墙，而将状态检测防火墙称为 动态包过滤 防火墙。

38. VPN 是利用 Internet 等 公共网络 的基础设施，通过 隧道 技术，为用户提供一条与专网相同

的安全通道。

39. VPN 系统中的三种典型技术分别是 隧道技术 、 身份认证技术 和 加密技术。

40. 目前身份认证技术可分为 PKI 和非 PKI 两种类型，其中在 VPN 的用户身份认证中一般采用非PKI 认证方式，而信息认证中采用 PKI 认证方式。

三、判断题（每小题 1 1 分，共 0 10 分）

41．Feistel 是密码设计的一个结构，而非一个具体的密码产品。 （√ ）

42. 暴力破解与字典攻击属于同类网络攻击方式，其中暴力破解中所采用的字典要比字典攻击中使

用的字典的范围要大。 （ √ ）

43. DHCP 服务器只能给客户端提IP地址和网关地址， 而不能提供 DNS 服务器的 IP 地址。（× ）

44. 间谍软件能够修改计算机上的配置文件。 （× ）

45. 蠕虫既可以在互联网上传播，也可以在局域网上传播。而且由于局域网本身的特性，蠕虫在局

域网上传播速度更快，危害更大。 （√ ）

46. 与 IDS 相比，IPS 具有深层防御的功能。 （√ ）

47. 当硬件配置相同时，代理防火墙对网络运行性能的影响要比包过滤防火墙小。 （× ）

48. 在传统的包过滤、代理和状态检测 3 类防火墙中，只有状态检测防火墙可以在一定程度上检测

并防止内部用户的恶意破坏。 （√ ）

49. 防火墙一般采用“所有未被允许的就是禁止的”和“所有未被禁止的就是允许的”两个基本准

则，其中前者的安全性要比后者高。 （√ ）

50. 在利用 VPN 连接两个 LAN 时，LAN 中必须使用 TCP/IP 协议。 （ × ）

四 、 名词解释 （每 小题 4 4 分，共 0 20 分）

51．DNS 缓存中毒

答：DNS 为了提高查询效率，采用了缓存机制，把用户查询过的最新记录存放在缓存中，并设置生

存周期（Time To Live，TTL） 。在记录没有超过 TTL 之前，DNS 缓存中的记录一旦被客户端查询，DNS 服务器（包括各级名字服务器）将把缓存区中的记录直接返回给客户端，而不需要进行逐级查询，提高了查询速率。 （2 分）DNS 缓存中毒利用了 DNS 缓存机制，在 DNS 服务器的缓存中存入大量错误的数据记录主动供用户查询。由于缓存中大量错误的记录是攻击者伪造的，而伪造者可能会根据不同的意图伪造不同的记录。由于 DNS 服务器之间会进行记录的同步复制，所以在 TTL 内，缓存中毒的 DNS 服务器有可能将错误的记录发送给其他的 DNS 服务器， 导致更多的 DNS 服务器中毒。 （2 分）

52．机密性、完整性、可用性、可控性

答：机密性是确保信息不暴露给未经授权的人或应用进程（1 分）；完整性是指只有得到允许的人

或应用进程才能修改数据，并且能够判别出数据是否已被更改（1 分）；可用性是指只有得到授权

的用户在需要时才可以访问数据，即使在网络被攻击时也不能阻碍授权用户对网络的使用（1 分）；

可控性是指能够对授权范围内的信息流向和行为方式进行控制（1 分）

53．PMI

答：PMI（授权管理基础设施）是在 PKI 发展的过程中为了将用户权限的管理与其公钥的管理分离，

由 IETF 提出的一种标准。PMI 的最终目标就是提供一种有效的体系结构来管理用户的属性。PMI

以资源管理为核心，对资源的访问控制权统一交由授权机构统一处理（2 分） 。同 PKI 相比，两者主要区别在于 PKI 证明用户是谁，而 PMI 证明这个用户有什么权限、能干什么。PMI 需要 PKI 为其提供身份认证。PMI 实际提出了一个新的信息保护基础设施，能够与 PKI 紧密地集成，并系统地建立起对认可用户的特定授权，对权限管理进行系统的定义和描述，完整地提供授权服务所需过程。

54．防火墙

答：防火墙是指设置在不同网络（如可信赖的企业内部局域网和不可信赖的公共网络）之间或网络

安全域之间的一系列部件的组合（2 分），通过监测、限制、更改进入不同网络或不同安全域的数

据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以防止发生不可预测的、潜在破坏

性的入侵，实现网络的安全保护。（2 分）

55．VPN

答：VPN（虚拟专用网）是利用 Internet 等公共网络的基础设施，通过隧道技术，为用户提供一与

专用网络具有相同通信功能的安全数据通道，实现不同网络之间以及用户与网络之间的相互连接（2

分） 。 从 VPN 的定义来看， 其中 “虚拟” 是指用户不需要建立自己专用的物理线路， 而是利用 Internet等公共网络资源和设备建立一条逻辑上的专用数据通道，并实现与专用数据通道相同的通信功能；“专用网络”是指这一虚拟出来的网络并不是任何连接在公共网络上的用户都能够使用的，而是只有经过授权的用户才可以使用。同时，该通道内传输的数据经过了加密和认证，从而保证了传输内容的完整性和机密性。（2 分）

五 、 简答题 （每小题 0 10 分，共 2 20 0 分）

56． 根据实际应用，以个人防火墙为主，简述防火墙的主要功能及应用特点。

答：防火墙是指设置在不同网络（如可信赖的企业内部局域网和不可信赖的公共网络）之间或网络

安全域之间的一系列部件的组合，通过监测、限制、更改进入不同网络或不同安全域的数据流，尽

可能地对外部屏蔽网络内部的信息、结构和运行状况，以防止发生不可预测的、潜在破坏性的入侵，

实现网络的安全保护。（2 分）

个人防火墙是一套安装在个人计算机上的软件系统，它能够监视计算机的通信状况，一旦发现有对

计算机产生危险的通信就会报警通知管理员或立即中断网络连接，以此实现对个人计算机上重要数

据的安全保护。（2 分）

个人防火墙是在企业防火墙的基础上发展起来，个人防火墙采用的技术也与企业防火墙基本相同，

但在规则的设置、防火墙的管理等方面进行了简化，使非专业的普通用户能够容易地安装和使用。

（2 分）

为了防止安全威胁对个人计算机产生的破坏，个人防火墙产品应提供以下的主要功能。防止 Internet

上用户的攻击、阻断木马及其他恶意软件的攻击、为移动计算机提供安全保护、与其他安全产品进

行集成。（4 分）

57． 如图所示，描述 DDoS 攻击的实现方法。

DDoS 攻击是利用一批受控制的主机向一台主机发起攻击，其攻击的强度和造成的威胁要比 DoS 攻击严重得多，当然其破坏性也要强得多。 （2 分）

在整个 DDoS 攻击过程中，共有四部分组成：攻击者、主控端、代理服务器和被攻击者，其中每一

个组成在攻击中扮演的角色不同。

（1） 攻击者。攻击者是指在整个 DDoS 攻击中的主控台，它负责向主控端发送攻击命令。与

DoS 攻击略有不同，DDoS 攻击中的攻击者对计算机的配置和网络带宽的要求并不高，只要能够向

主控端正常发送攻击命令即可。 （2 分）

（2） 主控端。主控端是攻击者非法侵入并控制的一些主机，通过这些主机再分别控制大量的

代理服务器。攻击者首先需要入侵主控端，在获得对主控端的写入权限后，在主控端主机上安装特

定的程序， 该程序能够接受攻击者发来的特殊指令， 并且可以把这些命令发送到代理服务器上。 （2

分）

（3） 代理服务器。代理服务器同样也是攻击者侵入并控制的一批主机，同时攻击者也需要在

入侵这些主机并获得对这些主机的写入权限后，在上面安装并运行攻击器程序，接受和运行主控端

发来的命令。代理服务器是攻击的直接执行者，真正向被攻击主机发送攻击。 （2 分）

（4）被攻击者。是 DDoS 攻击的直接受害者，目前多为一些大型企业的网站或数据库系统。 （2

分）

网络安全与技术试题及参考答案

一、选择题，共15 题。

（1） 4.5.6.7 这个IP地址所属的类别是   A   。

A.  A类， B.  B类， C.  C类， D.  D类

（2）在下列数中，一个B类子网掩码允许有的数字是   C   个1，且其余位都为0。

A. 9， B. 14，C. 17，D. 3

（3）如果一个A类地址的子网掩码中有14个1，它能确定  C    个子网。

A. 32， B. 8，C. 64，D.128

（4）路由器在两个网段之间转发数据包时，读取其中的   A   地址来确定下一跳的转发路径。

A. IP， B. MAC，C. 源，D. ARP

（5）IP包在网络上传输时若出现差错，差错报告被封装到ICMP分组传送给  A    。

A.发送者， B.接收者，C. 一个路由器，D.上述选项中的任何一项。

（6）UDP、TCP和SCTP都是   D    层协议。

A. 物理， B. 数据链路，C. 网络，D.传输

（7）UDP需要使用   A   地址，来给相应的应用程序发送用户数据报。

A. 端口， B. 应用程序，C. 因特网，   D.物理

（8）IP负责  A      之间的通信，它使用   D       地址进行寻址；

A. 主机到主机；     B. 进程到进程； C. 物理；    D. IP

（9）TCP负责   B    之间的通信，它使用    C     地址进行寻址。

A. 主机到主机；     B. 进程到进程； C. 端口号；    D. IP

（10）     c   地址唯一地标识一个正在运行的应用程序，它由      D   地址的组合构成。

A. IP， B. 传输层协议，C. 网卡的MAC，D.套接字，E. 端口号

（11）面向连接的并发服务器使用  D      端口号进行网络通信服务。

A. 临时， B. 公认，C. 主动，   D.（A）和（B）

（12）在电子邮件地址 macke@pit.arc.nasa.gov 中，域名部分是  B      。

A. macke，B. pit.arc.nasa.gov，C. macke@pit.arc.nasa.gov，D.(A)和（B）

（13）电子邮件客户端通常需要用    A    协议来发送邮件。

A. 仅SMTP， B.仅POP，  C. SMTP和POP，  D.以上都不正确

（14）TCP不适合于传输实时通信数据，是因为  C    。

A. 没有提供时间戳，B.不支持多播，C.丢失分组需要重新传输，D.所有上述选项

（15）下列关于IPv4地址的描述中哪些是错误的？     DF

A．IP地址的总长度为32位

B．每一个IP地址都由网络地址和主机地址组成

C．D类地址属于组播地址

D．一个C类地址拥有8位主机地址，可给256台主机分配地址

E．所有的A类地址的首位一定是“0”

F．A类地址拥有最多的网络数

（15）在OSI参考模型的描述中，下列说法中不正确的是   C     。

A．OSI参考模型定义了开放系统的层次结构

B．OSI参考模型是一个在制定标准时使用的概念性的框架

C．OSI参考模型的每层可以使用上层提供的服务

D．OSI参考模型是开放系统互联参考模型

（16）在应用层协议中，   B       既可使用传输层的TCP协议，又可用UDP协议。

A.SNMP           B.DNS             C.HTTP                D.FTP

（17）在OSI参考模型中，同一结点内相邻层之间通过      A      来进行通信。

A．接口       B．进程       C．协议       D．应用程序

（18）OSI参考模型的数据链路层的功能包括    A       。

A．保证数据帧传输的正确顺序、无差错和完整性

B．提供用户与传输网络之间的接口

C．控制报文通过网络的路由选择

D．处理信号通过物理介质的传输

（19）100Mbps快速以太网与10Mbps传统以太网的帧结构    C     。

A．完全不同          B．帧头控制字节不同

C．完全相同          D．可以相同也可以不同

（20）   C    的物理层标准要求使用非屏蔽双绞线。

A．10 BASE-2    B．10 BASE-5   C．100BASE-TX     D．100 BASE-FX

（21）当一个以太网中的一台源主机要发送数据给位于另一个网络中的一台目的主机时，以太帧头部的目的地址是      B     ，IP包头部的目的地址必须是   D     。

A．路由器的IP地址               B．路由器的MAC地址

C．目的主机的MAC地址           D．目的主机的IP地址

（22）当一个发往目的主机的IP包经过多个路由器转发时，以下哪种情况正确地描述了包内IP地址的变化？    D      。

A当IP包在每跳段中传输时，目的地址改为下个路由器的IP地址。

B当一个路由器将IP包发送到广域网WAN时，目的IP地址经常变化。

C目的IP地址将永远是第一个路由器的IP地址。

D目的IP地址固定不变。

（23）以下哪个协议被用于动态分配本地网络内的IP地址？  A      。

A. DHCP       B. ARP         C. proxy ARP       D. IGRP

（24）E-mail安全传输的方法称为 C    。

A． TLS        B.  SA安全关联组             C.  S/MIME     D.  IPSec

（25）   B    可以根据报文自身头部包含的信息来决定转发或阻止该报文。

A．代理防火墙             B. 包过滤防火墙  C. 报文摘要                D. 私钥

（26）  D     协议主要用于加密机制。

A．HTTP                      B. FTP                 C. TELNET                  D. SSL

（27）属于被动攻击的恶意网络行为是  B     。

A．缓冲区溢出             B. 网络监听                C. 端口扫描                D. IP欺骗

（28）向有限的存储空间输入超长的字符串属于   A  攻击手段。

A．缓冲区溢出             B. 运行恶意软件         C. [浏览](http://action.vogate.com/click/click.php?ads_id=1779&site_id=6235007045037770&click=1&url=http%3A//www.vogate.com/emc.php&v=0&k=%u6D4F%u89C8&s=http%3A//yuege.cn/read.php%3F194&rn=81649)恶意代码网页  D. 打开病毒附件

（29）IPSec需要使用一个称为B      的信令协议来建立两台主机之间的逻辑连接。

A．AH认证头部协议     B. SA安全关联组协议       C. PGP隐私  D. TLS传输安全协议

（30）在IP互联网层提供安全的一组协议是   D       。

A．TLS                B. SSH                 C. PGP                 D. IPSec

（31） A      是IP层的安全协议，它只能提供完整性和鉴别功能，不能提供信息保密。

A．AH                  B. PGP                 C. ESP                  D. IPSec

（32）虚拟专网VPN使用  C    来保证信息传输中的保密性。

A．IPSec                     B. 隧道                C.（A）和（B）        D. 以上都不正确

（33）在VPN中，对  A      进行加密。

A．内网数据报  B. 外网数据报  C. 内网和外网数据报  D. 内网和外网数据报都不

二、叙述回答题：

（1）电子商务中安全电子交易SET系统的双重签名作用是什么？它是怎样实现的？

答：在安全电子交易SET中，持卡人购物时需要向供货商发送两个信息：订货单信息OI和加密的支付卡信息PI。其中OI是发给供货商的，而加密后的PI要经过供货商转交给支付网关银行。同一交易的OI和PI是相互关联的，利用双重前面对二者的报文摘要进行签名，可以分别向供货商和银行证明OI和PI的真实性。

（2）简述X.509的作用是什么？与其他同类系统相比，它的特点是什么。

答： X.509是一个世界统一的公钥证书协议。它的作用是：权威机构对证书持有者的公钥进行认证，对持卡人的身份进行认证。它的使用不需要实时上网验证，可以脱离网络使用。

（3）简述RSA和DES加密算法在信息的保密性、完整性和抗拒认方面的概念和特点。

答： RSA便于确认安全性，它使用一对公开密钥和私有密钥，它的保密性取决于大素数的运算难度，与Hash报文摘要结合使用，实现对报文的完整性确认，以及防拒认，适合于对小数据量报文的加密。

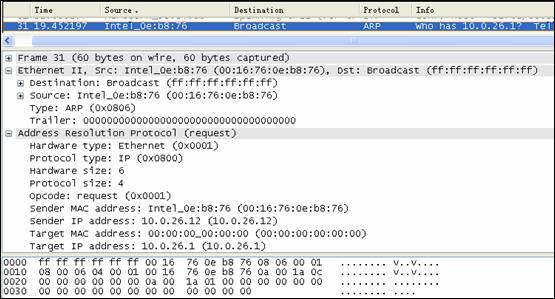
而DES对通信数据是否已经被泄密的确认较困难，它的保密性取决于对称密钥的安全性，通过对报文摘要的加密实现完整性确认，在实现抗拒认方面较困难。

（4）分别用实例说明网络安全所提供的5种服务的用途：信息保密，信息的完整性确认，身份认证，防拒认，网络实体的认证识别。

答：参看教材340页。

三、网络信息数据分析题：

（1）在校园的局域网中捕获到一个以太网帧，此帧的全部数据如下图所示，请对照相关协议的数据结构图，回答以下问题：



A．此帧的用途和目的是什么？地址解析协议的ARP查询。

B．此帧的目的物理地址是 ff:ff:ff:ff:ff:ff，它属于（广播、单播）地址。

C．它的目的IP地址是 10.0.26.1     ，它属于（广播、单播）地址。

D．此的源物理地址是  00:16:76:0e:b8:76 。

E．它的源IP地址是 10.0.26.12           ，它属于（公网、私网）IP地址。

F．此帧属于以太网帧，还是IEEE802.3帧？为什么？

答：因为类型字段0806表示ARP协议，它大于0600，所以属于以太网，版本II。

G．此帧中封装的上层协议是什么？

答：ARP协议。

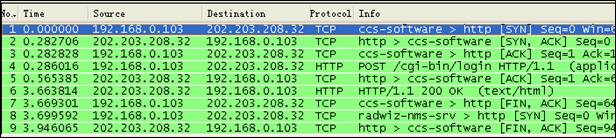
H．此帧中有没有填充字段？在什么情况下需要进行填充？

答：有，填充了18字节的0，这是为了保证CSMA/CD“载波侦听/多路访问/冲突检测”协议的正确实施，即以太网的最短帧长必须大于64字节。

I．如果有一台网络计算机对此帧收到此帧后发出响应，响应中应当包含什么内容？

答：即ARP响应，其中应当包含被查询主机的MAC地址和IP地址，参看教材82页。

（2）下图是一台计算机访问一个Web网站时的数据包序列。分析图中数据简要回答以下问题：



A．客户机的IP地址是 192.168.0.103  ，它属于（公网，私网）地址。

B．Web服务器的IP地址是 202.203.208.32 ，它属于（公网，私网）地址。

C．客户机访问服务器使用的传输层协议是 TCP ，应用层协议是 HTTP  ，应用层协议的版本号是  HTTP/1.1   。

D．客户机向服务器请求建立TCP连接的数据包的号数是 1    。

E．客户机向服务器发送用户名和口令进行请求登录的数据包的号数是   4    。

F．此次访问中，客户机使用的端口名称是 ccs-doftware ，服务器使用的端口名称是  http 。

G．服务器对客户机的响应报文中，代码200的含义是  请求被成功接受 。

H．在TCP的6比特的控制字段中：

[SYN]的含义是  请求建立TCP连接 。[SYN, ACK]的含义是  可以建立连接  。

[ACK]的含义是  确认  。[FIN, ACK]的含义是  同意结束 ，

[FIN]的含义是   结束，参看教材150页  。

I．服务器根据请求向客户机发送网页的第一个数据帧的号数是    6    。

1. **单项选择题**
2. Chinese Wall 模型的设计宗旨是：（A）。

A、用户只能访问哪些与已经拥有的信息不冲突的信息   
B、用户可以访问所有信息

C、用户可以访问所有已经选择的信息   
D、用户不可以访问哪些没有选择的信息

1. 安全责任分配的基本原则是：（C）。

A、“三分靠技术，七分靠管理” B、“七分靠技术，三分靠管理”

C、“谁主管，谁负责” D、防火墙技术

1. 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（B）不属于信息运行安全技术的范畴。

A、风险分析 B、审计跟踪技术 C、应急技术 D、防火墙技术

1. 从风险的观点来看，一个具有任务紧急性，核心功能性的计算机应用程序系统的开发和维护项目应该（A）。

A、内部实现 B、外部采购实现 C、合作实现 D、多来源合作实现

1. 从风险分析的观点来看，计算机系统的最主要弱点是（B）。

A、内部计算机处理 B、系统输入输出 C、通讯和网络 D、外部计算机处理

1. 从风险管理的角度，以下哪种方法不可取？（D）

A、接受风险 B、分散风险 C、转移风险 D、拖延风险

1. 当今IT的发展与安全投入，安全意识和安全手段之间形成（B）。

A、安全风险屏障 B、安全风险缺口 C、管理方式的变革 D、管理方式的缺口

1. 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（D）。

A、已买的软件 B、定做的软件 C、硬件 D、数据

1. 当一个应用系统被攻击并受到了破坏后，系统管理员从新安装和配置了此应用系统，在该系统重新上线前管理员不需查看：（C）

A、访问控制列表 B、系统服务配置情况

1. 审计记录 D、用户账户和权限的设置

10、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行（B）。

1. 逻辑隔离 B、物理隔离 C、安装防火墙 D、VLAN 划分

11、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？（D）

A、威胁、脆弱性 B、系统价值、风险

C、信息安全、系统服务安全 D、受侵害的客体、对客体造成侵害的程度业务

12、公司应明确员工的雇佣条件和考察评价的方法与程序，减少因雇佣不当而产生的安全风险。人员考察的内容不包括（B）。

A、身份考验、来自组织和个人的品格鉴定 B、家庭背景情况调查

C、学历和履历的真实性和完整性 D、学术及专业资格

13、计算机信息的实体安全包括环境安全、设备安全、（B）三个方面。

A运行安全 B、媒体安全 C、信息安全 D、人事安全

14、目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（B）

A、公安部 B、国家保密局

C、信息产业部 D、国家密码管理委员会办公室

15、目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（B）

A、GB/T 18336-2001 信息技术安全性评估准则

B、GB 17859-1999 计算机信息系统安全保护等级划分准则

C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构

D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

16、确保信息没有非授权泄密，即确保信息不泄露给非授权的个人、实体或进程，不为其所用，是指（C）。

A、完整性 B、可用性 C、保密性 D、抗抵赖性

17、如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（A）

A、自动软件管理 B、书面化制度 C、书面化方案 D、书面化标准

18、如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？（A）

A、计算风险 B、选择合适的安全措施

C、实现安全措施 D、 接受残余风险

19、软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（A）

A、软件中止和黑客入侵 B、远程监控和远程维护

C、软件中止和远程监控 D、远程维护和黑客入侵

20、 管理审计指（C）

A、保证数据接收方收到的信息与发送方发送的信息完全一致

B、防止因数据被截获而造成的泄密

C、对用户和程序使用资源的情况进行记录和审查

D、保证信息使用者都可

21、为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（A）

A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B、进行离职谈话，禁止员工账号，更改密码

C、让员工签署跨边界协议

D、列出员工在解聘前需要注意的所有责任

22、为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（D）

A、人际关系技能 B、项目管理技能 C、技术技能 D、沟通技能

23、我国的国家秘密分为几级？（A）

A、3 B、4 C、5 D、6

24、系统管理员属于（C）。

A、决策层 B、管理层

C、执行层 D、既可以划为管理层，又可以划为执行层

25、下列哪一个说法是正确的？（C）

A、风险越大，越不需要保护 B、风险越小，越需要保护

C、风险越大，越需要保护 D、越是中等风险，越需要保护

26、下面哪类访问控制模型是基于安全标签实现的？（B）

A、自主访问控制 B、强制访问控制

C、基于规则的访问控制 D、基于身份的访问控制

27、下面哪项能够提供最佳安全认证功能？（B）

A、这个人拥有什么 B、这个人是什么并且知道什么

C、这个人是什么 D、这个人知道什么

28、下面哪一个是国家推荐性标准？（A）

A、GB/T 18020-1999 应用级防火墙安全技术要求

B、SJ/T 30003-93 电子计算机机房施工及验收规范

C、GA243-2000 计算机病毒防治产品评级准则

D、ISO/IEC 15408-1999 信息技术安全性评估准则

29、下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（C）

A、对安全违规的发现和验证是进行惩戒的重要前提

B、惩戒措施的一个重要意义在于它的威慑性

C、处于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训

D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

30、下面哪一项最好地描述了风险分析的目的？（C）

A、识别用于保护资产的责任义务和规章制度

B、识别资产以及保护资产所使用的技术控制措施

C、识别资产、脆落性并计算潜在的风险

D、识别同责任义务有直接关系的威胁

31、下面哪一项最好地描述了组织机构的安全策略？（A）

A、定义了访问控制需求的总体指导方针

B、建议了如何符合标准

C、表明管理意图的高层陈述

D、表明所使用的技术控制措施的高层陈述

32、下面哪一种风险对电子商务系统来说是特殊的？（D）

A、服务中断 B、应用程序系统欺骗

C、未授权的信息泄露 D、确认信息发送错误

33、下面有关我国标准化管理和组织机构的说法错误的是？（C）

A、国家标准化管理委员会是统一管理全国标准化工作的主管机构

B、国家标准化技术委员会承担国家标准的制定和修改工作

C、全国信息安全标准化技术委员负责信息安全技术标准的审查、批准、编号和发布

D、全国信息安全标准化技术委员负责统一协调信息安全国家标准年度技术项目

34、项目管理是信息安全工程师基本理论，以下哪项对项目管理的理解是正确的？（A）

A、项目管理的基本要素是质量，进度和成本

B、项目管理的基本要素是范围，人力和沟通

C、项目管理是从项目的执行开始到项目结束的全过程进行计划、组织

D、项目管理是项目的管理者，在有限的资源约束下，运用系统的观点，方法和理论，对项目涉及的技术工作进行有效地管理

35、信息安全的金三角是（C）。

A、可靠性，保密性和完整性 B、多样性，冗余性和模化性

C、保密性，完整性和可用性 D、多样性，保密性和完整性

36、信息安全风险缺口是指（A）。

A、IT的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

37、信息安全风险应该是以下哪些因素的函数？（A）

A、信息资产的价值、面临的威胁以及自身存在的脆弱性等

B、病毒、黑客、漏洞等

C、保密信息如国家密码、商业秘密等

D、网络、系统、应用的复杂的程度

38、信息安全工程师监理的职责包括？（A）

A、质量控制，进度控制，成本控制，合同管理，信息管理和协调

B、质量控制，进度控制，成本控制，合同管理和协调

C、确定安全要求，认可设计方案，监视安全态势，建立保障证据和协调

D、确定安全要求，认可设计方案，监视安全态势和协调

39、信息安全管理最关注的是？（C）

A、外部恶意攻击 B、病毒对PC的影响

C、内部恶意攻击 D、病毒对网络的影响

40、信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（C）

A、信息的价值 B、信息的时效性

C、信息的存储方式 D、法律法规的规定

41、信息网络安全的第三个时代是（A）

A、主机时代，专网时代，多网合一时代 B、主机时代，PC时代，网络时代

C、PC时代，网络时代，信息时代 D、2001年，2002年，2003年

42、一个公司在制定信息安全体系框架时，下面哪一项是首要考虑和制定的？（A）

A、安全策略 B、安全标准 C、操作规程 D、安全基线

43、以下哪个不属于信息安全的三要素之一？（C）

A、机密性 B、完整性 C、抗抵赖性 D、可用性

44、以下哪一项安全目标在当前计算机系统安全建设中是最重要的？（C）

A、目标应该具体 B、目标应该清晰

C、目标应该是可实现的 D、目标应该进行良好的定义

45、以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（A）

A、制度和措施 B、漏洞分析

C、意外事故处理计划 D、采购计划

46、以下哪一项是对信息系统经常不能满足用户需求的最好解释？（C）

A、没有适当的质量管理工具 B、经常变化的用户需求

C、用户参与需求挖掘不够 D、项目管理能力不强

47、以下哪一种人给公司带来了最大的安全风险？（D）

A、临时工 B、咨询人员 C、以前的员工 D、当前的员工

48、以下哪种安全模型未使用针对主客体的访问控制机制？（C）

A、基于角色模型 B、自主访问控制模型

C、信息流模型 D、强制访问控制模型

49、以下哪种措施既可以起到保护的作用还能起到恢复的作用？（C）

A、对参观者进行登记 B、备份

C、实施业务持续性计划 D、口令

50、以下哪种风险被定义为合理的风险？（B）

A、最小的风险 B、可接受风险

C、残余风险 D、总风险

51、以下人员中，谁负有决定信息分类级别的责任？（B）

A、用户 B、数据所有者 C、审计员 D、安全官

52、有三种基本的鉴别的方式：你知道什么，你有什么,以及（C）。

A、你需要什么 B、你看到什么 C、你是什么 D、你做什么

53、在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（B）

A、自下而上 B、自上而下 C、上下同时开展 D、以上都不正确

54、在风险分析中，下列不属于软件资产的是（D）

A、计算机操作系统 B、网络操作系统

C、应用软件源代码 D、外来恶意代码

55、在国家标准中，属于强制性标准的是：（B）

A、GB/T XXXX-X-200X B、GB XXXX-200X

C、DBXX/T XXX-200X D、QXXX-XXX-200X

56、在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（A）

A、当信息安全事件的负面影响扩展到本组织意外时

B、只要发生了安全事件就应当公告

C、只有公众的什么财产安全受到巨大危害时才公告

D、当信息安全事件平息之后

57、在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？（A）

A、标准（Standard） B、安全策略（Security policy）

C、方针（Guideline） D、流程(Proecdure)

58、在信息安全管理工作中“符合性”的含义不包括哪一项？（C）

A、对法律法规的符合 B、对安全策略和标准的符合

C、对用户预期服务效果的符合 D、通过审计措施来验证符合情况

59、在许多组织机构中，产生总体安全性问题的主要原因是（A）。

A、缺少安全性管理 B、缺少故障管理

C、缺少风险分析 D、缺少技术控制机制

60、职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（D）

A、数据安全管理员 B、数据安全分析员

C、系统审核员 D、系统程序员

61、中国电信的岗位描述中都应明确包含安全职责，并形成正式文件记录在案，对于安全职责的描述应包括（D）。

A、落实安全政策的常规职责 B、执行具体安全程序或活动的特定职责

C、保护具体资产的特定职责 D、以上都对

62、终端安全管理目标：规范支撑系统中终端用户的行为，降低来自支撑系统终端的安全威胁，重点解决以下哪些问题？（A）。

A、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

B、终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

C、终端接入和配置管理；桌面及主机设置管理；终端防病毒管理

D、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理

63、著名的橘皮书指的是（A）。

A、可信计算机系统评估标准(TCSEC) B、信息安全技术评估标准（ITSEC）

C、美国联邦标准（FC） D、通用准则（CC）

64、资产的敏感性通常怎样进行划分？（C）

A、绝密、机密、敏感 B、机密、秘密、敏感和公开

C、绝密、机密、秘密、敏感和公开等五类

D、绝密、高度机密、秘密、敏感和公开等五类

65、重要系统关键操作操作日志保存时间至少保存（C）个月。

A、1 B、2 C、3 D、4

66、安全基线达标管理办法规定：BSS系统口令设置应遵循的内控要求是（C）

A、数字+字母 B、数字+字母+符号

C、数字+字母+字母大小写 D、数字+符号

67、不属于安全策略所涉及的方面是（D）。

A、物理安全策略 B、访问控制策略

C、信息加密策略 D、防火墙策略

68、“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（C）。

A、“普密”、“商密”两个级别 B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别

D、“一密”、“二密”，“三密”、“四密”四个级别

69、对MBOSS系统所有资产每年至少进行（A）次安全漏洞自评估。

A、1 B、2 C、3 D、4

70、下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（A）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

71、中国电信各省级公司争取在1-3年内实现CTG-MBOSS 系统安全基线“达标”（C）级以上。

A、A级 B、B级 C、C级 D、D级

72、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

73、获取支付结算、证劵交易、期货交易等网络金融服务的身份认证信息（B）组以上的可以被《中华人民共和国刑法》认为是非法获取计算机信息系统系统认定的“情节严重”。

A、5 B、10 C、-15 D、20

74、基准达标项满（B）分作为安全基线达标合格的必要条件。

A、50 B、60 C、70 D、80

75、《国家保密法》对违法人员的量刑标准是（A）。

A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑

B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑

C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑

D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

76、$HOME/.netrc文件包含下列哪种命令的自动登录信息？（C）

A、rsh B、ssh C、ftp D、rlogin

77、/etc/ftpuser文件中出现的账户的意义表示（A）。

A、该账户不可登录ftp B、该账户可以登录ftp C、没有关系 D、缺少

78、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

79、Linux系统/etc目录从功能上看相当于Windows的哪个目录？（B）

A、program files B、Windows C、system volume information D、TEMP

80、Linux系统格式化分区用哪个命令？（A）

A、fdisk B、mv C、mount D、df

81、在Unix系统中，当用ls命令列出文件属性时，如果显示-rwxrwxrwx,意思是（A）。

A、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示其他用户的访问权限

B、前三位rwx表示文件同组用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

C、前三位rwx表示文件同域用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

D、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示同域用户的访问权限

82、Linux系统通过（C）命令给其他用户发消息。

A、less B、mesg C、write D、echo to

83、Linux中，向系统中某个特定用户发送信息，用什么命令？（B）

A、wall B、write C、mesg D、net send

84、防止系统对ping请求做出回应，正确的命令是：（C）。

A、echo 0>/proc/sys/net/ipv4/icmp\_ehco\_ignore\_all

B、echo 0>/proc/sys/net/ipv4/tcp\_syncookies

C、echo 1>/proc/sys/net/ipv4/icmp\_echo\_ignore\_all

D、echo 1>/proc/sys/net/ipv4/tcp\_syncookies

85、NT/2K模型符合哪个安全级别？（B）

A、B2 B、C2 C、B1 D、C1

86、Red Flag Linux指定域名服务器位置的文件是（C）。

A、etc/hosts B、etc/networks C、etc/rosolv.conf D、/.profile

87、Solaris操作系统下，下面哪个命令可以修改/n2kuser/.profile文件的属性为所有用户可读、科协、可执行？（D）

A、chmod 744 /n2kuser/.profile B、 chmod 755 /n2kuser/.profile

C、 chmod 766 /n2kuser/.profile D、 chmod 777 /n2kuser/.profile

88、如何配置，使得用户从服务器A访问服务器B而无需输入密码？（D）

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhost文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/etc/hosts.equiv文件

89、Solaris系统使用什么命令查看已有补丁列表？（C）

A、uname –an B、showrev C、oslevel –r D、swlist –l product ‘PH??’

90、Unix系统中存放每个用户信息的文件是（D）。

A、/sys/passwd B、/sys/password C、/etc/password D、/etc/passwd

91、Unix系统中的账号文件是（A）。

A、/etc/passwd B、/etc/shadow C、/etc/group D、/etc/gshadow

92、Unix系统中如何禁止按Control-Alt-Delete关闭计算机？（B）

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

93、Unix中。可以使用下面哪一个代替Telnet，因为它能完成同样的事情并且更安全？（B）

A、S-TELNET B、SSH C、FTP D、RLGON

94、Unix中，默认的共享文件系统在哪个位置？（C）

A、/sbin/ B、/usr/local/ C、/export/ D、/usr/

95、Unix中，哪个目录下运行系统工具，例如sh,cp等？（A）

A、/bin/ B、/lib/ C、/etc/ D、/

96、U盘病毒依赖于哪个文件打到自我运行的目的？（A）

A、autoron.inf B、autoexec.bat C、config.sys D、system.ini

97、Windows nt/2k中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

98、Windows 2000目录服务的基本管理单位是（D）。

A、用户 B、计算机 C、用户组 D、域

99、Windows 2000系统中哪个文件可以查看端口与服务的对应？（D）

A、c:\winnt\system\drivers\etc\services B、c:\winnt\system32\services

C、c:\winnt\system32\config\services D、c:\winnt\system32\drivers\etc\services

100、Windows NT/2000 SAM存放在（D）。

A、WINNT B、WINNT/SYSTEM32

C、WINNT/SYSTEM D、WINNT/SYSTEM32/config

101、 Windows NT/2000中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

102、Windows NT的安全标识（SID）串是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是什么？（C）

A、击键速度 B、用户网络地址 C、处理当前用户模式线程所花费CPU的时间 D、PING的响应时间

103、Windows NT和Windows 2000系统能设置为在几次无效登录后锁定账号，可以防止：（B）。

A、木马 B、暴力破解 C、IP欺骗 D、缓冲区溢出攻击

104、Windows主机推荐使用（A）格式。

A、NTFS B、FAT32 C、FAT D、Linux

105、XP当前的最新补丁是（C）。

A、SP1 B、SP2 C、SP3 D、SP4

106、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

107、当你感觉到你的Win2003运行速度明显减慢，当打开任务管理器后发现CPU使用率达到了100%，你认为你最有可能受到了（D）攻击。

A、缓冲区溢出攻击 B、木马攻击 C、暗门攻击 D、DOS攻击

108、档案权限755，对档案拥有者而言，是什么含义？（A）

A、可读，可执行，可写入 B、可读

C、可读，可执行 D、可写入

109、如何配置，使得用户从服务器A访问服务器B而无需输入密码（D）。

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhosts文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/et/hosts.equiv文件

110、要求关机后不重新启动，shutdown后面参数应该跟（C）。

A、–k B、–r C、-h D、 –c

111、一般来说，通过web运行http服务的子进程时，我们会选择（D）的用户用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

112、以下哪项技术不属于预防病毒技术的范畴？（A）

A、加密可执行程序 B、引导区保护

C、系统监控与读写控制 D、校验文件

113、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？（B）

A、缓冲区溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDos攻击

114、与另一台机器建立IPC$会话连接的命令是（D）。

A、net user [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

B、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$) user:Administrator / passwd:aaa

C、net user \192.168.0.1IPC$ D、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

115、在NT中，如果config.pol已经禁止了对注册表的访问，那么黑客能够绕过这个限制吗？怎样实现？（B）

A、不可以 B、可以通过时间服务来启动注册表编辑器

C、可以通过在本地计算机删除config.pol文件 D、可以通过poledit命令

116、在NT中，怎样使用注册表编辑器来严格限制对注册表的访问？（C）

A、HKEY\_CURRENT\_CONFIG,连接网络注册、登录密码、插入用户ID

B、HKEY\_CURRENT\_MACHINE,浏览用户的轮廓目录，选择NTUser.dat

C、HKEY\_USERS,浏览用户的轮廓目录，选择NTUser.dat

D、HKEY\_USERS,连接网络注册，登录密码，插入用户ID

117、在Solaris 8下，对于/etc/shadow文件中的一行内容如下“root:3vd4NTwk5UnLC:9038::::::”,以下说法正确的是：（E）。

A、这里的3vd4NTwk5UnLC是可逆的加密后的密码

B、这里的9038是指从1970年1月1日到现在的天数

C、这里的9038是指从1980年1月1日到现在的天数

D、这里的9038是指从1980年1月1日到最后一次修改密码的天数

E-以上都不正确

118、在Solaris 8下，对于/etc/shadow文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（A）。

A、是/etc/passwd文件格式 B、是/etc/shadow文件格式

C、既不是/etc/passwd也不是/etc/shadow文件格式

D、这个root用户没有SHELL，不可登录

E、这个用户不可登录，并不是因为没有SHELL

119、在Solaris系统中，终端会话的失败登录尝试记录在下列哪个文件里面?(D)

A、-/etc/default/login B、/etc/nologin

C、/etc/shadow D、var/adm/loginlog

120、在Windows 2000中，以下哪个进程不是基本的系统进程:(D)

A、smss. exe B、csrss. Exe C、winlogon. exe D、-conime.exe

121、在Windows 2000中可以察看开放端口情况的是:(D)。

A、nbtstat B、net C、net show D、netstat

122、在Windows 2003下netstat的哪个参数可以看到打开该端口的PID?(C)（格式到此）

A、a B、n C、o D 、p

123、在使用影子口令文件(shadowedpasswords)的Linux系统中，/etc/passwd文件和/etc/shadow文件的正确权限分别是(C)。

A、rw-r-----,-r-------- B、rw-r--r--,-r--r--r—

C、rw-r--r--,-r-------- Drw-r--rw-,-r-----r--

124、制定数据备份方案时，需要重要考虑的两个因素为适合的备份时间和(B)。

A、备份介质 B、备份的存储位置

C、备份数据量 D、恢复备份的最大允许时间

125、周期性行为，如扫描，会产生哪种处理器负荷?(A)

A、Idle Ioad B、Usage Ioad C、Traffic load D、以上都不对

126、主要由于(D)原因，使Unix易于移植

A、Unix是由机器指令书写的 B、Unix大部分由汇编少部分用C语言编写

C、Unix是用汇编语言编写的 D、Unix小部分由汇编大部分用C语言编写

127、HP-UX系统中，使用(A)命令查看系统版本、硬件配置等信息。

A、uname -a B、ifconfig C、netstat D、ps -ef

128、Linux文件权限一共10位长度，分成四段，第三段表示的内容是(C)。

A、文件类型 B、文件所有者的权限

C、文件所有者所在组的权限 D、其他用户的权限

129、在云计算虚拟化应用中，VXLAN技术处于OS工网络模型中2-3层间，它综合了2层交换的简单性与3层路由的跨域连接性。它是通过在UDP/IP上封装Mac地址而实现这一点的。在简单应用场合，vxLAN可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?(C)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

130、Linux中，什么命令可以控制口令的存活时间了(A)。

A、chage B、passwd C、chmod D、umask

131、Qfabric技术是使用市场上现成的计算和存储网元并利用行业标准的网络接口将它们连接后组建大规模的数据中心，以满足未来云计算的要求。该技术概念是哪个厂家主推的概念?(B)

A、惠普 B、uniper C、Cisco与Vmware D、博科Brocade

132、为了检测Windows系统是否有木马入侵，可以先通过(B)命令来查看当前的活动连接端口。

A、ipconfig B、netstat -rn C、tracert –d D、netstat -an

133、网络营业厅提供相关服务的可用性应不低于（A）。

A、99.99% B、99.9% C、99% D、98.9%

134、IRF(Intelligent Resilient Framework)是在该厂家所有数据中心交换机中实现的私有技术，是应用在网络设备控制平面的多虚拟技术。该技术属于哪个厂家?(A)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

135、Windows NT的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:(D)。

A、击键速度 B、当前用户名

C、用户网络地址 D、处理当前用户模式线程所花费CPU的时间

136、脆弱性扫描，可由系统管理员自行进行检查，原则上应不少于(B)。

A、每周一次 B、每月一次 C、每季度一次 D、每半年一次

137、下面哪一个情景属于身份验证(Authentication)过程?(A)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

138、下面哪一个情景属于授权(Authorization)过程?(B)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

139、下列哪一条与操作系统安全配置的原则不符合?(D)

A、关闭没必要的服务 B、不安装多余的组件

C、安装最新的补丁程序 D、开放更多的服务

140、关于DDoS技术，下列哪一项描述是错误的(D)。

A、一些DDoS攻击是利用系统的漏洞进行攻击的

B、黑客攻击前对目标网络进行扫描是发功DDoS攻击的一项主要攻击信息来源

C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的DDoS攻击入侵

D、DDoS攻击不对系统或网络造成任何影响

141、关于PPP协议下列说法正确的是:(C)。

A、PPP协议是物理层协议

B、PPP协议是在HDLC协议的基础上发展起来的

C、PPP协议支持的物理层可以是同步电路或异步电路

D、PPP主要由两类协议组成:链路控制协议族CLCP)和网络安全方面的验证协议族(PAP和CHAP)

142、接口被绑定在2层的zone，这个接口的接口模式是（C）。

A、NAT mode B、Route mode

C、-Transparent mode D、NAT或Route mode

143、接入控制方面，路由器对于接口的要求包括：（D）。

A、串口接入 B、局域网方式接入 C、Internet方式接入 D、VPN接入

144、局域网络标准对应OSI模型的哪几层？（C）。

A、上三层 B、只对应网络层 C、下三层 D、只对应物理层

145、拒绝服务不包括以下哪一项？（D）。

A、DDoS B、畸形报文攻击 C、Land攻击 D、ARP攻击

146、抗DDoS防护设备提供的基本安全防护功能不包括（A）。

A、对主机系统漏洞的补丁升级 B、检测DDoS攻击

C、DDoS攻击警告 D、DDoS攻击防护

147、路由器产品提供完备的安全架构以及相应的安全模块，在软、硬件层面设置重重过滤，保护路由器业务安全。其中不对的说法是：（C）。--》缺少D选项

A、路由器产品支持URPF，可以过滤大多数虚假IP泛洪攻击

B、路由器产品支持CAR功能，可以有效限制泛洪攻击

C、路由器产品不支持ACL配置功能，不能定制过滤规则

D、

148、路由器对于接入权限控制，包括：（D）。

A、根据用户账号划分使用权限 B、根据用户接口划分使用权限

C、禁止使用匿名账号 D、以上都是

149、路由器启动时默认开启了一些服务，有些服务在当前局点里并没有作用，对于这些服务：（C）。缺少D选项

A、就让他开着，也耗费不了多少资源 B、就让他开着，不会有业务去访问

C、必须关闭，防止可能的安全隐患 D、

150、设置Cisco设备的管理员账号时，应（C）。

A、多人共用一个账号 B、多人共用多个账号

C、一人对应单独账号 D、一人对应多个账号

151、什么命令关闭路由器的finger服务？（C）

A、disable finger B、no finger C、no finger service D、no service finger

152、什么是IDS？（A）

A、入侵检测系统 B、入侵防御系统 C、网络审计系统 D、主机扫描系统

153、实现资源内的细粒度授权，边界权限定义为：（B）。

A、账户 B、角色 C、权限 D、操作

154、使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）

A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

155、使用TCP 79端口的服务是：（D）。

A、telnet B、SSH C、Web D、Finger

156、使用一对一或者多对多方式的NAT转换，当所有外部IP地址均被使用后，后续的内网用户如需上网，NAT转换设备会执行什么样的动作？（C）

A、挤掉前一个用户，强制进行NAT转换 B、直接进行路由转发

C、不做NAT转换 D、将报文转移到其他NAT转换设备进行地址转换

157、私网地址用于配置本地网络、下列地址中属于私网地址的是？（C）

A、100.0.0.0 B、172.15.0.0 C、192.168.0.0 D、244.0.0.0

158、随着Internet发展的势头和防火墙的更新，防火墙的哪些功能将被取代。（D）

A、使用IP加密技术 B、日志分析工作

C、攻击检测和报警 D、对访问行为实施静态、固定的控制

159、随着安全要求的提高、技术的演进，（D）应逐步实现物理隔离，或者通过采用相当于物理隔离的技术（如MPLSVPN）实现隔离。

A、局域网 B、广域网及局域网 C、终端 D、广域网

160、通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出现崩溃，请问这种攻击属于何种攻击？（D）

A、拒绝服务（DoS）攻击 B、扫描窥探攻击

C、系统漏洞攻击 D、畸形报文攻击

161、通信领域一般要求3面隔离，即转发面、控制面、用户面实现物理隔离，或者是逻辑隔离，主要目的是在某一面受到攻击的时候，不能影响其他面。路由器的安全架构在实现上就支持：（D）

A、转发面和控制面物理隔离 B、控制面和用户面逻辑隔离

C、转发面和用户面逻辑隔离 D、以上都支持

162、网管人员常用的各种网络工具包括telnet、ftp、ssh等，分别使用的TCP端口号是（B）。

A、21、22、23 B、23、21、22 C、23、22、21 D、21、23、22

163、网络安全工作的目标包括：（D）。

A、信息机密性 B、信息完整性 C、服务可用性 D、以上都是

164、网络安全在多网合一时代的脆弱性体现在（C）。

A、网络的脆弱性 B、软件的脆弱性 C、管理的脆弱性 D、应用的脆弱性

165、应限制Juniper路由器的SSH（A），以防护通过SSH端口的DoS攻击。

A、并发连接数和1分钟内的尝试连接数 B、并发连接数

C、1分钟内的尝试连接数 D、并发连接数和3分钟内的尝试连接数

166、应用网关防火墙的逻辑位置处在OSI中的哪一层？（C）

A、传输层 B、链路层 C、应用层 D、物理层

167、应用网关防火墙在物理形式上表现为？（B）

A、网关 B、堡垒主机 C、路由 D、交换机

168、用来追踪DDoS流量的命令式：（C）

A、ip source-route B、ip cef C、ip source-track D、ip finger

169、用于保护整个网络IPS系统通常不会部署在什么位置？（D）

A、网络边界 B、网络核心 C、边界防火墙内 D、业务终端上

170、用于实现交换机端口镜像的交换机功能是：（D）

A、PERMIT LIST B、PVLAN C、VTP D、SPAN

171、有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（D）。

A、L2TP是由PPTV协议和Cisco公司的L2F组合而成

B、L2TP可用于基于Internet的远程拨号访问

C、为PPP协议的客户建立拨号连接的VPN连接

D、L2TP只能通过TCP/IP连接

172、有关PPTP（Point-to-Point Tunnel Protocol）说法正确的是（C）。

A、PPTP是Netscape提出的 B、微软从NT3.5以后对PPTP开始支持

C、PPTP可用在微软的路由和远程访问服务上 D、它是传输层上的协议

173、有一些应用，如微软Out look或MSN。它们的外观会在转化为基于Web界面的过程中丢失，此时要用到以下哪项技术：（B）

A、Web代理 B、端口转发 C、文件共享 D、网络扩展

174、预防信息篡改的主要方法不包括以下哪一项？（A）

A、使用VPN技术 B、明文加密 C、数据摘要 D、数字签名

175、域名服务系统（DNS）的功能是（A）。

A、完成域名和IP地址之间的转换 B、完成域名和网卡地址之间的转换

C、完成主机名和IP地址之间的转换 D、完成域名和电子邮件地址之间的转换

176、源IP为100.1.1.1，目的IP为100.1.1.255，这个报文属于什么攻击？（B）（假设该网段掩码为255.255.255.0）

A、LAND攻击 B、SMURF攻击 C、FRAGGLE攻击 D、WINNUKE攻击

177、在AH安全协议隧道模式中，新IP头内哪个字段无需进行数据完整性校验？（A）

A、TTL B、源IP地址 C、目的IP地址 D、源IP地址+目的IP地址

178、在C/S环境中，以下哪个是建立一个完整TCP连接的正确顺序？（D）

A、SYN，SYN/ACK，ACK B、Passive Open,Active Open,ACK,ACK

C、SYN,ACK/SYN,ACK D、Active Open/Passive Open,ACK,ACK

179、在L2TP应用场景中，用户的私有地址分配是由以下哪个组建完成？（B）

A、LAC B、LNS C、VPN Client D、用户自行配置

180、在OSI模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（A）

A、应用层 B、物理层 C、会话层 D、网络层

181、在OSI参考模型中有7个层次，提供了相应的安全服务来加强信息系统的安全性。以下哪一层提供了抗抵赖性？（B）

A、表示层 B、应用层 C、传输层 D、数据链路层

182、在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（B）

A、产生日志的数量 B、攻击减少的速度

C、较低的价格 D、假阳性的减少量

183、在安全审计的风险评估阶段，通常是按什么顺序来进行的？（A）

A、侦查阶段、渗透阶段、控制阶段 B、渗透阶段、侦查阶段、控制阶段

C、控制阶段、侦查阶段、渗透阶段 D、侦查阶段、控制阶段、渗透阶段

184、在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（D）

A、IETF 因特网工程工作小组 B、ISO 国际标准组织

C、IANA 因特网地址指派机构 D、OSI 开放系统互联

185、在传输模式IPSec应用情况中，以下哪个区域数据报文可受到加密安全保护？（D）

A、整个数据报文 B、原IP头 C、新IP头 D、传输层及上层数据报文

186、在点到点链路中，OSPF的Hello包发往以下哪个地址？（B）

A、127.0.0.1 B、224.0.0.5 C、233.0.0.1 D、255.255.255.255

187、在建立堡垒主机时，（A）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

188、在进行Sniffer监听时，系统将本地网络接口卡设置成何种侦听模式？（D）

A、unicast单播模式 B、Broadcast广播模式

C、Multicast组播模式 D、Promiscuous混杂模式

189、在零传输（Zone transfers）中DNS服务使用哪个端口？（A）

A、TCP 53 B、UDP 53 C、UDP 23 D、TCP23

190、在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（C）

A、入网访问控制 B、权限控制 C、网络检测控制 D、防火墙控制

191、在思科设备上，若要查看所有访问表的内容，可以使用的命令式（B）

A、show all access-lists B、show access-lists

C、show ip interface D、show interface

192、在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的这是对（A）。

A、可用性的攻击 B、保密性的攻击 C、完整性的攻击 D、真实性的攻击

193、在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（C）

A、报文服务拒绝 B、假冒 C、数据流分析 D、报文服务更改

194、在以下OSI七层模型中，synflooding攻击发生在哪层？（C）

A、数据链路层 B、网络层 C、传输层 D、应用层

195、在以下哪类场景中，移动用户不需要安装额外功能（L2TP）的VPDN软件？（B）

A、基于用户发起的L2TP VPN B、基于NAS发起的L2TP VPN

C、基于LNS发起的L2TP VPN D、以上都是

196、账户口令管理中4A的认证管理的英文单词为：（B）

A、Account B、Authentication C、Authorization D、Audit

197、只具有（A）和FIN标志集的数据包是公认的恶意行为迹象。

A、SYN B、date C、head D、标志位

198、主从账户在4A系统的对应关系包含：（D）

A、1 -N B、1 -1 C、N -1 D、以上全是

199、主动方式FTP服务器要使用的端口包括（A）。

A、TCP 21 TCP 20 B、TCP21 TCP大于1024的端口

C、TCP 20、TCP 大于1024端口 D、都不对

200、下列（D）因素不是影响IP电话语音质量的技术因素。

A、时延 B、抖动 C、回波 D、GK性能

201、下列安全协议中使用包括过滤技术，适合用于可信的LAN到LAN之间的VPN（内部VPN）的是（D）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

202、下列不是抵御DDoS攻击的方法有（D）。

A、加强骨干网设备监控 B、关闭不必要的服务

C、限制同时打开的Syn半连接数目 D、延长Syn半连接的time out时间

203、下列措施不能增强DNS安全的是（C）。

A、使用最新的BIND工具 B、双反向查找

C、更改DNS的端口号 D、不要让HINFO记录被外界看到

204、下列各种安全协议中使用包过滤技术，适合用于可信的LAN到LAN之间的VPN，即内部网VPN的是（D）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

205、下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适？（D）

A、回应的比例 B、被动的防御 C、主动的防御 D、都不对

206、下列哪项是私有IP地址？（A）

A、10.5.42.5 B、172.76.42.5 C、172.90.42.5 D、241.16.42.5

207、下列哪一项能够提高网络的可用性？（B）

A、数据冗余 B、链路冗余 C、软件冗余 D、电源冗余

208、下列哪一种攻击方式不属于拒绝服务攻击：（A）。

A、LOphtCrack B、Synflood C、Smurf D、Ping of Death

209、下列哪一项是arp协议的基本功能？（A）

A、通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行

B、对局域网内的其他机器广播路由地址

C、过滤信息，将信息传递个数据链路层 D、将信息传递给网络层

210、最早的计算机网络与传统的通信网络最大的区别是什么？（A）

A、计算机网络采用了分组交换技术 B、计算机网络采用了电路交换技术

C、计算机网络的可靠性大大提高 D、计算机网络带宽和速度大大提高

211、以下哪个属于IPS的功能？（A）

A、检测网络攻击 B、网络流量检测 C、实时异常告警 D、以上都是

212、以下说法错误的是（C）。

A、安全是一个可用性与安全性之间的平衡过程 B、安全的三要素中包含完整性

C、可以做到绝对的安全 D、网络安全是信息安全的子集

213、以下属于4A策略管理模块可以管理的为（C）。

A、访问控制策略 B、信息加密策略 C、密码策略 D、防火墙策略

214、最早研究计算机网络的目的是什么？（B）

A、共享硬盘空间、打印机等设备 B、共享计算资源

C、直接的个人通信 D、大量的数据交换

215、防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为（C）。

A、内容过滤 B、地址转换 C、透明代理 D、内容中转

216、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）。

A、防火墙 B、CA中心 C、加密机 D、防病毒产品

217、网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（D）。

A、多重安全网关 B、防火墙 C、Vlan隔离 D、物理隔离

218、下列哪项不是Tacacs+协议的特性。（A）

A、扩展记账 B、加密整个数据包 C、使用TCP D、支持多协议

219、一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（A）

A、最小特权 B、阻塞点 C、失效保护状态 D、防御多样化

220、包过滤防火墙工作的好坏关键在于？（C）

A、防火墙的质量 B、防火墙的功能 C、防火墙的过滤规则设计 D、防火墙的日志

221、对于日常维护工作，连接路由器的协议通常使用：（B）。缺少D选项

A、TELNET，简单，容易配置 B、SSH &SSHv2 加密算法强劲，安全性好

C、TELNET配置16位长的密码，加密传输，十分安全 D、

222、BOTNET是（C）。

A、普通病毒 B、木马程序 C、僵尸网络 D、蠕虫病毒

223、监听的可能性比较低的是（B）数据链路。

A、Ethernet B、电话线 C、有线电视频道 D、无线电

224、当IPS遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（B）。

A、pass B、bypass C、watchdog D、HA

225、网络环境下的security是指（A）。

A、防黑客入侵，防病毒，窃取和敌对势力攻击

B、网络具有可靠性，可防病毒，窃密和敌对势力攻击

C、网络具有可靠性，容灾性，鲁棒性

D、网络的具有防止敌对势力攻击的能力

226、某一案例中，使用者已将无线AP的SSID广播设置为禁止，并修改了默认SSID值，但仍有未经授权的客户端接入该无线网络，这是因为（D）

A、禁止SSID广播仅在点对点的无线网络中有效

B、未经授权客户端使用了默认SSID接入

C、无线AP开启了DHCP服务

D、封装了SSID的数据包仍然会在无线AP与客户端之间传递

227、为了保护DNS的区域传送（zone transfer），应该配置防火墙以阻止（B）。

1.UDP

2.TCP

3.53

4.52

A、1,3 B、2,3 C、1,4 D、2,4

228、以下不属于代理服务技术优点的是（D）。

A、可以实现身份认证 B、内部地址的屏蔽盒转换功能

C、可以实现访问控制 D、可以防范数据驱动侵袭

229、应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（C）。

A、60% B、70% C、80% D、90%

230、TCP协议与UDP协议相比，TCP是（B），UDP是（）。

A、设置起来麻烦；很好设置 B、容易；困难

C、面向连接的；非连接的 D、不可靠的；可靠的

231、交换机转发以太网的数据基于：（B）。

A、交换机端口号 B、MAC地址 C、IP地址 D、数据类别

232、HTTP，FTP，SMTP建立在OSI模型的哪一层？（D）

A、2层-数据链路层 B、3层-网络层 C、4层-传输层 D、7层-应用层

233、网络安全的基本属性是（D）。

A、机密性 B、可用性 C、完整性 D、以上都是

234、网络安全的主要目的是保护一个组织的信息资产的（A）。

A、机密性、完整性、可用性 B、参照性、可用性、机密性、

C、可用性、完整性、参照性 D、完整性、机密性、参照性

235、DBS是采用了数据库技术的计算机系统。DBS是一个集合体，包含数据库、计算机硬件、软件和（C）。

A、系统分析员 B、程序员 C、数据库管理员 D、操作员

236、MySQL -h host -u user -p password命令的含义如下，哪些事正确的？（D）

A、-h后为host为对方主机名或IP地址 B、-u后为数据库用户名

C、-p后为密码 D、以上都对

237、Oracle当连接远程数据库或其它服务时，可以指定网络服务名，Oracle9i支持5中命名方法，请选择错误的选项。（D）

A、本地命名和目录命名 B、Oracle名称（Oracle Names）

C、主机命名和外部命名 D、DNS和内部命名

238、Oracle的数据库监听器（LISTENER）的默认通讯端口是？（A）

A、TCP 1521 B、TCP 1025 C、TCP 1251 D、TCP 1433

239、Oracle默认的用户名密码为（A）。

A、Scote/tiger B、root C、null D、rootroot

240、Oracle数据库中，物理磁盘资源包括哪些（D）。

A、控制文件 B、重做日志文件 C、数据文件 D、以上都是

241、Oracle中启用审计后，查看审计信息的语句是下面哪一个？（C）

A、select \* from SYS.AUDIT$ B、select \* from syslogins

C、select \* from SYS.AUD$ D、AUDIT SESSION

242、SMTP的端口？（A）

A、25 B、23 C、22 D、21

243、SQL Server的登录账户信息保存在哪个数据库中？（C）

A、model B、msdb C、master D、tempdb

244、SQL Sever的默认DBA账号是什么？（B）

A、administrator B、sa C、root D、SYSTEM

245、SQL Sever的默认通讯端口有哪些？（B）

A、TCP 1025 B、TCP 1433 C、UDP 1434 D、TCP 14333 E、TCP 445

246、SQL Sever中可以使用哪个存储过程调用操作系统命令，添加系统账号？（B）

A、xp\_dirtree B、xp\_cmdshell C、xp\_cmdshell D、xpdeletekey

247、SQL Sever中下面哪个存储过程可以执行系统命令？（C）

A、xp\_regread B、xp\_command C、xp\_cmdshell D、sp\_password

248、SQL的全局约束是指基于元祖的检查子句和（C）。

A、非空值约束 B、域约束子句 C、断言 D、外键子句

249、SQL数据库使用以下哪种组件来保存真实的数据？（C）

A、Schemas B、Subschemas C、Tables D、Views

250、SQL语句中，彻底删除一个表的命令是（B）。

A、delete B、drop C、clear D、remore

251、SQL语言可以（B）在宿主语言中使用，也可以独立地交互式使用。

A、-极速 B、-嵌入 C、-混合 D、-并行

252、SSL安全套接字协议所用的端口是（B）。

A、80 B、443 C、1433 D、3389

253、不属于数据库加密方式的是（D）。

A、库外加密 B、库内加密 C、硬件/软件加密 D、专用加密中间件

254、测试数据库一个月程序主要应对的风险是（B）。

A、非授权用户执行“ROLLBACK”命令 B、非授权用户执行“COMMIT”命令

C、非授权用户执行“ROLLRORWARD”命令 D、非授权用户修改数据库中的行

**255、查看Oracle 8i及更高版本数据库的版本信息的命令是（C）。----缺少CD选项**

**A、cd $Oracle\_HOME/orainst B、C-cd $Oracle\_HIME/orainst C、 D、**

256、从安全的角度来看，运行哪一项起到第一道防线的作用？（C）

A、远端服务器 B、WEB服务器 C、防火墙 D、使用安全shell程序

257、从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（B）。

A、每个分割区G有g=|G|记录，其中g=0或g>=n，且g为偶数，

B、记录必须成对地加入G或从G中删除

C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从m各分割区G1，G2，… …Gm中每一个分割区而来的，则统计信息g（G1VG2V… …VGm）是允许发布

D、记录必须不对地加入G或从G中删除

258、单个用户使用的数据库视图的描述为（A）。

A、外模式 B、概念模式 C、内模式 D、存储模式

259、对于IIS日志记录，推荐使用什么文件格式？（D）

A、Microsoft IIS日志文件格式 B、NCSA公用日志文件格式

C、ODBC日志记录格式 D、W3C扩展日志文件格式

**260、对于IIS日志文件的存放目录，下列哪项设置是最好的？（D）----缺少D选型**

**A、%WinDir%\System32\LogFiles B、C:\Inetpub\wwwroot\LogFiles**

**C、C:\LogFiles..)-F:\LogFiles D、**

261、对于IIS日志文件的访问权限，下列哪些设置是正确的？（D）

A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）

B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）

C、SYSTEM（完全控制）Administrator（完全控制）Inernet来宾账户（读取和运行） D、SYSTEM（完全控制）Administrator（完全控制）

262、对于数据库的描述一下哪项说法是正确的？（A）

A、数据和一系列规则的集合 B、一种存储数据的软件

C、一种存储数据的硬件 D、是存放人量数据的软件

263、攻击者可能利用不必要的extproc外部程序调用功能获取对系统的控制权，威胁系统安全。关闭Extproc功能需要修改TNSNAMES.ORA和LISTENER.ORA文件删除一下条目，其中有一个错误的请选择出来（A）。

A、sys\_ertproc B、icache\_extproc

C、PLSExtproc D、extproc

264、关系数据库中，实现实体之间的联系是通过表与表之间的（D）。

A、公共索引 B、公共存储

C、公共元组 D、公共属性

265、关系型数据库技术的特征由一下哪些元素确定的？（A）

A、行和列 B、节点和分支

C、Blocks和Arrows D、父类和子类

266、关于WEB应用软件系统安全，说法正确的是（D）？

A、Web应用软件的安全性仅仅与WEB应用软件本身的开发有关

B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C、黑客的攻击主要是利用黑客本身发现的新漏洞

D、以任何违反安全规定的方式使用系统都属于入侵

267、目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（D）？

A、数据库系统庞大会提供管理成本 B、数据库系统庞大会降低管理效率

C、数据的集中会降低风险的可控性 D、数据的集中会造成风险的集中

268、哪一个是PKI体系中用以对证书进行访问的协议（B）？

A、SSL B、LDAP C、CA D、IKE

269、如果一个SQL Server数据库维护人员，需要具有建立测试性的数据库的权限，那么应该指派给他哪个权限（A）？

A、Database Creators B、System Administrators

C、Server Administrators D、Security Adiministrators

270、如果以Apache 为WWW服务器，（C）是最重要的配置文件。

A、access.conf B、srm.cong C、httpd.conf D、mime.types

271、若有多个Oracle数据需要进行集中管理，那么对sysdba的管理最好选择哪种认证方式（B）？

A、系统认证 B、password文件认证方式 C、域认证方式 D、以上三种都可

272、数据库管理系统DBMS主要由哪两种部分组成？（A）

A、文件管理器和查询处理器 B、事务处理器和存储管理器

C、存储管理器和查询处理器 D、文件管理器和存储管理器

273、数据库系统与文件系统的最主要区别是（B）。

A、数据库系统复杂，而文件系统简单

B、文件系统不能解决数据冗余和数据独立性问题，而数据库系统可以解决

C、文件系统只能管理程序文件，而数据库系统能够管理各宗类型的文件

D、文件系统管理的数据量较少，而数据库系统可以管理庞大的数据量

274、为了防止电子邮件中的恶意代码，应该由（A）方式阅读电子邮件。

A、纯文本 B、网页 C、程序 D、会话

275、为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机（D）？

A、SMTP身份认证 B、逆向名字解析 C、黑名单过滤 D、内容过滤

276、为什么要对数据库进行“非规范化”处理（B）？

A、确保数据完整性 B、增加处理效率 C、防止数据重复 D、节省存储空间

277、下列不属于WEB安全性测试的范畴的是（A）？

A、数据库内容安全性 B、客户端内容安全性

C、服务器端内容安全性 D、日志功能

278、下列操作中，哪个不是SQL Server服务管理器功能（A）？

A、执行SQL查询命令 B、停止SQL Server 服务

C、暂停SQL Server服务 D、启动SQL Server服务

279、下列关于IIS的安全配置，哪些是不正确的（C）？

A、将网站内容移动到非系统驱动程序 B、重命名IUSR账户

C、禁用所有WEB服务扩展 D、创建应用程序池

280、下列哪些不是广泛使用http服务器？（D）

A、W3C B、Apache C、IIS D、IE

281、下列哪些属于WEB脚本程序编写不当造成的（C）？

A、IIS5.0 Webdav Ntdll.dll远程缓冲区一处漏洞

B、apache可以通过../../../../../../../etc/passwd方位系统文件

C、登陆页面可以用password=’a’or’a’=’a’绕过

D、数据库中的口令信息明文存放

282、下列哪种方法不能有效的防范SQL进入攻击（C）？

A、对来自客户端的输入进行完备的输入检查

B、把SQL语句替换为存储过程、预编译语句或者使用ADO命令对象

C、使用SiteKey技术

D、关掉数据库服务器或者不使用数据库

283、下列哪种工具不是WEB服务器漏洞扫描工具（B）？

A、Nikto B、Web Dumper C、paros Proxy D、Nessus

284、下列哪种攻击不是针对统计数据库的（D）？

A、小查询集合大查询集攻击 B、中值攻击 C、跟踪攻击 D、资源解析攻击

285、下列哪项中是数据库中涉及安全保密的主要问题（A）？

A、访问控制问题 B、数据的准确性问题

C、数据库的完整性问题 D、数据库的安全性问题

286、下列应用服务器中，不遵循J2EE规范的是（C）？

A、MTS B、WebLogic C、Oracle 9iApplication Server D、WebSpere

287、下面关于IIS报错信息含义的描述正确的是（B）？

A、401-找不到文件 B、403-禁止访问 C、404-权限问题 D、500-系统错误

288、下面关于Oracle进程的描述，哪项是错误的（B）？

A、运行在Windows平台上的Oracle能让每个用户组程序化地打开新的进程，这是一个安全隐患

B、在Windows平台，除了Oracle.exe进程外还有其他的独立进程

C、unix平台上有多个独立运行的进程，包括数据写进程、日志写进程、存档进程、系统监控进程、进程监控进程

D、有一个特殊的内存区域被映射为\*nix平台上的所有进程，此区域时系统全局去

289、下面哪一项是与数据库管理员（DBA）职责不相容的（C）？

A、数据管理 B、信息系统管理 C、系统安全 D、信息系统规划

290、下面选型中不属于数据库安全控制的有（D）。

A、信息流控制 B、推论控制 C、访问控制 D、隐通道控制

291、下面选型中不属于数据库安全模型的是（D）。

A、自主型安全模型 B、强制型安全模型 C、基于角色的模型 D、访问控制矩阵

292、一般来说，通过WEB运行http服务的子进程时，我们会选择（D）的用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

293、一下不是数据库的加密技术的是（D）。

A、库外加密 B、库内加密 C、硬件加密 D、固件加密

294、一下对于Oracle文件系统描述错误的是（B）？

A、\*nix下Oracle的可执行文件在$Oracle\_HOME/bin/Oracle,$Oracle\_HOME/bin也应该包含在路径环境变量内

B、Windows下Oracle的可执行文件在%Oracle\_HOME%\bin\Oracle.exe,其他

C、硬件加密 D、固件加密

295、以下几种功能中，哪个是DBMS的控制功能（A）？

A、数据定义 B、数据恢复 C、数据修改 D、数据查询

296、以下哪个安全特征和机制是SQL数据库所特有的（B）？

A、标识和鉴别 B、数据恢复 C、数据修改 D、数据查询

297、以下哪个是数据库管理员（DBA）可以行使的职责（A）？

A、系统容量规划 B、交易管理 C、审计 D、故障承受机制

298、以下哪条命令能利用“SQL注入”漏洞动用XP\_cmdshell存储过程，获得某个子目的清单？（A）

A、http://localhost/script?’:EXEC+master..XP\_cmdshell+’dir’:--

B、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’:--

C、http://localhost/script?0’:EXEC+master..XP\_cmdshell+’ dir’:--

D、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’--

299、以下哪条命令能利用“SQL”漏洞动用XP\_cmdshell存储过程，启动或停止某项服务？（B）

A、http://localhost/script?’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;-

B、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;--

C、http://localhost/script?1’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ; --

D、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ --

300、以下哪项不属于访问控制策略的实施方式？（D）

A、子模式法 B、修改查询法 C、集合法 D、验证法

301、以下哪一项是和电子邮件系统无关的？（）

A、PEM(Privacy enhanced mail) B、PGP(Pretty good privacy)

C、X.500 D、X.400

302、以下哪种方法可以用于对付数据库的统计推论？（C）

A、信息流控制 B、共享资源矩阵 C、查询控制 D、间接存取

303、以下是对层次数据库结构的描述，请选择错误描述的选项。（C）

A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来

B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据

C、它的优点是用户不需要十分熟悉数据库结构

D、层次数据库模型的结构就像是一棵倒转的树

304、以下是对单用户数据库系统的描述，请选择错误描述的选项（C）。

A、单用户数据库系统是一种早期的最简单的数据库系统

B、在单用户系统中，整个数据库系统，包括应用程序、DBMS、数据，都装在一台计算机之间不能共享数据

C、在单用户系统中，由多个用户共用，不同计算机之间能共享数据

D、单用户数据库系统已经不适用于现在的使用，被逐步淘汰了

305、以下是对分布式结构数据库系统的描述，请选择错误描述的选项。（D）

A、分布式结构的数据库系统的数据在逻辑上是一个整体，但物理地分布在计算机网络的不同节点上，每个节点上的主机又带有多个终端用户

B、网络中的每个节点都可以独立的处理数据库中的数据，执行全局应用

C、分布式结构的数据库系统的数据分布存放给数据的处理、管理和维护带来困难

D、分布式结构的数据库系统的数据只在存放在服务器端，其他节点只进行处理和执行

306、以下是对关系数据库结构的描述，请选择错误描述的选项。（D）

A、数据存储的主要载体是表，或相关数据组

B、有一对一、一对多、多对多三种表关系

C、表关联是通过引用完整性定义的，这是通过主码和外码（主键或外键约束条件实现的）

D、缺点是不支持SQL语言

307、以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（A）

A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力

B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行DBMS功能又执行应用程序

C、在网络中把某些节点的计算机专门用于执行DBMS核心功能，这台计算机就成为数据库服务器

D、其他节点上的计算机安装DBMS外围应用开发工具和应用程序，支持用户的应用，称为客户机

308、以下是对面向对象数据库结构的描述，请选择错误描述的选项。（C）

A、它允许用对象的概念来定义与关系数据库交互

B、面向对象数据库中有两个基本的结构：对象和字面量

C、优点是程序员需要掌握与面向对象概念以及关系数据库有关的存储

D、缺点是用户必须理解面向对象概念，目前还没有统一的标准，稳定性还是一个值得关注的焦点

309、以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（D）

A、主从式结构是指一个主机带多个终端的多用户结构

B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上

C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源

D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈

311、在GRUB的配置文件grub.conf中，“timeout=-1”的含义是（C）。

A、不等待用户选择，直接启动默认的系统

B、在10秒钟内，等待用户选择要启动的系统

C、一直等待用户选择要启动的系统

D、无效

312、在Oracle中，quota可以限制用户在某个表空间上最多可使用多少字节，如果要限制data\_ts表500K，以下哪个是正确的命令？（B）

A、quo 500k in data\_ts B、quota 500K on data\_ts

C、quota data\_ts ,imit 500K D、quota data\_ts on 500K

313、在Oracle中，建表约束包括引用完整性约束、check完整性约束，还有以下三项是正确的，请排除一个错误选项。（D）

A、非空完整性约束 B、唯一完整性约束

C、主码完整性约束 D、数据角色性约束

314、在Oracle中，将scott的缺省表空间改为data2\_ts，下列哪个是正确的？（A）

A、ALTER USER scott DEFAULT TABLESPACE data2\_ts

B、ALTER DEFAULT TABLESPACE data2\_ts USER scott

C、ALTER USER scott TABLESPACE DEFAULT data2\_ts D、ALTER scott USER DEFAULT TABLESPACE data2\_ts

315、在Oracle中，将scott的资源文件改为otherprofile，下列哪个是正确的？（C）

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

316、在Oracle中，将当前系统所有角色都授予scott，除Payroll外，下列哪个是正确的？（D）

A、ALTER DEFAULT ROLLE USER　　scott ALL EXCEPT Payroll

B、ALTER USER DEFAULT ROLLE ALL EXCEPT Payroll

C、ALTER DEFAULT ROLLE ALL EXCEPT USER scott

D、ALTER USER scott DEFAULT ROLLE ALL EXCEPT Payroll

317、在Oracle中，用ALTER将scott的口令改为hello，下列哪个是正确的？（A）

A、ALTER USER scott IDENTIFIED BY hello

B、ALTER scott USER IDENTIFIED BY hello

C、ALTER USER scott IDENTIFIED AS hello

D、ALTER USER hello IDENTIFIED BY scott

318、在WEB应用软件的基本结构中，客户端的基础是（A）。

A、HTML文档 B、客户端程序

C、HTML协议 D、浏览器

319、在WEB应用软件的系统测试技术中，下面不属于安全性测试内容的是（C）。

A、客户端的内容安全性 B、服务器的内容安全性

C、数据库的内容安全性 D、Cookie安全性

320、在典型的WEB应用站点的层次结构中，“中间件”是在哪里运行的？（C）

A、浏览器客户端 B、web服务器

C、应用服务器 D、数据库服务器

321、在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（C）

A、对话管理服务 B、事务管理服务

C、资源管理服务 D、控制管理服务

322、主要用于加密机制的协议时（D）。

A、HTTP B、FTP C、TELNETD D、SSL

323、分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？（D）

A、自主性 B、可靠性 C、灵活性 D、数据备份

324、下面对Oracle的密码规则描述，哪个是错误的？（D）

A、Oracle密码必须由英文字母，数值，#，下划线(\_)，美元字符（$）构成，密码的最大长度为30字符，并不能以“$”，“#”，“\_”或任何数字卡头；密码不能包含像“SELECT”，“DELETE”，“CREATE”这类的ORACLE/SQL关键字

B、Oracle的若算法加密机制（）两个相同的用户名和密码在两台不同的ORACLE数据库机器中，将具有相同的哈希值。这些哈希值存储在SYS.USER表中，可以通过像DBA\_USE这类的试图来访问

C、Oracle默认配置下，每个中户如果有10此的失败登录，此账户将会被锁定

D、SYS账户在Oracle数据库中有最高权限，能够做任何事情，包括启动/关闭Oracle数据库，如果SYS被锁定，将不能访问数据库

325、无论是哪一种Web服务器，都会受到HTTP协议本身安全问题的困扰，这样的信息系统安全漏洞属于（C）。

A、设计型漏洞 B、开发型漏洞 C、运行型漏洞 D、以上都不是

326、SSL加密的过程包括以下步骤：（1）通过验证以后，所有数据通过密钥进行加密，使用DEC和RC4加密进行加密；（2）随后客户端随机生成一个对称密钥；（3）信息通过HASH加密，或者一次性加密（MD5SHA）进行完整性确认；（4）客户端和服务器协商建立加密通道的特定算法。正确的顺序的是（D）

A、（4）（3）（1）（2） B、（4）（1）（3）（2） C、（4）（2）（3）（1） D、（4）（2）（3）（1）

327、影响WEB系统安全的因素，不包括？（C）

A、复杂应用系统代码量大、开发人员多、难免出现疏忽

B、系统屡次升级、人员频繁变更，导致代码不一致

C、历史遗留系统、试运行系统等对个WEB系统运行于不同的服务器上

D、开发人员未经安全编码培训

328、Oracle通过修改用户密码策略可提高密码强度，以下哪个密码策略参数中文描述是错误的？（A）

A、PASSWORD\_MAX 登录超过有效次数锁定时间

B、FAILED\_LOGIN\_ATTEMPTS 最大错误登录次数

C、PASSWORD\_GRACE\_TIME 密码失效后锁定时间

D、PASSWORD\_LIFE\_TIME 口令有效时间

329、SQL Server服务有一个启动账号，默认账号是属于administrators组，现在为了安全需要创建一个新的服务启动账号，它需要哪些权限既能兼顾安全又能保证启动数据库成功，请排除一个错误的。（D）

A、数据库本地目录的读写权限 B、启动本地服务的权限

C、读取注册表的权限 D、通过API访问Windows Resource

330、作为一台运行IIS 在Internet发布站点的Windows Web服务器，下面哪项服务不是必需的？（B）

A、IIS Admin B、Net Logon

C、Performance Logs and Alerts D、World Wide Web Publishing

331、数据库中超级账户不能被锁定，其中Oracle的是（），mysql的是（），SQLServer的是（C）。

A、sa，root，sys B、admin，root，sa

C、sys，root，sa D、sys，admin，sa

332，Oracle的安全机制，是由（A）、实体权限和角色权限这三级体系结构组成的。

A、系统权限 B、索引权限 C、操作权限 D、命令控制

333、对SQL数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（B）

A、-- B、- C、-= D、-+

334、在Web页面中增加验证码功能后，下面说法正确的是（A）。

A、可以增加账号破解等自动化软件的攻击难度 B、可以防止文件包含漏洞 C、可以防止缓冲溢出 D、可以防止 浏览

335、以下破解Oracle密码哈希值的步棸，其中哪个描述是错误的？（B）

A、用Sqlplus直接登录到Oracle数据库，使用select username，password form dba\_users命令查看数据库中的用户名和密码，此时看到的密码是哈希值

B、在Cain的Cracker菜单点击导入用户名和哈希值，可直接显示用户密码明文

C、在Cain的Cracker菜单点解导入用户名和哈希值，只能通过字典破解 D、在Cain的Rainbow生成的表会占用大量的硬盘空间和内存，可是破解速度和效率很高

336、在数据库向因特网开放前，哪个步棸是可以忽略的？（B）

A、安全安装和配置操作系统和数据库系统

B、应用系统应该在内网试运行3个月

C、对应用软件如Web也没、ASP脚本等进行安全性检查

D、网络安全策略已经生效

337、如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf文件，查看是否包含如下设置，选出一个正确的（D）。

A、audit=filename B、sys=filename C、event=filename D、log=filename

338、针对一台对外提供Web服务的Windows服务器，下列关于账户权限控制，哪些项是不合理的？（C）

A、限制匿名账户对Web内容的目录写权限

B、从Everyone组中删除“从网络访问此计算机” 用户权限

C、禁用IUSR-MACHE和IWAN\_MACHINE账户

D、本地登录时必须使用Administrators账户

339、网上营业中间件如果启用了SSl，应采用不低于（C）版本的SSL，采用经国家密码管理局认可的密码算法。

A、2.0 B、2.5 C、3.0 D、3.1

340、SQL Server默认的具有DBA权限的账号是什么？（C）

A、root B、admin C、sa D、system

341、（A）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

342、（C）是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

343、《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（B）。

A、GA 163-1997 B、GA 267-2000

C、GA 243-2000 D、GB 17859-1999

344、安装了合格防雷保安器的计算机信息系统，还必须在（C）雷雨季节前对防雷保安器、保护接地装置进行一次年度检查，发现不合格时，应及时修复或更换。

A、第三年 B、第二年 C、每年 D、当年

345、使用IIalon灭火的工作原理是什么？（C）

A、降低温度 B、隔绝氧气和可燃物

C、破坏氧气和可燃物之间的化学反应 D、减少氧气

346、白炽灯、高压汞灯与可燃物、可燃结构之间的距离不应小于（C）cm。

A、30 B、40 C、50 D、60

347、被电击的人能否获救，关键在于（D）。

A、触电的方式 B、人体电阻的大小

C、触电电压的高底 D、能否尽快脱离电源和施行紧急救护

348、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）。

A、可以随意弯折 B、转弯是，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

349、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

350、长期在高频电磁场作用下，操作者会有什么不良反应？（B）

A、呼吸困难 B、神经失常 C、疲劳无力

351、触电事故中，绝大部分是由于（A）导致人身伤亡的。

A、人体接受电流遭到电击 B、烧伤 C、触电休克

352、从业人员发现直接危及人身安全的紧急情况时，例如气体灭火系统开始开启时，应（A）。

A、停止作业，立即撤离危险现场 B、继续作业

C、向上级汇报，等待上级指令

353、从业人员既是安全生产的保护对象，又是实现安全生产的（C）。

A、关键 B、保证 C、基本要素

354、低压验电笔一般适用于交、直流电压未（C）伏以下。

A、220 B、380 C、500

355、电流为（B）毫安是，称为致命电流。

A、50 B、100 C、120 D、150

356、电器的保险丝只能装在（B）上。

A、零线 B、火线 C、底线

357、电器着火是不能用（C）灭火。

A、四氧化碳或1211灭火 B、沙土 C、水

358、对不符合防雷标准、规范防雷工程专业设计方案，以下（B）应当按照审核结论进行修改并重新报批。

A、建设单位 B、防雷工程专业设计单位 C、工程施工单位

359、发现人员触电时，应（B），使之脱离电源。

A、立即用手拉开触电人员 B、用绝缘物体拨开电源或触电者 C、用铁棍拨开电源线

360、凡设在年平均雷电日大于（C）的地区的计算机信息系统，原则上均应装设计算机信息系统防雷保安器，以防止雷电电磁脉冲过电压和过电流侵入计算机信息系统设备。

A、40 B、45 C、5 D、15

361、废电池随处丢弃会造成（B）的污染。

A、白色污染 B、重金属污染 C、酸雨

362、干粉灭火器多长时间检查一次？（A）

A、半年 B、一年 C、三个月 D、两年

363、根据国家相关规定，电压（D）以下不必考虑防止电击的安全？

A、48伏 B、36伏 C、65伏 D、25伏

364、根据作业环境的不同，安全帽的颜色也不同，如在爆炸性作业场所工作宜戴（A）安全帽。

A、红色 B、黄色 C、白色

365、关于空气的正向压力，下面哪项描述是正确的？（B）

A、当门打开时，空气向内流动 B、当门打开，空气向外流动

C、当发生火灾，系统自动切断电源 D、当发生火灾，烟雾向另外一间房间流动

366、国家颁布的《安全色》标准中，表示警告、主要的颜色为（C）。

A、红色 B、蓝色 C、黄色

367、火灾中对人员威胁最大的是（B）。

A、火 B、烟气 C、可燃物

368、机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（B）m。

A、0.1 B、0.6 C、1.2 D、0.3

369、计算机电源系统的所有节点均应镀铅锡处理（B）连接。

A、热压 B、冷压 C、焊锡 D、直接

370、计算机系统接地应采用（A）。

A、专用底线 B、和大楼的钢筋专用网相连

C、大楼的各种金属管道相连 D、没必要

371、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

372、计算机系统应选用（A）电缆。

A、铜芯 B、铅芯

C、铁芯 D、没有要求

373、进行腐蚀品的装卸作业应戴（B）手套。

A、帆布 B、橡胶 C、棉布

374、人体在电磁场作用下，由于（C）将使人体受到不同程度的伤害。

A、电流 B、电压 C、棉布

375、身上着火后，下列哪种灭火方法是错误的（C）。

A、就地打滚 B、用厚重衣物覆盖压灭火苗 C、迎风快跑

376、生产经营单位必须为从业人员提供符合国家标准或（C）标准的劳动防护用品。

A、当地 B、本单位 C、行业

377、使用新设备，必须了解、掌握其安全技术特征，采取有效的安全防护措施，并对从业人员进行专门的安全生产。（B）

A、当地 B、本单位 C、行业

378.实验地点相对湿度大于75%时，则此实验环境属于易触电的环境：（A）

A、危险 B、特别危险 C、一般

379、通过人身的安全交流电流规定在(A)以下。

A、10mA B、30mA C、50mA

380、下列不属于对物理层信息窃取的是(D)

A、对存储介质的盗取 B、对监视器的窃听

C、对网络线路的窃听 D、对设备屏蔽电磁干扰

381、新、改、扩建项目的安全设施投资应当纳入(C)。

A、企业成本 B、安措经费 C、建设项目概算

382、液体表面的蒸汽与空气形成可燃气体，遇到点火源时，发生一闪即灭的现象称为(C)

A、爆炸 B、蒸发 C、闪燃

383、防雷保安器：防止(B)破坏计算机信息系统的保安装置，可分为两大类：电源

线防雷保安器（简称电源防雷保安器）和信号传输线防雷保安器（简称通道防雷保安器）。

A、直击雷 B、感应雷 C、雷暴 D、雷电电磁脉冲

384、EMC标准是为了保证(D)正常工作而制走的。

A、网络 B、媒体 C、信息 D、系统和设备

385、以下不符合防静电要求的是(B)。

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

386、以下哪些属于系统的物理故障？(A)

A、硬件故障与软件故障 B、计算机病毒

C、人为的失误 D、网络故障和设备环境故障

387、用灭火器灭火时，灭火器的喷射口应该对准火焰的(C)。

A、上部 B、中部 C、根部

388、运输、携带、邮寄计算机信息媒体进出靖的，应当如实向(A)申报。

A、海关 B、工商

C、税务 D、边防

389、在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ (B)

A、产生静电 B、计算机部件腐蚀

C、有污染物 D、B+A

390、在空气不流通的狭小地方使用二氧化碳灭火器可能造成的危险是(B)。

A中毒 B缺氧 C爆炸

391、在雷雨天不要走近高压电杆、铁塔、避雷针、远离至少(C)米以外。

A、IO米 B、15米 C、20米

392、在易燃易爆场所穿(C)最危险。

A、布鞋 B、胶鞋 C、带钉鞋

393、在遇到高压电线断落地面时，导线断落点(B)m内，禁止人员进入。

A、IO B、20 C、30

394、数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？(C)

A、30%-40% B、40%-50% C、45%-60% D、50%-70%

395、计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所

以防雷保安器必须有合理的(B)。

A、屏蔽配置 B、接地配置

C、分流配置 D、均压配置

396、计算站场地宜采用(A)蓄电池。

A、封闭式 B、半封闭式

C、开启式 D、普通任意的

397、多层的楼房中，最适合做数据中心的位置是(D)。

A、楼 B、地下室

C、顶楼 D、除以上外的任何楼层

398、计算机机房是安装计算机信息系统主体的关键场所，是(A)工作的重点，所以

对计算机机房要加强安全管理。

A、实体安全保护 B、人员管理

C、媒体安全保护 D、设备安全保护

399、区域安全，首先应考虑（B），用来识别来访问的用户的身份，并对其合法性进行验证，主要通过特殊标示符、口令、指纹等来实现。

A、来访者所持物 B、物理访问控制 C、来访者所具有的特征 D、来访者所知信息

400、在计算机房出入口处或值班室，应设置（D）和应急断电装置。

A、 电视 B、电扇 C、报警器 D、应急电话

401、下列（A）灭火器是扑救精密仪器火灾的最佳选择。

A、二氧化碳灭火剂 B、干粉灭火剂 C、泡沫灭火剂

402、电气安全主要包括人身安全、（B）安全。

A、照明 B、设备 C、电器 D、空调

403、（C）基于IDEA算法。

A、S/MIME B、SET C、PGP D、SSL

404、

405、(C)是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

406、(D)是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。

A、认证机构 B、密码 C、票据 D、数字证书

407、（D）协议主要用于加密机制。

A、HTTP B、FTP C、TELNET D、SSL

408、（A）原则保证只有发送方与接收方能访问消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

409、（D）原则允许某些用户进行特定访问。

A、保密性 B、鉴别 C、完整性 D、访问控制

410、（B）增加明文冗余度。

A、混淆 B、扩散 C、混淆与扩散 D、都不是

411、3DES加密算法的密钥长度是：（A）。

A、168 B、128 C、56 D、256

412、AES密钥长度不能是（D）。

A、128位 B、192位 C、256位 D、512位

413、AES算法是哪种算法？（A）。

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

414、AES属于哪种加密方式？（B）。

A、流加密 B、分组加密 C、异或加密 D、认证加密

415、CA指的是（A）。

A、证书授权 B、加密认证 C、虚拟专用网 D、安全套接层

416、DES经过（A）轮运算后，左右两部分合在一起经过一个末置换，输出一个64位的密文。（A）

A、16 B、8 C、32 D、4

417、DES算法是哪种算法？（A）

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

418、DES属于哪种加密方式？（B）

A、流加密 B、块加密 C、异或加密 D、认证加密

419、DNSSec中并未采用（C）。

A、数字签名技术 B、公钥加密技术 C、地址绑定技术 D、报文摘要技术

420、ECB指的是（D）。

A、密文链接模式 B、密文反馈模式 C、输出反馈模式 D、电码本模式

421、EC-DSA复杂性的程度是（D）。

A、简单 B、最简单 C、困难 D、最困难

422、EFS可以用在什么文件系统下（C）。

A、FAT16 B、FAT32 C、NTFS D、以上都可以

423、IDEA的密钥长度是多少bit？（D）。

A、56 B、64 C、96 D、128

424、Kerberos是80年代中期，麻省理工学院为Athena项目开发的一个认证服务系统，其目标是把认证、记账和（B）的功能扩展到网络环境。

A、访问控制 B、审计 C、授权 D、监控

425、Kerberos是为TCP/IP网络设计的基于（B）的可信第三方鉴别协议，负责在网络上进行仲裁及会话密钥的分配。

A、非对称密钥体系 B、对称密钥体系 C、公钥体系 D、私钥体系

426、Kerberos是一种网络认证协议。它采用的加密算法是（C）。

A、RSA B、PGP C、DES D、MD5

427、Kerberos算法是一个（B）。

A、面向访问的保护系统 B、面向票据的保护系统

C、面向列表的保护系统 D、面向门与锁的保护系统

428、Kerberos提供的最重要的安全服务是？（A）。

A、鉴别 B、机密性 C、完整性 D、可用性

429、MD5产生的散列值是多少位？（C）。

A、56 B、64 C、128 D、160

430、MD5是按每组512位为一组来处理输入的信息，经过一系列变换后，生成一个（B）为散列值。

A、64 B、128 C、256 D、512

431、MD5是以512位分组来处理输入的信息，每一分组又被划分为（A）32位子分组。

A、16个 B、32个 C、64个 D、128个

432、MD5算法将输入信息M按顺序每组（D）长度分组，即：M1，M2，...，Mn-1，Mn。

A、64位 B、128位 C、256位 D、512位

433、PKI（公共密钥基础结构）中应用的加密方式为（B）。

A、对称加密 B、非对称加密 C、HASH加密 D、单向加密

434、PKI的全称是（D）。

A、Private Key Intrusion B、Public Key Intrusion

C、Private Key Infrastructure D、Public Key Infrastructure

435、PKI无法实现（D）。

A、身份认证 B、数据的完整性 C、数据的机密性 D、权限分配

436、RC4是由RIVEST在1987年开发的一种流式的密文，就是实时地把信息加密成一个整体，它在美国一般密钥长度是128位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）。

A、64位 B、56位 C、40位 D、32位

437、RSA公钥加密系统中，他想给她发送一份邮件，并让她知道是他发出，应选用的加密秘钥是（C）。

A、他的公钥 B、她的公钥 C、他的私钥 D、她的私钥

438、RSA使用不方便的最大问题是（A）。

A、产生密钥需要强大的计算能力 B、算法中需要大数

C、算法中需要素数 D、被攻击过很多次

439、RSA算法建立的理论基础是（C）。

A、DES B、替代想组合 C、大数分解和素数检测 D、哈希函数

440、SHA-1产生的散列值是多少位？（D）。

A、56 B、64 C、128 D、160

441、按密钥的使用个数，密码系统可以分为（C）。

A、置换密码系统和易位密码系统 B、分组密码系统和序列密码系统

C、对称密码系统和非对称密码系统 D、密码系统和密码分析系统

442、充分发挥了DES和RSA两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是：（C）。

A、数字签名 B、数字指纹 C、数字信封 D、数字时间戳

443、从技术角度上看数据安全的技术特征主要包含哪几个方面？（B）。

A、数据完整性、数据的方便性、数据的可用性 B、数据的完整性、数据的保密性、数据的可用性 C、数据的稳定性、数据的保密性、数据的可用性 D、数据的方便性、数据的稳定性、数据的完整性

444、单项散列函数的安全性来自于他的（A）。

A、单向性 B、算法复杂性 C、算法的保密性 D、离散性

445、电路网关防火墙工作在OSI协议的哪一层？（A）。

A、传输层 B、链路层 C、应用层 D、物理层

446、电子邮件的机密性与真实性是通过下列哪一项实现的？（A）

A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密

B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密

C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密

D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

447、端对端加密只需要保证消息都在哪里进行加密？（A）

A、源点和目的地节点 B、经过的每一个节点

C、源点和中间经过的每一个节点 D、所有节点

448、对明文字母重新排列，并不隐藏他们的加密方法属于（C）。

A、置换密码 B、分组密码 C、易位密码 D、序列密码

449、对网络中两个相邻节点之间传输的数据进行加密保护的是（A）。

A、节点加密 B、链路加密 C、端到端加密 D、DES加密

450、发送消息和用发送方私钥加密哈希加密信息将确保消息的：（A）。

A、真实性和完整性 B、真实性和隐私 C、隐私和不可否认性 D。隐私和不可否性

451、高级加密标准AES算法中，加密回合数不可能是（D）。

A、10 B、12 C、14 D、16

452、公钥机制利用一对互相匹配的（B）进行加密，解密。

A、私钥 B、密钥 C、数字签名 D、数字证书

453、公钥加密体制中，没有公开的是（A）。

A、明文 B、密文 C、公钥 D、算法

454、公钥证书提供了一种系统的、可扩展的、统一的（A）。

A、公钥分发方案 B、实现不可否认方案

C、对称密钥分发方案 D、保证数据完整性方案

455、关于CA和数字证书的关系，以下说法不正确的是（B）。

A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由CA签发

B、数字证书一般依靠CA中心的对称密钥机制来实现

C、在电子交易中，数字证书可以用于表明参与方的身份

D、数字证书能以一种不能被假冒的方式证明证书持有人身份

456、关于数字签名说法正确的是（A）。

A、数字签名的加密方法以目前的计算机的运算能力来破解是不现实的

B、采用数字签名，不能够保证信息自签发后到收到为止没有做过任何修改（能保证信息收到后没做个任何修改）

C、采用数字签名，能够保证信息是有签名者自己签名发送的，但由于不是真实的签名，签名者容易否认（签名不容易否认）

D、用户可以采用公钥对信息加以处理，形成数字签名（需使用私钥对信息加以处理）

457、基于私有密钥体制的信息认证方法采用的算法是（D）。

A、素数检测 B、非对称算法 C、RSA算法 D、对称加密算法

458、加密技术不能实现（D）。

A、数据信息的完整性 B、基于密码技术的身份认证 C、机密文件加密 D基于IP头信息的包过滤

459、加密技术不能提供以下哪种安全服务？（D）。

A、鉴别 B、机密性 C、完整性 D可用性

460、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）。

A、对称密钥加密 B、非对称密钥加密 C、 D

461、假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（A）。

A、对称加密技术 B、分组加密技术 C、公钥加密技术 D、单项函数密码技术

462、就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。（C）

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

463、利用非对称密钥体制实现加密通信时，若A要向B发送加密信息，则该加密信息应该使用（B）。

A、A的公钥加密 B、B的公钥加密 C、A的私钥加密 D、B的私钥加密

464、利用物理设备将各类型的无法预测的输入集中起来生成随机数的设备是（A）。

A、随机数生成器 B、伪随机数生成器 C、中央处理 D、非易失存储

465、链路加密要求必须先对链路两端的加密设备进行（C）。

A、异步 B、重传 C、同步 D、备份

466、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？（C）

A、对称的公钥算法 B、非对称私钥算法 C、对称密钥算法 D、非对称密钥算法

467、密码分析的目的是什么？（A）

A、确定加密算法的强度 B、增加加密算法的代替功能

C、减少加密算法的换为功能 D、确定所使用的换位

468、请从下列各项中选出不是HASH函数算法的一项。（D）

A、MD5 B、SHA C、HMAC D、MMAC

469、如今，DES加密算法面临的问题是（A）。

A、密钥太短，已经能被现代计算机暴力破解 B、加密算法有漏洞，在数学上已被破解 C、留有后门，可能泄露部分信息 D、算法过于陈旧，已经有更好的替代方案

470、若单项散列函数的输入串有很小的变化，则输出串（A）。

A、可能有很大的变化 B、一定有很大的变化 C、可能有很小的变化 D、一定有很小的变化

471、散列算法可以做哪些事？（C）。

A、碰撞约束 B、入侵检测 C、组合散列 D、随机数生成器

472、身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（B）。

A、可信性 B、访问控制 C、完整性 D、保密性

473、数字签名常用的算法有（B）。

A、DES算法 B、RSA算法 C、Hash函数 D、AES算法

474、数字签名和随机数挑战不能防范以下哪种攻击或恶意行为？（D）。

A、伪装欺骗 B、重放攻击 C、抵赖 D、DOS攻击

475、数字签名可以解决（D）。

A、数据被泄露 B、数据被篡改 C、未经授权擅自访问 D、冒名发送数据或发送后抵赖

476、数字签名通常使用（B）方式。

A、公钥密码体系中的私钥 B、公钥密码系统中的私钥对数字摘要进行加密

C、密钥密码体系 D、公钥密码体系中公钥对数字摘要进行加密

477、数字信封是用来解决（C）。

A、公钥分发问题 B、私钥分发问题 C、对称密钥分发问题 D、数据完整性问题

478、数字证书不包括（B）。

A、签名算法 B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号 D、颁发数字证书单位的数字签名

479、数字证书的应用阶段不包括（D）。

A、证书检索 B、证书验证 C、密钥恢复 D、证书撤销

480、下列说法中错误的是（D）。

A、非对称算法也叫公开密钥算法 B、非对称算法的加密密钥和解密密钥是分离的 C、非对称算法不需要对密钥通信进行保密 D、非对称算法典型的有RSA算法、AES算法等

481、下列算法中，哪种不是对称加密算法？（C）

A、AES B、DES C、RSA D、RC5

482、下列算法中属于Hash算法的是（C）。

A、DES B、IDEA C、SHA D、RSA

483、以下对于链路加密哪项是正确的？（B）

A、消息只在源点加密，目的节点解密 B、消息在源点加密，在每一个经过的节点解密并加密 C、消息在所有经过的节点中都是加密的，但只在目的节点解密 D、消息以明文形式在节点之间传输

484、以下各种加密算法中属于单钥制加密算法的是（A）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密算法

485、以下各种加密算法中属于双钥制加密算法的是（D）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密486、以下各种算法中属于古典加密算法的是（B）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密487、以下关于CA认证中心说法正确的是（C）。

A、CA认证时使用对称密钥机制的认证方法 B、CA认证中心支负责签名，不负责证书的产生 C、CA认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份 D、CA认证中心不用保持中立，可以随便找一个用户来作为CA认证中心

488、以下关于VPN说法正确的是（B）。

A、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B、VPN指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接

C、VPN不能做到信息认证和身份认证 D、VPN只能提供身份认证、不能提供加密数据的功能

489、以下关于数字签名说法正确的是（D）。

A、数字签名是在所传输的数据后附上一段和传输数据毫无关系的数字信息

B、数字签名能够解决数据的加密传输，即安全传输问题

C、数字签名一般采用对称加密机制 D、数字签名能够解决篡改、伪造等安全性问题

490、以下密码使用方法中正确的是（D）。

A、将密码记录在日记本上以避免忘记 B、任何情况下均不得使用临时性密码

C、密码中的字母不得重复 D、不要使用全部由字母组成的密码

491、以下哪个不包含在证书中？（C）

A、密钥采取的算法 B、公钥及其参数 C、私钥及其参数 D、签发证书的CA名称

492、以下哪个选项不会破坏数据库的完整性？（A）

A、对数据库中的数据执行删除操作 B、用户操作过程中出错

C、操作系统的应用程序错误 D、DBMS或操作系统程序出错

493、以下哪项不属于数据库系统实体安全？（B）

A、环境安全 B、线路安全 C、设备安全 D、媒体安全

494、以下哪一种算法产生最长的密钥？（D）

A、Diffe-Hellman B、DES C、IDEA D、RSA

495、以下认证方式中，最为安全的是（D）。

A、用户名+密码 B、卡+密码 C、用户名+密码+验证码 D、卡+指纹

496、远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（B）

A、知道什么 B、拥有什么 C、是谁 D、双因素认证

497、在3DES算法中，密钥最高可达到多少位？（C）

A、96 B、128 C、168 D、200

498、在IPSec中，（C）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的IPSec协议、密码算法、密钥等信息。

A、ESP B、SPI C、SA D、SP

499、在IPSec中，IKE提供（B）方法供两台计算机建立。

A、解释域 B、安全关联 C、安全关系 D、选择关系

500、在RIP的MD5认证报文中，经过加密的密钥是放在哪里的？（B）

A、保温的第一个表项里 B、报文的最后一个表项里

C、报文的第二个表项里 D、报文头里

501、在非对称加密算法中，涉及到的密钥个数是？（B）

A、一个 B、两个 C、三个 D、三个以上

502、在高级加密标准AES算法中，区块大小为（A）。

A、128位 B、192位 C、256位 D、512位

503、在给定的密钥体制中，密钥与密码算法可以看成是（A）。

A、前者是可变的，后者是固定的 B、前者是固定的，后者是可变的

C、两者都是可变的 D、两者都是固定的

504、在公钥体制中，不公开的是（B）。

A、公钥 B、私钥 C、公钥和私钥 D、私钥和加密算法

505、在密码学中，需要被交换的原消息被称为什么？（D）

A、密文 B、算法 C、密码 D、明文

506、一般证书采用哪个标准？（D）

A、ISO/IEC 15408 B、ISO/IEC 17799 C、BS 7799 D、X. 509V3

507、一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（D）

A、信息的数据和时间戳 B、识别发信的计算机

C、对信息内容进行加密 D、对发送者的身份进行识别

508、在数据库中，下列哪些数据不能加密？（A）

A、索引字段 B、存放日期字段

C、存放密码的 D、存放名称字段

509、在一个网络节点中，链路加密仅在以下哪项中提供安全性？（D）

A、数据链路层 B、物理层

C、通信层 D、通信链路

510、在以下隧道协议中，属于三层隧道协议的是（D）。

A、L2F B、PPTP C、L2TP D、IPSec

511、以下哪一项是基于一个大的整数很难分解成两个素数因数？（B）

A、ECC B、RSA C、DES D、D-H

512、以下哪种数据加密技术可以在基础架构层面进行？（A）

A、IPSec B、Secure Sockets Layer

C、Transport Layer Securit D、RSA

513、目前最安全的身份认证机制是（A）。

A、一次口令机制 B、双因素法

C、基于智能卡的用户身价认证 D、身价认证的单因素法

514、当数据库由于各种原因而使其完整性遭到破坏时，必须采取以下哪项措施来恢复数据库？（C）

A、重新安装数据库 B、换一种数据库

C、使用数据库备份 D、将数据库中的数据利用工具导出，并保存

515、PGP加密算法是混合使用（B）算法和IDEA算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES B、RSA C、IDEA D、AES

516、以下哪些软件是用于加密的软件？（A）

A、PGP B、SHA C、EFS D、DES

517、如果消息接受方要确定发送方身价，则要使用（B）原则。

A、保密性 B、鉴别 C、完整性 D、访问控制

518、对于现代密码破解，（D）是最常的方法。

A、攻破算法 B、监听截获 C、信息猜测 D、暴力破解

519、非对称密码技术的缺点有哪些？（B）

A、密钥持有量减少 B、加/解密速度慢 C、耗用资源较少 D、以上都是

520、CA不能提供下列哪种证书？（D）

A、个人数字证书 B、SSL服务器证书

C、安全电子邮件证书 D、SET服务器证书

521、以下关于混合加密方式说法正确的是（B）。

A、采用公开密钥体制进行通信过程中的加解密处理

B、采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C、采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D、采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密

处理速度快的双重优点

522、果要保证（C）原则，则不能在中途修改消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

523、口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（D）

A、长期没有修改的口令 B、过短的口令

C、两个人共用的口令 D、设备供应商提供的默认的口令

524.非对称密钥的密码技术具有很多优点，其中不包括：（B）。

A、可提供数字签名、零知识证明等额外服务

B、加密/解密速度快，不需占用较多资源

C、通信双方事先不需要通过保密信道交换密钥

D、密钥持有量大大减少

525．DES是一种block（块）密文的加密算法，是把数据加密成多大的块？（B）

A、32位 B、64位 C、128位 D、256位

526．CA数字证书中不包含的信息有（C）。

A、CA的数字签名 B、证书申请者的个人信息

C、证书申请者的私钥 D、证书申请者的公钥信息

527．以下关于对称密钥加密说法正确的是（C）。

A、加密方和解密可以使用不同的算法 B、加密密钥和解密密钥可以是不同的

C、加密密钥和解密密钥必须是相同的 D、密钥的管理非常简单

528、在为计算机设置使用密码时，下面（D）密码是最安全的。

A、12345678 B、66666666

C、20061001 D、72aB@#41

529、（C）的攻击者发生在Web应用层？

A、25% B、50%

C、75% D、90%

530、“U盘破坏者”病毒（Worm.vhy）采用（B）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。

A、网上邻居 B、我的电脑

C、我的文档 D、收藏夹

531、“冲击波”病毒运行时会将自身复制到Windows目录下，并命名为（C）

A、Gsrss.exe B、msbast.exe

C、msblast.exe D、lsass.exe

532、Code Red 爆发于2001年7月，利用微软的IIS漏洞在Web服务器之间传播。针对这一漏洞，微软早在2001年三月就发布了相关的补丁。如果今天服务器仍然感染Code Red，那么属于哪个阶段的问题？（A）

A、系统管理员维护阶段的失误 B、微软公司软件的设计阶段的失误

C、最终用户使用阶段的失误 D、微软公司软件的实现阶段的失误

533、病毒的传播机制主要有哪些？（D）

A、移动存储 B、电子邮件 C、网络共享 D、以上均是

534、病毒的反静态反汇编技术都有（D）。

A、数据压缩 B、数据加密 C、感染代码 D、以上均是

535、病毒在感染计算机系统时，一般（B）感染系统的。

A、病毒程序都会在屏幕上提示，待操作者确认（允许）后

B、实在操作者不觉察的情况下

C、病毒程序会要求操作者制定存储的磁盘和文件夹后

D、在操作者为病毒制定存储的文件名以后

536、杀毒软件时提示“重新启动计算机后删除文件”其主要原因是（A）

A、文件插入了系统关键进程，杀毒时无法处理

B、文件是病毒文件，无法处理

C、由于病毒的加壳形式不同，杀毒时无法正确处理

D、文件正在运行且无法安全的结束，需要其他处理方法

537、蠕虫的目标选择算法有（D）。

A、随机性扫描 B、基于目标列表的扫描

C、顺序扫描 D、以上均是

538、网络钓鱼是指（A）

A、通过大量发送声来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息。

B、网上进行钓鱼活动

C、通过网络组织钓鱼活动，从而获得利益 D、以上都不是

539、不属于常见把入侵主机的信息发送给攻击者的方法是（D）。

A、E-MAIL B、UDP C、ICMP D、连接入侵主机

540、不属于黑客被动攻击的是（A）

A、缓冲区溢出 B、运行恶意软件 C、浏览恶意代码网页 D、打开病毒附件

541、不属于黑客前期收集信息的工具是（D）

A、Nmap B、Xscan C、Nslookup D、LC

542、常见Web攻击方法，不包括？（D）

A、利用服务器配置漏洞 B、恶意代码上传下载

C、构造恶意输入（SQL注入攻击、命令注入攻击、跨站脚本攻击）

D、业务测试

543、常用的抓包软件有（A）。

A、ethereal B、MS office C、fluxay D、netscan

544.网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（A）

A、密码加密后，不会被窃听 B、Cookie字段可以被窃听

C、报文和帧可以窃听 D、高级窃听者还可以进行ARPSpoof，中间人攻击

545、除了在代码设计开发阶段预防SQL注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（C）

A、禁止将任何高权限账号（例如sa,dba等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户

B、拒绝用户访问敏感的系统存储过程

C、禁止用户访问的数据库表 D、限制用户所能够访问的数据库表

546、防止用户被冒名所欺骗的方法是（A）。

A、对信息源发放进行身份验证 B、进行数据加密

C、对访问网络的流量进行过滤和保护 D、采用防火墙

547、给电脑设置多道口令，其中进入电脑的第一道口令是（B）。

A、系统口令 B、CMOS口令

C、文件夹口令 D、文档密码

548、攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息重新发往B称为（D）。

A、中间人攻击 B、口令猜测器和字典攻击

C、强力攻击 D、回放攻击

549、故意制作、传播计算机病毒，造成计算机信息系统不能正常运行，但如果后果不严重就无罪，可以原谅，这种说法（C）。

A、不对，对这种蓄意破坏行为不能原谅 B、即使不是故意的，后果也不很严重

C、对。我国实行成文法，根据《中华人民共和国刑法》第286条的规定，只有造成严重后果者才有罪

D、无法断定

550、关于80年代Mirros蠕虫危害的描述，哪句话是错误的？（B）

A、占用了大量的计算机处理器的时间，导致拒绝股务

B、窃取用户的机密信息，破坏计算机数据文件

C、该蠕虫利用Unix系统上的漏洞传播

D、大量的流量堵塞了网络，导致网络瘫痪

551、关于黑客注入攻击说法错误的是： (D)

A、它的主要原因是程序对用户的输入缺乏过滤

B、一般情况下防火墙对它无法防范

C、对它进行防范时要关注操作系统的版本和安全补丁

D、注入成功后可以获取部分权限

552、基于主机评估报告对主机进行加固时，第一步是（B）。

A、账号、口令策略修改 B、补丁安装

C、文件系统加固 D、日志审核增强

553、计算机病毒会对下列计算机服务造成威胁，除了（C）。

A、完整性 B、有效性

C、保密性 D、可用性

554、计算机病毒是一段可运行的程序，它一般（C）保存在磁盘中。

A、作为一个文件 B、作为一段数据

C、不作为单独文件 D、作为一段资料

555、什么方式能够从远程绕过防火墙去入侵一个网络？(D)

A、IP services\_ B、Active ports

C、Identified network topology D、Modem banks

556、输入法漏洞通过（D）端口实现的。

A、21 B、23 C、445 D、3389

557、特洛伊木马攻击的威胁类型属于（B）。

A、授权侵犯威胁 B、植入威胁

C、渗入威胁 D、旁路控制威胁

558、通常黑客扫描目标机的445端口是为了(B)。

A、利用NETBIOS SMB服务发起DOS攻击

B、发现并获得目标机上的文件及打印机共享

C、利用SMB服务确认Windows系统版本

D、利用NETBIOS服务确认Windows系统版本

559、网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？(A)

A、残余风险评估阶段 B、检查阶段

C、入侵检测系统监控阶段 D、网络异常流量临控阶段

560、网络病毒预防范阶段的主要措施是什么？(A)

A、强制补丁、网络异常流量的发现 B、强制补丁、入侵检测系统监控

C、网络异常流量的发现、入侵检测系统的监控阶段 D、缺少D选项

561、下列除了(B)以外，都是防范计算机病毒侵害的有效方法。

A、使用防病毒软件 B、机房保持卫生，经常进行消毒

C、避免外来的磁盘接触系统 D、网络使用防病毒网关设备

562、下列除了(A)以外，都是计算机病毒传

A、通过操作员接触传播 B、通过U盘接触传播

C、通过网络传播 D、通过电子播的途径邮件传播

563、下列措施中，(C)不是减少病毒的传染

和造成的损失的好办法。

A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B、外来的文件要经过病毒检测才能使用，不要使用盗版软件

C、不与外界进行任何交流，所有软件都自行开发

D、定期用抗病毒软件对系统进行查毒、杀毒

564、下列哪项是跨站脚本Cross Site Scripting攻击具体事例？（B）

A、搜索用户 B、发帖子，发消息 C、上传附件 D、下载文件

565、下列哪项为信息泄露与错误处理不当Information Leakage and Improper

Error Handlina攻击具体实例？(D)

A、不明邮件中隐藏的html链接 B、发帖子，发消息

C、上传附件 D、错误信息揭示路径

566、下面哪一项是黑客用来实施DDoS攻击的工具？(D)

A、LC5 B、Rootkit C、Icesword D、Trinoo

567、以下哪个工具可以抹去所有NT/2K配置，并将其还原到初始状态？(A)

A、Rollback. exe B、Recover. exe C、Zap. exe D、Reset. exe

568、以下哪个工具通常是系统自带任务管理器的替代？(D)

A、Regmon B、Filemon C、Autoruns D、Process explorer

569、以下哪个针对访问控制的安全措施是最容易使用和管理的？(C)

A、密码 B、加密标志 C、硬件加密 D、加密数据文件

570、以下哪项不是分布式拒绝服务攻击常用的工具？(D)

A、Trinoo B、Trinoo C、TFN D、synkill

571、以下哪项不属于针对数据库的攻击？(D)

A、特权提升 B、强力破解弱口令或默认的用户名及口令

C、SQL注入 D、利用xss漏洞攻击

572、以下哪项工具不适合用来做网络监听？(B)

A、sniffer B、Webscan C、 Windump D、 D-Iris

573、以下哪项是SYN变种攻击经常用到的工具？(B)

A、sessionIE B、synkill C、TFN D、Webscan

574、以下哪一项不是流氓软件的特征？(D)

A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装

B、通常添加驱动保护使用户难以卸载

C、通常会启动无用的程序浪费计算机的资源

D、通常会显示下流的言论

575、一个数据仓库中发生了安全性破坏。以下哪一项有助于安全调查的进行？(B)

A、访问路径 B、时戳 C、数据定义 D、数据分类

576、以下哪一项不属于恶意代码？(C)

A、病毒 B、蠕虫 C、宏 D、特洛伊木马

577、以下哪一项不属于计算机病毒的防治策略？(D)

A、防毒能力 B、查毒能力 C、杀毒能力 D、禁毒能力

578、以下哪一项是常见Web站点脆弱性扫描工具？(A)

A、Appscan B、Nmap C、Sniffer D、LC

579、以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？(A)

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将臀陆信息写入记事本

580、以下哪种符号在SQL注入攻击中经常用到？(D)

A、$\_ B、1 C、@ D、;

581、以下哪种工具能从网络上检测出网络监听软件(A)

A、sniffdet, , B、purify, , C、Dsniff D、WireShark

582、以下哪种攻击可能导致某些系统在重组IP分片的过程中宕机或者重新启动？(B)

A、分布式拒绝服务攻击 B、Ping of Death

C、NFS攻击 D、DNS缓存毒化攻击

583、下面哪部分不属于入侵的过程？(B)

A、数据采集 B、数据存储 C、数据检测 D、数据分析

584、以下对木马阐述不正确的是(A)。

A、木马可以自我复制和传播

B、有些木马可以查看目标主机的屏幕

C、有些木马可以对目标主机上的文件进行任意揉作

D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。

585、由于攻击者可以借助某种手段，避开DBMS以及应用程序而直接进入系统访问

数据，我们通常采取以下哪种方式来防范？(A)

A、数据库加密

B、修改数据库用户的密码，将之改得更为复杂

C、使用修改查询法，使用户在查询数据库时需要满足更多的条件

D、使用集合法

586、在大多数情况下，病毒侵入计算机系统以后，(D)。

A、病毒程序将立即破坏整个计算机软件系统

B、计算机系统将立即不能执行我们的各项任务

C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

587、在确定威胁的可能性时，可以不考虑以下哪项？(D)

A、威胁源 B、潜在弱点

C、现有控制措施 D、攻击所产生的负面影响

588、在以下人为的恶意攻击行为中，属于主动攻击的是(A)。

A、身份假冒 B、数据GG C、数据流分析 D、非法访问

589、下面哪一种攻击方式最常用于破解口 令？(B)

A、哄骗( spoofing) B、字典攻击(dictionary attack)

C、拒绝服务(DoS) D、WinNuk

590、针对DNS服务器发起的查询DoS攻击，属于下列哪种攻击类型？(C)

A、syn flood B、ack flood C、 udpflood D、Connection flood

591、下列哪项不是安全编码中输入验证的控制项？(D)

A、数字型的输入必须是合法的数字

B、字符型的输入中对’进行特殊处理

C、验证所有的输入点，包括Get，Post，Cookie以及其他HTTP头

D、正确使用静态查询语句，如PreDaredStatement

592、以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？(C)

A、早期的SMTP协议没有发件人认证的功能

B、网络上存在大量开放式的邮件中转服务器，导致垃圾邮件的来源难于追查

C、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因

D、Internet分布式管理的性质，导致很难控制和管理

593、以下哪种方法是防止便携式计算机机密信息泄露的最有效方法？（A）

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将登录信息写入记事本

594、以下哪种攻击属于DDoS类攻击？（A）

A、SYN变种攻击 B、smurf攻击 C、arp攻击 D、Fraggle攻击

595、URL访问控制不当不包括（D）

A、Web应用对页面权限控制不严 B、缺乏统一规范的权限控制框架

C、部分页面可以直接从URL中访问 D、使用分散登录认证

596、Web应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（A）

A、静态密码 B、短信挑战 C、指纹认证 D、图片认证

597、Web应用漏洞按类别进行排名，由多到少正确的顺序为？（A）

A、跨站脚本、注入、恶意代码、引用不当

B、注入、跨站脚本、恶意代码、引用不当

C、恶意代码、跨站脚本、注入、引用不当

D、引用不当、跨站脚本、注入、恶意代码

598、从技术角度，以下不是漏洞来源的是（D）

A、软件或协议设计时候的瑕疵 B、软件或协议实现中的弱点

C、软件本身的瑕疵 D、显示卡内存容量过低

599、（C）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A、身份假冒 B、数据篡改 C、信息窃取 D、越权访问

600、有关密码学分支的定义，下列说法中错误的是（D）

A、密码学是研究信息系统安全保密的科学，由两个相互对立、相互斗争、而且又相辅相成、相互渗透的分支科学所组成的、分别称为密码编码学和密码分析学

B、密码编码学是对密码体制、密码体制的输入输出关系进行分析、以便推出机密变量、包括明文在内的敏感数据

C、密码分析学主要研究加密信息的破译或信息的伪造

D、密码编码学主要研究对信息进行编码，实现信息的隐藏

601、与RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（C）

A、数字签名 B、鉴别机制 C、加密机制 D、数据完整性

602、以下哪项是数据库加密方法中的库外加密的缺点？（A）

A、即使访问一条数据也要对整个数据库解密 B、密钥管理比较复杂

C、加密之后不能完整的查询数据 D、密钥过于简单，容易被破解

603、以下哪项数据中涉及安全保密的最主要问题？（A）

A、访问控制问题 B、数据完整性 C、数据正确性 D、数据安全性

604、以下哪一个最好的描述了数字证书？（A）

A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，它使得黑客不能得知用户的身份

C、网站要求用户使用用户名和密码登陆的安全机制

D、伴随在线交易证明购买的收据

605、TCP SYN Flood网络攻击时利用了TCP建立连接过程需要（C）次握手的特点而完成对目标进行攻击的。

A、1 B、2 C、3 D、6

二、多项选择题（606-789）

606、COBIT度量过程的三个纬度分别是（ABC）。

A、能力 B、绩效 C、控制度 D、能力成熟度

607、IT系统内网与互联网连接检查手段有哪些？（BCD）

A、工具扫描 B、人员访谈 C、人工检查 D、文档检查

608、公司应该采取以下措施，对第三方访问进行控制。（ABCD）

A、公司应于第三发公司法人签署保密协议，并要求其第三方个人签署保密承诺，此项工作应在第三方获得网络与信息资产的访问权限之前完成

B、实行访问授权管理，未经授权，第三方不得进行任何形式的访问

C、公司应加强第三方访问的过程控制，监督其活动及操作，对其进行适当的安全宣传与培训

D、第三方人员应佩戴易于识别的标志，并在访问公司重要场所时有专人陪同

609、计算机信息系统安全的三个相辅相成，互补互通的有机组成部分是（ABD）

A、安全策略 B、安全法规 C、安全技术 D、安全管理

610、劳动合同中应包含网络与信息安全条款，这些条款规定（ACD）。

A、员工的安全责任和违约罚则

B、安全责任不可延伸至公司场所以外和正常工作时间以外

C、安全责任可延伸至公司场所以外和正常工作时间以外

D、如必要，一些安全责任应在雇佣结束后延续一段特定的时间

611、审核是网络安全工作的核心，下列应用属于主动审核的是：（CD）

A、Windows事件日志记录 B、数据库的事务日志记录

C、防火墙对访问站点的过滤 D、系统对非法链接的拒绝

612、通用准则CC实现的目标有（ABC）

A、成为统一的国际通用安全产品、系统的安全标准

B、在不同国家达成协议，相互承认产品安全等级评估

C、概述IT产品的国际通用性 D、都不是

613、系统用户账号登记表应包括（ABCD）。

A、使用者姓名、部门、职务、联系电话 B、账号权限

C、批准人、开通人 D、开通时间、到期日

614、下列情况哪些是对公司经营管理的影响为“一般”级别的互联网网络安全事件？（ABD）

A、发生未到达“预警”的一般性安全事件

B、出现新的漏洞，尚未发现利用方法或利用迹象

C、有来自境外的网络性能明显下降的报警，并且其技术原因普遍适用于我国互联网 D、出现新的蠕虫/病毒或其它恶意代码，尚未证明可能造成严重危害

615、信息安全的主要原则有（BCD）

A、认证性 B、保密性 C、可用性 D、完整性

**616、针对支撑系统，除业务关联性、对业务网络的影响，资产价值主要体现在（ACD）几个方面。 缺少D选项**

**A、业务收益的影响 B、设备购买成本 C、面向客户的重要程度 D、**

617、IT系统病毒泛滥的主要原因有哪些？（ABCD）

A、主机和终端防病毒软件缺乏统一管理

B、主机和终端防病毒软件没有设置为自动更新或更新周期较长

C、防病毒服务器没有及时更新放病毒库

D、缺乏防病毒应急处理流程和方案

618、IT系统病毒防护评估检查对象包括哪些内容？（ABCD）

A、防病毒服务器 B、重要应用Windows主机

C、Windows终端 D、主机管理员

619、互联网连接防火墙设备的安全策略配置要求包括哪几点（ABCD）。

A、远程登录是否禁止telnet方式 B、最后一条策略是否是拒绝一切流量

C、是否存在允许any to any的策略

D、是否设置了管理IP，设备只能从管理IP登录维护

620、《安全基线标准》在安全管理层面主要围绕哪几部分考评安全基线？（ABC）

A、组织架构管理 B、人员安全管理 C、运维安全管理 D、制度安全管理

621、IT系统维护人员权限原则包括（ACD）。

A、工作相关 B、最大授权 C、最小授权 D、权限制约

622、安全系统加固手册中关于造成系统异常中断的各方面因素，主要包括哪三方面（ABD）

A、人为原因 B、环境原因 C、生产原因 D、设备原因

623、IT系统维护人员权限原则包括（ACD）

A、工作相关 B、最大授权 C、最小授权 D、权限制约

624、计算当前Linux系统中所有用户的数量，可以使用（ABC）命令

A、wc -l /etc/passwd B、wc -l</etc/passwd

C、cat/etc/passwd|wc -l D、cat/etc/passwd>wc -l

625、Solarid系统中，攻击者在系统中增加账户会改变哪些文件？（AB）

A、shadow B、passwd C、inetd,conf D、hosts

626、Syn Flood攻击的现象有以下哪些？（ABC）

A、大量连接处于SYN\_RCVD状态 B、正常网络访问受阻

C、系统资源使用率高

627、UNIX安全审计的主要技术手段有哪些？（ABCDEF）

A、文件完整性审计 B、用户、弱口令审计 C、安全补丁审计

D、端口审计 E、进程审计 F、系统日志审计

628、Unix系统提供备份工具有（ABCD）

A、cp：可以完成把某一目录内容拷贝到另一目录

B、tar：可以创建、把文件添加到或从一个tar档案中解开文件

C、cpio：把文件拷贝进或拷贝出一个cpio档案或tar档案

D、dump：用来恢复整个文件系统或提取单个文件

629、操作系统应利用安全工具提供以下哪些访问控制功能？（ABC）

A、验证用户身份，必要的话，还应进行终端或物理地点识别

B、记录所有系统访问日志

C、必要时，应能限制用户连接时间 D、都不对

630、从哪些地方可以看到遗留痕迹？（ABCD）

A、回收站 B、最近使用过的文件 C、注册表 D、文件最后更改的时间戳631、

632、关于Windows活动目录说法正确的是（ABD）。

A、活动目录是采用分层结构来存储网络对象信息的一种网络管理体系

B、活动目录可以提供存储目录数据和网络用户级管理员使用这些数据的方法

C、利用活动目录来实现域内计算机的分布式管理

D、活动目录与域紧密结合构成与目录林和域目录树，使大型网络中庞大、复杂的网络管理、控制、访问变得简单，使网络管理效率更高

633、建立堡垒主机的一般原则是（AC）。

A、最简化原则 B、复杂化原则 C、预防原则 D、网络隔离原则

634、逻辑空间主要包括哪些部分？（ABDE）

A、TABLESPACES B、SEGMENTS C、DATAFILE

D、EXTENTS E、BLOCK

635、哪些属于Windows日志？（ABCD）

A、AppEvent.Evt B、SecEvent.Evt C、SysEvent.Evt D、W3C扩展日志

636、如何设置listener口令？（ACDE）

A、以Oracle用户运行lsnrctl命令 B、set log\_file

C、change\_password D、set password E、save\_config

637、审计启动其日志有哪两种存放方式？（BD）

A、NONE B、OS C、TRUE D、SYS.AUD$

638、生产服务器通常都是UNIX平台，资产价值最高，不直接连接外部网络，主要的安全需求是（ABD）

A、访问控制 B、账号口令 C、数据过滤 D、权限管理和补丁管理

639、使用md5sum工具对文件签名，以下说法正确的是？（ADE）

A、md5sum对任何签名结果是定长的16字节

B、md5sum对文件签名具有不可抵赖性

C、md5sum是对文件进行加密运算得出签名，不同文件结果几乎不相同

D、md5sum是对文件进行哈希运算得出签名，不同文件结果几乎不相同

E、md5sum对文件签名时，与文件的日期和时间无关

640、为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有（ABCD）

A、口令/账号加密 B、定期更换口令

C、限制对口令文件的访问 D、设置复杂的、具有一定位数的口令

641、文件系统是构成Linux基础，Linux中常用文件系统有（ABD）？

A、ext3 B、ext2 C、hfs D、reiserfs

642、下列关于UNIX下日志说法正确的是（AC）

A、wtmp记录每一次用户登录和注销的历史信息

B、acct记录每个用户使用过的命令

C、sulog记录su命令的使用情况

D、acct记录当前登录的每个用户

643、下列哪些操作可以看到自启动项目？（ABD）

A、注册表 B、开始菜单 C、任务管理器 D、msconfig

644、下列哪些命令行可用于查看当前进程？（ABC）

A、Ps -ef B、Strings -f/proc/[0-9]\*/cmdline

C、Ls -al /proc/[0-9]\*/exe D、Cat/etc/inetd.conf

645、下面操作系统中，哪些是UNIX操作系统？（CD）

A、Red-hat Linux B、Novell Netware C、Free BSD D、SCO Unix

646、严格的口令策略应当包含哪些要素（ABC）

A、满足一定的长度，比如8位以上 B、同时包含数字，字母和特殊字符

C、系统强制要求定期更改口令 D、用户可以设置空口令

647、在Solaris 8 下，使用ps -ef命令列出进程中有一行如下“root 1331 0 00:01:00? 0:00 /usr/sbin/inetd -s -t”，以下说法正确的是（ABE）

A、参数-t是trace，记录包括IP和PORT等信息

B、参数-t对于UDP服务无效 C、进程启动的时间不能确定

D、进程已经运行了1分钟 E、进程的父进程号是1

648、在Solaris 8 下，以下说法正确的是：（AB）

A、/etc/rc2.d里S开头的文件在系统缺省安装的缺省级别会自动运行

B、/etc/rc3.d里S开头的文件在系统缺省安装的缺省级别会自动运行

C、/etc/init.d里的文件在系统启动任何级别时会自动运行

D、init 0是进入单用户级别 E、init 6命令会运行所有级别的rc目录下以S开头的文件

649、在Solaris 8 下，以下说法正确的是：（BC）

A、PATH环境变量最后带有“.”，会使当前目录的命令比其他目录的命令有限执行

B、可以修改/etc/inittab里ttymon的参数，使得登录的SHELL在无输入时自动退出

C、在使用/bin/ksh时，可以设置TMOUT值，使得登录的SHELL在无输入时自动退出

D、在/etc/login中，可以设置TIMEOUT值，使得登录的SHELL在无输入时自动退出

E、tar xvf命令的意思是以tar格式解开输入，并且保持文件属性等参数不变

650、在配置Apache访问控制时，Allow和Deny指令可以允许或拒绝来自特定主机名或主机名地址的访问。那么下列哪些配置是不正确的？（AD）

A、Order allow,deny Allow from 192.101.205

B、B、Order deny,allow Deny from all Allow from example

C、C、Order deny,allow Deny from 192.101.205

D、D、Order allow,deny Deny from 192.101.205 Allow from all

651、造成操作系统安全漏洞的原因是（ABC）。

A、不安全的编程语言 B、不安全的编程习惯

C、考虑不周的架构设计 D、人为的恶意破坏

652、针对Linux主机，一般的加固手段包括（ABC）。

A、打补丁 B、关闭不必要的服务 C、限制访问主机 D、切断网络

653、做系统快照，查看端口信息的方式有（AD）。

A、netstat -an B、net share C、net use D、用taskinfo来查看连接情况

654、网厅安全解决方案主要从哪几个方面对网厅安全进行建议和指导？（ABCD）

A、安全管理 B、安全防护 C、安全运维 D、灾备/恢复

655、IT系统软件设计中应当考虑并执行安全审计功能，详细记录访问信息的活动，包括（ABCD）。

A、记录的活动以是否有数据的修改、应用程序的异常关闭、异常删除触发

B、应用系统应当配置单独的审计数据库，审计记录应单独存放，并设置严格的边界访问控制，只有安全管理人员才能够看到审计记录

C、信息系统的审计功能包括：事件日期、时间、发起者信息、类型、描述和结果

D、应用系统的审计进程为后台处理，与应用系统运行同步进行，并且对于审计进程应当涉及相应的守护进程，一旦出现异常停止系统可重新启动审计进程，从而保障审计的“完整性”

656、IPSec的配置步骤包括：（ABCD）

A、防火墙基本配置 B、定义保护数据流和域间规则

C、配置IPSec安全提议 D、配置IKEPeer

657、Juniper路由器在配置SSH访问时应注意如下（ABCD）细节。

A、建立允许访问的SSH-ADDRESSES过滤器

B、确保只允许来自内部接口的授权用户访问

C、针对SSH进行限速以保护路由引擎

D、过滤器应用在loopback接口

658、对于使用RPF反向地址验证，以下说法错误的是：（BCD）。

A、对称路由可以使用 B、非对称路由可以使用

C、有些情况不可以使用，但与对称或非对称路由无关

D、在任何情况下都可以使用

659、防病毒服务升级检查包括如下几项内容？（ABC）

A、检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决

B、在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本

C、对重要的服务器，定期抽查防病毒客户端的病毒库升级情况

660、防范DOS攻击的方法主要有（ABCD）。

A、安装Dos检测系统 B、对黑洞路由表里的地址进行过滤

C、及时打好补丁 D、正确配置TCP/IP参数

661、防火墙trust域中的客户机通过nat访问untrust中的服务器的ftp服务，已经允许客户机访问服务器的tcp21端口，但只能登陆到服务器，却无法下载文件，以下解决办法中可能的是：（ABC）

A、修改trust untrust域间双向的默认访问策略为允许

B、FTP工作方式为port模式时，修改untrust trust域间in方向的默认访问策略为允许 C、在trust untrust域间配置中启用detect ftp

D、FTP工作方式为passive模式时，修改untrust trust域间in方向的默认访问策略为允许

662、防火墙不能防止以下哪些攻击？（ABD）

A、内部网络用户的攻击 B、传送已感染病毒的软件和文件

C、外部网络用户的IP地址欺骗 D、数据驱动型的攻击

663、防火墙常见的集中工作模式有（ABC）。

A、路由 B、NAT C、透明 D、旁路

664、防火墙的缺陷主要有（ABCD）。

A、限制有用的网络服务 B、无法防护内部网络用户的攻击

C、不能防备新的网络安全问题 D、不能完全防止传送已感染病毒的软件或文件

665、防火墙的日志管理应遵循如下原则：（BC）

A、本地保存日志 B、本地保存日志并把日志保存到日志服务器上

C、保持时钟的同步 D、在日志服务器保存日志

666、防火墙的特征是（ABCD）。

A、保护脆弱和有缺陷的网络服务 B、加强对网络系统的访问控制

C、加强隐私，隐藏内部网络结构 D、对网络存取和访问进行监控审计

667、防火墙的主要功能有哪些？（ABCD）

A、过滤进、出网络的数据 B、管理进、出网络的访问行为

C、封堵某些禁止的业务，对网络攻击进行检测和报警

D、记录通过防火墙的信息内容和活动

668、防火墙的作用主要有（ABCD）。

A、实现一个公司的安全策略 B、创建一个阻塞点

C、记录Internet活动 D、限制网络暴露

669、防火墙技术，涉及到（ABCD）。

A、计算机网络技术 B、密码技术 C、软件技术 D、安全操作系统

670、防火墙可以部署在下列位置：（ABCD）。

A、安全域边界 B、服务器区域边界

C、可信网络区域和不可信网络区域之间 D、根据网络特点设计方案

671、防火墙配置时应确保（ABCD）服务不开放。

A、Rlogin B、NNTP C、Finger D、NFS

672、启用Cisco设备的访问控制列表，可以起到如下作用（ABC）。

A、过滤恶意和垃圾路由信息 B、控制网络的垃圾信息流

C、控制未授权的远程访问 D、防止DDoS攻击

673、如果Cisco设备的VTY需要远程访问，则需要配置（ABCD）。

A、至少8位含数字、大小写、特写字符的密码 B、远程连接的并发数目

C、访问控制列表 D、超市退出

674、如果需要配置Cisco路由器禁止从网络启动和自动从网络下载初始配置文件，配置命令包括（AB）。

A、no boot network B、no service config C、no boot config D、no service network

675、入侵检测的内容主要包括：（BC）。

A、独占资源、恶意使用 B、试图闯入或成功闯入、冒充其他用户

C、安全审计 D、违反安全策略、合法用户的泄露

676、入侵检测系统包括以下哪些类型？（AC）

A、主机入侵检测系统 B、链路状态入侵检测系统

C、网络入侵检测系统 D、数据包过滤入侵检测系统

677、随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器（sniffer）来监听整个子网的办法不再可行。可选择解决的办法有（ABCD）。

A、使用交换机的核心芯片上的一个调试的端口

B、把入侵检测系统放在交换机内部或防火墙等数据流的关键入口

C、采用分解器（tap）

D、使用以透明网桥模式接入的入侵检测系统

678、通常要求把路由器的日志存储在专用日志服务器上，假设把Cisco路由器日志存储在192.168.0.100的syslog服务器上，需要在路由器侧配置的操作时：（ABCD）。

A、使用Router(config)# logging on启用日志：使用Router(config)# logging trap information将记录日志级别设定为“information”

B、使用Routee(config)# logging192.168.0.100将记录日志类型设定为“local6”

C、使用(config)# logging facility local6将日志发送到192.168.0.100

D、使用(config)# logging sourceinterface loopback0设定日志发送源loopback0

679、通过SSL VPN接入企业内部的应用，其优势体现在哪些方面：（ABCD）。

A、应用代理 B、穿越NAT和防火墙设备

C、完善的资源访问控制 D、抵御外部攻击

680、网络地址端口转换（NAPT）与普通地址转换有什么区别？（AD）

A、经过NAPT转换后，对于外网用户，所有报文都来自于同一个IP地址

B、NAT只支持应用层的协议地址转换

C、NAPT只支持网络层的协议地址转换

D、NAT支持网络层的协议地址转换

681、网络攻击的类型包括以下哪几种？（ABCD）

A、窃取口令 B、系统漏洞和后门 C、协议缺陷 D、拒绝服务

682、网络面临的典型威胁包括（ABCD）。

A、未经授权的访问 B、信息在传送过程中被截获、篡改

C、黑客攻击 D、滥用和误用

683、网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，该类病毒程序大规模爆发后，会对相关网络造成拒绝服务攻击，为了防止受到网络蠕虫的侵害，应当注意对（ACD）及时进行升级更新。

A、计算机操作系统 B、计算机硬件 C、文字处理软件 D、应用软件

684、下列关于NAT地址转换的说法中哪些事正确的：（ABCD）。

A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

B、地址转换可以按照用户的需要，在局域网内向外提供FTP、WWW、Telnet等服务

C、有些应用层协议在数据中携带IP地址信息，对它们作NAT时还要修改上层数据中的IP地址信息

D、对于某些非TCP、UDP的协议（如ICMP、PPTP），作上层NAT时，会对它们的特征参数（如ICMP的id参数）进行转换。

685、下列哪两项正确描述了由WPA定义的无线安全标准？（BC）

A、使用公开密钥的认证方法 B、当客户端连接的时候都要进行动态密钥交换

C、包含PSK认证 D、定制了一个经常更换的静态的加密密钥来增强安全性

686、下列配置中，可以增强无线AP（access point）安全性的有（ABCD）。

A、禁止SSID广播 B、禁用DHCP服务

C、采用WPA2-PSK加密认证 D、启用MAC地址接入过滤

687、下面可以攻击状态检测的防火墙方法有：（ABD）

A、协议隧道攻击 B、利用FTP-pasv绕过防火墙认证的攻击

C、ip欺骗攻击 D、反弹木马攻击

688、下面什么路由协议不可以为HSRP的扩充：（ABC）

A、SNMP B、CDP C、HTTP D、VRRP

689、下面什么协议有MD5认证：（ABC）

A、BGP B、OSPF C、EIGER D、RIPversion 1

690、下面是网络安全技术的有：（ABC）

A、防火墙 B、防病毒 C、PKI D、UPS

691、选购一个防火墙时应该考虑的因素有：（ABCD）

A、网络受威胁的程度 B、可能受到的潜在损失

C、站点是否有经验丰富的管理员 D、未来扩展的需要

692、一台路由器的安全快照需要保存如下哪些信息？（AB）

A、当前的配置--running-config B、当前的开放端口列表

C、当前的路由表 D、当前的CPU状态

693、以下对于包过滤防火墙的描述正确的有（ACD）。

A、难以防范黑客攻击 B、处理速度非常慢

C、不支持应用层协议 D、不能处理新的安全威胁

694、以下对于代理防火墙的描述正确的有（ABCD）。

A、能够理解应用层上的协议 B、时延较高，吞吐量低

C、能做复杂一些的访问控制，并做精细的认证和审核 D、可伸缩性较差

695、以下关于L2TP VPN配置注意事项的说法中正确的有：（ABC）

A、L2TP的LNS端必须配置虚拟接口模板（Virtual-Template）的IP地址，该虚拟接口模板需要加入域

B、防火墙缺省需要进行隧道的认证。如果不配置认证，需要undo tunnel authentication命令

C、为了使L2TP拨号上来的用户分配的地址不能喝内网用户的地址在同一个网段

D、LNS端不允许配置多个L2TP-Group

1. 以下哪几项关于安全审计和安全审计系统的描述是正确的？（CD）

A、对入侵和攻击行为只能起到威慑作用

B、安全审计不能有助于提高系统的抗抵赖性

C、安全审计是对系统记录和活动的独立审查和检验

D、安全审计系统可提供侦破辅助和取证功能

697、以下哪些属于网络欺骗方式？（ABCD）

A、IP欺骗 B、ARP欺骗 C、DNS欺骗 D、Web欺骗

698、以下哪些是防火墙规范管理需要的？（ABCD）

A、需要配置两个防火墙管理员 B、物理访问防火墙必须严密地控制

C、系统软件、配置数据文件在更改后必须进行备份

D、通过厂商指导发布的硬件和软件的bug和防火墙软件升级版

699、以下硬件安装维护重要安全提示正确的有：（ABCD）

A、不要在雷雨天气进行故障处理 B、保持故障处理区域的干净、干燥

C、上防静电手套或防静电腕带再执行安装和更换操作

D、在使用和操作设备时，需要按照正确的操作流程来操作

700、以下属于DTE(Data Terminal Equipment)数据终端设备的有（AB）

A、路由器 B、PC C、交换机 D、HUB

701、在防火墙的“访问控制”应用中，内网、外网、DMZ三者的访问关系为：（ABD）

A、内网可以访问外网 B、内网可以访问DMZ区

C、DMZ区可以访问内网 D、外网可以访问DMZ区

702、关于GRE校验和验证技术，当本端配置了校验和而对端没有配置校验和时，以下叙述正确的有（BC）。

A、本端对接收报文检查校验和 B、对端对接收报文检查校验和

C、本端对发送报文计算校验和 D、对端对发送报文计算校验和

703、配置PPP链路层协议时，链路层协议状态始终不能转为Up状态的处理建议：（ABCD）

A、PPP链路两端的接口上配置的参数和验证方式都必须一致，LCP检查才能成功

B、如果LCP协商失败，请检查LCP配置协商参数

C、请检查验证方式配置是否正确。因为LCP协商中，包含验证方式的协商。因为LCP协商中，包含验证方式的协商。验证方式协商失败也会导致LCP协商失败

D、接口试图下先执行shutdown命令将接口关闭，再执行undo shutdown命令重启接口

704、对DNSSEC的描述正确的有（AC）。

A、为DNS数据提供来源验证，即保证数据来自正确的名称服务器

B、DNSSEC可防御DNS Query Flood攻击

C、为域名数据提供完整性验证，即保证数据在传输的过程中没有被篡改

D、实施DNSSEC后，只需升级软件系统，对网络、服务器等硬件设备不需考虑

705、MySQL安装程序会给出三种选择，用户可以根据自身的需要选择一种适合的安装方式，以下哪些是正确的？（ABD）

A、Typical（典型安装） B、Compact(最小安装)

C、Full(全部安装) D、Custom(选择安装)

706、MySQL中用DROP语句可删除数据库和数据表，以下哪句是正确的语法？（ABCD）

A、DROP TABLE table\_name1 B、DROP TABLE table\_name1,table\_name2

C、DROP TABLE IF EXISTS table\_name1 D、DROP DATABASE DB name1

707、Oracle 7.2之前的数据库连接用户名和密码在网络传输时是不进行加密的，为了要和旧版本兼容Oracle数据库9.02存在DBLINK\_ENCRYPT\_LOGIN参数用来调节数据库连接时用户名和密码的加密特性，以下说法正确的是：（ACD）。

A、DBLINK\_ENCRYPT\_LOGIN为TRUE时，数据库连接加密用户名和密码

B、DBLINK\_ENCRYPT\_LOGIN时，数据库连接不加密用户名和密码

C、DBLINK\_ENCRYPT\_LOGIN为FALSE时，如果加密的数据库连接失败，会尝试不加密的连接

D、DBLINK\_ENCRYPT\_LOGIN为TRUE时，加密的数据库连接失败，也不会尝试不加密的连接

708、Oracle实例主要由哪两部分组成：（AC）

A、内存 B、Share pool buffer C、后台进程 D、pmon和smon

709、Oracle中如何设置audit trail审计，正确的说法是：（ABD）

A、在init.ora文件中设置“audit\_trail = true”或者“audit\_trail = db”

B、以SYSDBA身份使用AUDIT ALL ON SYS.AUD$ BY ACCESS，语句对audit trail审计

C、Oracle不支持对audit trail的审计

D、在设置audit trail审计前，要保证已经打开Oracle的审计机制

710、SQL Server的登录认证种类有以下哪些？（ACD）

A、Windows认证模式 B、双因子认证模式

C、混合认证模式 D、SQL Server认证

711、SQL Server的取消权限的操作有以下哪些？（ABC）

A、在“详细信息”窗格中右击要授予/拒绝/取消其权限的用户定义的角色

B、单击“属性”命令在“名称”下单击“权限”单击列出全部对象

C、选择在每个对象上授予拒绝或废除的权限，选中标志表示授予权限，X表示拒绝权限，空框表示废除权限，只列出适用于该对象的权限

D、回到“数据库用户属性”对话框中，再点击“确定”按钮，所有的设置就完成了

712、SQL Server中ALTER DATABASE可以提供以下哪些功能选项？（ABCD）

A、更改数据库名称 B、文件组名称 C、数据文件 D、日志文件的逻辑名称

713、SQL Server中关于实例的描述，请选择正确的答案。（ABD）

A、如果安装选择“默认”的实例名称。这时本SQL Server的名称将和Windows 2000服务器的名称相同

B、SQL Server可以在同一台服务器上安装多个实例

C、SQL Server只能在一台服务器上安装一个实例

D、实例各有一套不为其他实例共享的系统及用户数据库，所以各实例的运行是独立的。

714、SQL Server中使用企业管理器从数据库中删除数据或日志文件的步骤如下，正确的步骤是？（ABCD）

A、展开服务器组，然后展开服务器

B、展开“数据库”文件夹，右击要从中删除数据或日志文件的数据库，然后单击“属性”命令

C、若要删除数据文件，单击“常规”选项卡。若要删除日志文件，单击“事务日志”选项卡

D、在“文件名”列户，单击要删除的文件名旁边的箭头，再点DELETE键，文件名旁出现十字光标，表明将删除此文件

715、参数REMOTE\_LOGIN\_PASSWORDFILE在Oracle数据库实例的初始化参数文件中，此参数控制着密码文件的使用及其状态，以下说法正确的是：（ABCD）

A、NONE：只是Oracle系统不使用密码文件，不允许远程管理数据库

B、EXCLUSIVE：指示只有一个数据库实例可以使用密码文件

C、SHARED：指示可有多个数据库实例可以使用密码文件

D、以上说法都正确

716、关于SQL Server 2000中的SQL账号、角色，下面说法正确的是：（ABC）

A、PUBLIC,guest为缺省的账号 B、guest不能从master数据库清除

C、可以通过删除guest账号的角色，从而消弱guest可能带来的安全隐患

D、SQL Server角色的权限是不可以修改的

717、连接MySQL后选择需要的数据库DB\_NAME？以下哪些方法是对的（AC）

A、连接后用USE DB\_NAME选择数据库

B、连接后用SET DB\_NAME选择数据库

C、用mysql -h host -u user -p DB\_NAME连接数据库

D、用mysql -h host -u user -p -T DB\_NAME连接数据库

718、如果数据库不需要远程访问，可以禁止远程tcp/ip连接，以增强安全性。可选择的有效方法：（AC）

A、用防火墙封堵数据库侦听端口避免远程连接 B、禁止tcp/ip协议的使用

C、在mysqld服务器中参数中添加 --skip-networking启动参数来使mysql

D、在/etc/my.cnf下添加remoteConnnect=disable

719、以下哪些MySQL中GRANT语句的权限指定符？（ABCDEF）

A、ALTER B、CREATE C、DELETE

D、UPLOAD E、DROP F、INSERT

720、用THC组织的Oracle的工具，通过sniffer方式抓取数据库的认证信息可有效破解Oracle密码，以下哪些数据是必须获取的？（ABC）

A、AUTH\_SESSKEY B、AUTH\_PASSWORD C、用户名 D、实例名

721、在Oracle 9数据库可以通过配置$Oracle\_HOME\network\admin\sqlnet.ora文件实现数据库层次的基于TCP协议和地址的访问控制。下面说法正确的是：（ABCD）

A、首先需要配置TCP,VALIDNODE\_CHECKING=yes启用节点检查功能

B、其次配置TCP.INVITED\_NODES=192.168.0.12，192.168.0.33将会允许地址是192.168.0网段的12和33的主机访问

C、然后配置TCP.EXCLUDED\_NONES=192.168.0.123将会禁止地址是192.168.0网段的123的主机访问

D、要以上配置生效必须重启lsnrctl监听器

722、在SQL Server 2000中，如果想查询当前数据库服务器软件的版本，可以使用下面哪些方式（ABCD）

A、在查询分析器中通过如下语句查询SELECT ServerPROPERTY(‘productversion’),ServerPROPERTY(‘productlevel’),ServerPROPERTY(‘edition’)

B、在命令行下，用SQL Server自带的管理工具osql连接进入数据库，输入select@@version

C、企业管理器查看服务器属性 D、在SQL Server服务管理器里面查看“关于”

723、在SQL Server 2000中一些无用的存储过程，这些存储过程极容易被攻击者利用，攻击数据库系统。下面的存储过程哪些可以用来执行执行系统命令或修改注册表？（ABC）

A、xp\_cmdshell B、xp\_regwrite C、xp\_regdeletekey D、select \* from master

724、在SQL Server中创建数据库，如下哪些描述是正确的？（ABCD）

A、创建数据库的权限默认授权sysadmin和dbcreator固定服务器角色的成员，但是它仍可以授予其他用户

B、创建数据库的用户将成为该数据库的所有者

C、在一个服务器上，最多可以创建32,767个数据库

D、数据库名称必须遵循标示符规则

725、在对SQL Server 2000的相关文件、目录进行安全配置时，下面可以采用的措施是：（ABCD）

A、删除缺省安装时的例子样本库

B、将存放数据的库文件，配置权限为administrators组、system和启动SQL Server服务的用户账号及DBA组具有完全控制权限

C、对SQL Server安装目录，去除everyone的所有控制权限

D、将数据库数据相关的文件，保存在非系统盘的NTFS独立分区

726、sybase数据库文件系统需要哪些裸设备？（ABCD）

A、master B、proce C、data D、log

727、Oracle支持哪些加密方式？（ABCD）

A、DES B、RC4\_256 C、RC4\_40 D、DES40

728、SQL Server用事件探测器可以帮助排除故障和解决问题，创建跟踪的步骤如下哪些是正确的？（ABCD）

A、从“模板名称”下拉菜单为你创建跟踪选择一个模板

B、“事件探查器”主界面打开后，从“文件”菜单选择“新跟踪”

C、在“跟踪名称”文本框中输入你想要为这个跟踪创建的跟踪名称

D、修改这些默认的选项设置。通过点击“显示全部事件”和“显示全部列”复选框来查看其他的选项。

729、最重要的电磁场干扰源是：（BCD）

A、电源周波干扰 B、雷电电磁脉冲LEMP

C、电网操作过电压SEMP D、静电放电ESD

730、雷电侵入计算机信息系统的途径主要有：（ABD）

A、信息传输通道线侵入 B、电源馈线侵入 C、建筑物 D、地电位反击

731、电信生产其机房作业，是由专门的值机员、机务员来完成，作业内容是：固定电话、无线电话、电报、载波、短波、微波、卫星和电力等电信通信设备，使设备出去良好状态，保证其正常运行。（ABCD）

A、安装 B、值守 C、维护 D、检修

732、对计算机系统有影响的腐蚀性气体大体有如下几种：（ABCD）

A、二氧化硫 B、氢化硫 C、臭氧 D、一氧化碳

733、防火工作的基本措施有：（ABCD）

A、加强对人员的教育管理 B、加强对可燃物的管理

C、加强对物的管理 D、加强对火源、电源的管理

734、会导致电磁泄漏的有（ABCDE）

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

E、信号处理电

735、火灾自动报警、自动灭火系统部署应注意（ABCD）。

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、具有自动和手动两种触发装置

736、计算机场地安全测试包括（ABCD）。

A、温度，湿度，尘埃 B、照度，噪声，电磁场干扰环境场强

C、接地电阻，电压、频率 D、波形失真率，腐蚀性气体的分析方法

737、计算机信息系统设备处于不同雷电活动地区，其雷电电磁场强度有很大差异，根据这一差异，将被防护空间分为下列哪些防护区？（ABCD）

A、直击雷非防护区（LPZOA） B、直击雷防护区（LPZOB）

C、第一防护区（LPZI） D、后续防护区（LPZ2,3...等）

738、静电的危害有（ABCD）。

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

739、灭火的基本方法有（ABCD）。

A、冷却法 B、隔离法 C、窒息法 D、抑制

740、实体安全技术包括（ABD）。

A、环境安全 B、设备安全 C、人员安全 D、媒体安全

741、使用配有计算机的仪器设备时，不应该做的有：（ABCD）

A、更改登机密码和系统设置

B、自行安装软件

C、玩各种电脑游戏

D、将获得的图像、数据等资料存储在未予指定的硬盘分区上

742、硬件设备的使用管理包括（ABCD）。

A、严格按硬件设备的操作使用规程进行操作

B、建立设备使用情况日志，并登记使用过程

C、建立硬件设备故障情况登记表

D、坚持对设备进行例行维护和保养

743、预防静电的措施有（ABCD）。

A、接地 B、不使用或安装产生静电的设备

C、不在产生静电场所穿脱工作服 D、作业人员穿防静电鞋

744、在实验室中引起火灾的通常原因包括：（ABCD）

A、明火 B、电器保养不良

C、仪器设备在不使用时未关闭电源 D、使用易燃物品时粗心大意

745、直击雷：直接击在（ABCD）并产生电效应、热效应和机械力的雷电放电。

A、建筑物 B、构建物 C、地面突进物 D、大地或设备

746、员工区域安全守则包括：（ABCD）

A、非工作时间，员工进入或离开办公区域，应在值班人员处登记

B、外来人员进入办公区域或机房，相关员工必须全程陪同

C、将物品带入/带出公司，要遵守公司相关的规定及流程

D、参加会议时遵守会前、会中、会后的保密流程

747、机房出入控制措施包括：（ABCD）

A、机房接待前台须核查弄清业务系统安全区域的来访者的身份，并记录其进入和离开安全区域的日期与时间

B、机房须告知进入安全区的来访者，该区域的安全要求和紧急情况下的行动步骤

C、可采用强制性控制措施，对来访者的访问行为进行授权和验证

D、要求所有进出机房人员佩带易于辨识的标识

748、为了减小雷电损失，可以采取的措施有（ACD）

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

749、安全要求可以分解为（ABCDE）。

A、可控性 B、保密性 C、可用性 D、完整性 E、不可否认性

750、HASH加密使用复杂的数字算法来实现有效的加密，其算法包括（ABC）

A、MD2 B、MD4 C、MD5 D、Cost256

751、利用密码技术，可以实现网络安全所要求的。（ABCD）

A、数据保密性 B、数据完整性 C、数据可用性 D、身份验证

752、一个密码体系一般分为以下哪几个部分？（ABCD）

A、明文 B、加密密钥和解密密钥

C、密文 D、加密算法和解密算法

753、公钥密码体质的应用主要在于。（AC）

A、数字签名 B、加密 C、密钥管理 D、哈希函数

754、目前基于对称密钥体制的算法主要有。（BC）

A、RSA B、DES C、AES D、DSA

755、使用esp协议时，可以使用的加密运算是。（ABC）

A、DES B、3DES C、AES D、RSA

756、数字签名的作用是。（ACD）

A、确定一个人的身份 B、保密性

C、肯定是该人自己的签字 D、使该人与文件内容发生关系

757、以下属于对称加密算法的是：（ABD）

A、DES B、3DES C、SHA-1 D、RC4 E、MD5

758、在加密过程中，必须用到的三个主要元素是（ABC）

A、所传输的信息（明文） B、加密 钥匙（Encryption Key）

C、加密函数 D、传输信道

759、账号口令管理办法适用于所有和DSMP系统、智能网系统、彩铃平台相关的（ACD）

A、系统管理员 B、操作系统

C、操作维护人员 D、所有上述系统中存在的账号和口令

760、为保证密码安全，我们应采取的正确措施有（ABC）

A、不使用生日做密码 B、不使用少于5为的密码

C、不适应纯数字密码 D、将密码设的非常复杂并保证20位以上

761、公司在使用数据签名技术时，除充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名外，还应注意（ABCD）

A、采取保护公钥完整性的安全措施，例如使用公约证书

B、确定签名算法的类型、属性以及所用密钥长度

C、用于数字签名的密钥应不同于用来加密内容的密钥

D、符合有关数字签名的法律法规，必要时，应在合同或协议中规定使用数字签名的相 关事宜

762、相对于对称加密算法，非对称密钥加密算法（ACD）

A、加密数据的速率较低

B、更适合于现有网络中对所传输数据（明文）的加解密处理

C、安全性更好 D、加密和解密的密钥不同

763、一个典型的PKI应用系统包括（ABCD）实体

A、认证机构CA B、册机构RA C、证书及CRL目录库 D、用户端软件

764、加密的强度主要取决于（ABD）

A、算法的强度 B、密钥的保密性 C、明文的长度 D、密钥的强度

765、一下对于对称密钥加密说法正确的是（BCD）

A、对称加密算法的密钥易于管理 B、加解密双方使用同样的密钥

C、DES算法属于对称加密算法 D、相对于非对称加密算法，加解密处理速度比较快

766、在通信过程中，只采用数字签名可以解决（ABC）等问题

A、数据完整性 B、数据的抵抗赖性 C、数据的篡改 D、数据的保密性

767、对称密钥算法体系包括：（ABCDE）

A、明文(plaintext)：原始消息或数据，作为算法的输入

B、加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换

C、秘密密钥(secret key)：秘密密钥也是算法输入，算法进行的具体替换和转换取决于 这个密钥

D、密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对 于一个给定的消息，两个不同的密钥会产生两个不同的密文

、.解密算法(decryption algorithm)：本质上是加密算法的执行。它使用密文和统一密钥 产生原始明文

768、一下对于混合加密方式说法正确的是。（BCD）

A、 使用公开密钥密码体制对要传输的信息（明文）进行加解密处理

B、使用对称加密算法对要传输的信息（明文）进行加解密处理

C、使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信

D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的

769、电信的网页防篡改技术有（ABC）

A、外挂轮询技术 B、核心内嵌技术

C、时间触发技术 D、安装防病毒软件

770、病毒发展的趋势是？（ABC）

A、 范围更广 B、度更快 C、方式更多

771、病毒自启动方式一般有（ABC）

A、 修改注册表 B、将自身添加为服务

C、将自身添加到启动文件夹 D、修改系统配置文件

772、常见Web攻击方法有一下哪种？（ABCD）

A、SQL Injection B、Cookie欺骗 C、跨站脚本攻击

D、信息泄露漏洞 E、文件腹泻脚本存在的安全隐患

F、 GOOGLE HACKING

773、宏病毒感染一下哪些类型的文件？（ABCDEF）

A、DOC B、EXE C、XLS D、DOT

774、木马传播包括一下哪些途径：（ACD）

A、通过电子邮件的附件传播 B、通过下载文件传播

C、通过网页传播 D、通过聊天工具传播

775、目前最好的防病毒软件能做到的是（ABCD）

A、检查计算机是否感染病毒，消除已感染的任何病毒

B、杜绝病毒对计算的侵害

C、查出计算机已感染的已知病毒，消除其中的一部分

D、检查计算机是否染有已知病毒，并作相应处理

776、通用的DoS攻击手段有哪些？（CD）

A、 SYN Attack B、ICMP Flood C、UDP Flood

D、Ping of Death E、Tear Drop F、Ip Spoofing

777、以下关于蠕虫的描述正确的有：（ABCDEF）

A、 蠕虫具有自动利用网络传播的特点，在传播的同时，造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪

B、 隐藏式蠕虫的基本特征，通过在主机上隐藏，使得用户不容易发现它的存在

C、蠕虫需要传播受感染的宿主文件来进行复制

D、蠕虫的传染能力主要是针对计算机内的文件系统。

778、以下哪几种扫描检测技术属于被动式的检测技术？（AB）

A、 基于应用的检测技术 B、基于主动的检测技术

C、基于目标的漏洞检测技术 D、基于网络的检测技术

779、以下是检查磁盘与文件是否被病毒感染的有效方法：（BC）

A、 检查磁盘目录中是否有病毒文件 B、用抗病毒软件检查磁盘的各个文件

C、用放大镜检查磁盘编码是否有霉变现象 D、检查文件的长度是否无故变化

780、造成计算机不安全的因素有（BD）等多种。

A、 技术原因 B、自然原因 C、认为原因 D、管理原因

781、嗅探技术有哪些特点？（ABCD）

A、间接性 B、.直接性 C、隐蔽性 D、开放性

782、一个恶意的攻击者必须具备哪几点？（ABC）

A、 方法 B、机会 C、动机 D、运气

783、对于DOS网络攻击，可以采用以下哪些措施来缓解主机系统被攻击进程。（ACD）

A、缩短SYN Timeout时间和设置SYN Cookie B、增加网络带宽

C、在系统之前增加负载均衡设备 D、在防火墙上设置ACL或黑客路由

784、利用Bind/DNS漏洞攻击的分类主要有（ACD）

A、 拒绝服务 B、匿名登录 C、.缓冲区溢出

D、DNS缓存中毒 E、病毒或后门攻击

785、常见Web攻击方法有一下哪种？（ABCD）

A、 SQL Injection B、 Cookie欺骗 C、 跨站脚本攻击 D、信息泄露漏洞

786、黑客所使用的入侵技术主要包括（ABCDE）

A、协议漏洞渗透 B、密码分析还原 C、应用漏洞分析与渗透

D、拒绝服务攻击 E、病毒或后门攻击

787、主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有（ABC）

A、针对入侵者采取措施 B、修正系统

C、收集更详细的信息 D、入侵追踪

788、下面哪些漏洞属于网络服务类安全漏洞：（BC）

A、Windows 2000中文版输入法漏洞 B、IS Web服务存在的IDQ远程溢出漏洞

C、RPC DCOM服务漏洞 D、Web服务asp脚本漏洞

789、系统感染病毒后的现象有哪些？（ABCD）

A、系统错误或系统崩溃 B、系统反应慢，网络拥塞

C、陌生的进程或服务 D、陌生的自启动

**三、判断题：（790-1000）**

790、TCSEC将信息安全风机防护等级一共分为7个安全等级：D、C1、C2、B1、B2、B3、 A。(A)

A、正确 B、错误

791、通用标准v2版（CC）的安全等级是以EAL来表示的。（A）

A、正确 B、错误

792、一个企业的信息安全组织能否顺利开展工作（定期安全评估、日志安全巡检、定期安全审核、应急演练等），主要取决于公司领导对信息安全工作的认识程度和支持力度。（A）

A、正确 B、错误

793、在信息安全领域，CIA通常是指：保密性、完整性和可用性。（A）

A、正确 B、错误

794、信息安全是永远是相对的，并且需要不断持续关注和改进，永远没有一劳永逸的安全

防护措施。（A）

A、正确 B、错误

795、在信息安全领域，CIA通常是指：保密性、完整性和非抵赖性。（B）

A、正确 B、错误

796、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

797、信息安全的威胁主体包括内部人员、准内部人员、外部人员、系统自身等方面。（B）

A、正确 B、错误误

798、互联网网络安全事件根据危害和紧急程度分为一般、预警、报警、紧急、重大五种。 （B）

A、正确 B、错误

799、安全审计是从管理和技术两个方面检查公司的安全策略和控制措施的执行情况，发现安全隐患的过程。（A）

A、正确 B、错误

800、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

801、计算机系统安全是指应用系统具备访问控制机制，数据不被泄露、丢失、篡改等。（B）

A、正确 B、错误

802、主机加固完成后，一般可以有效保证主机的安全性增强。（A）

A、正确 B、错误

803、黑客在进行信息收集时，通常利用Windows的IPC漏洞可以获得系统用户的列表的信 息。（A）

A、正确 B、错误

804、Solaris系统中一般需要确认ROOT账号只能本地登录，这样有助于安全增强。（A）

A、正确 B、错误

805、HP-UX系统加固中在设置ROOT环境变量不能有相对路径设置。（A）

A、正确 B、错误

806、屏幕保护的木马是需要分大小写。（B）

A、正确 B、错误

807、安全审计就是日志的记录。（B）

A、正确 B、错误误

808、HP-UX系统加固中在设置通用用户环境变量不能有相对路径设置。（A）

A、正确 B、错误

809、AIX系统加固时，对系统配置一般需要自编脚本完成。（A）

A、正确 B、错误

810、Windows NT中用户登录域的口令是以明文方式传输的。（B）

A、正确 B、错误

811、操作系统普通用户账号审批记录应编号、留档。（A）

A、正确 B、错误

812、计算机病毒是计算机系统中自动产生的。（B）

A、正确 B、错误

813、主机系统加固时根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。（A）

A、正确 B、错误

814、4A系统的建设能够减轻账户管理员的维护工作。（A）

A、正确 B、错误

815、4A系统的接入管理可以管理到用户无力访问的接入。（B）

A、正确 B、错误

816、Cisco路由器可以使用enable password命令为特权模式的进入设置强壮的密码。（B）

A、正确 B、错误

817、Cisco设备的AUX端口默认是启用的。（A）

A、正确 B、错误

818、DHCP可以向终端提供IP地址、网关、DNS服务器地址等参数。（A）

A、正确 B、错误误

819、Inbound方向的NAT使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际IP地址。（B）

A、正确 B、错误

820、IPS设备即使不出现故障，它仍然是一个潜在的网络瓶颈，需要强大的网络结构来配合。（A）

A、正确 B、错误

821、IPS的过滤器规则不能自由定义。（B）

A、正确 B、错误

822、IPS的某些功能和防火墙类似。（A）

A、正确 B、错误

823、IPS和IDS都是主动防御系统。（B）

A、正确 B、错误

824、NAT是一种网络地址翻译的技术，它能是的多台没有合法地址的计算机共享一个合法的IP地址访问Internet。（A）

A、正确 B、错误

825、Netscreen的ROOT管理员具有的最高权限，为了避免ROOT管理员密码被窃取后造成威胁，应该限制ROOT只能通过CONSOLE接口访问设备，而不能远程登录。(A)

A、正确 B、错误

826、Netscreen防火墙的外网口应禁止PING测试，内网口可以不限制。（B）

A、正确 B、错误

827、OSI是开放的信息安全的缩写。（B）

A、正确 B、错误

828、OSI七层模型中，传输层数据成为段（Segment），主要是用来建立主机端到端连接，包括TCP和UDP连接。（A）

A、正确 B、错误

829、OSI中会话层不提供机密性服务。（A）

A、正确 B、错误

830、SSH使用TCP 79端口的服务。（B）

A、正确 B、错误

831、TCP/IP模型从下至上分为四层：物理层，数据链路层，网络层和应用层。（B）

A、正确 B、错误

832、TCP/IP模型与OSI参考模型的不同点在于TCP/IP把表示层和会话层都归于应用层，所以TCP/IP模型从下至上分为五层：物理层，数据链路层，网络层，传输层和应用层。 （A）

A、正确 B、错误

833、TCP/IP协议体系结构中，IP层对应OSI/RM模型的网络层。（A）

A、正确 B、错误

834、默认情况下需要关闭Cisco设备的Small TCP/UDP服务。（A）

A、正确 B、错误

835、缺省情况下，防火墙工作模式为路由模式，切换工作模式后可直接进行进一步配置。（B）

A、正确 B、错误

836、入侵检测具有对操作系统的校验管理，判断是否有破坏安全的用户活动。（A）

A、正确 B、错误

837、入侵检测可以处理数据包级的攻击。（B）

A、正确 B、错误

838、入侵检测系统不能弥补由于系统提供信息的质量或完整性的问题。（A）

A、正确 B、错误

839、入侵检测系统能够检测到用户的对主机、数据库的网络操作行为。（B）

A、正确 B、错误

840、入侵检测系统是一种对计算机系统或网络事件进行检测并分析这个入侵事件特征的过程。（A）

A、正确 B、错误

841、统计分析的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。（B）

A、正确 B、错误

842、统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。（A）

A、正确 B、错误

843、透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决IP地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的IP的地址。（A）

A、正确 B、错误

844、完整性分析的缺点是一般以批处理方式实现，不用于实时响应。（A）

A、正确 B、错误

845、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（B）

A、正确 B、错误

846、网络边界的Cisco路由器应关闭CDP服务。（A）

A、正确 B、错误

847、网络边界Cisco设备的CDP协议可以开放。（B）

A、正确 B、错误

848、网络层的防护手段（防火墙，SSL，IDS，加固）可以组织或检测到应用层攻击。（B）

A、正确 B、错误

849、针对不同的攻击行为，IPS只需要一个过滤器就足够了。（B）

A、正确 B、错误

850、主机型IDS其数据采集部分当然位于其所检测的网络上。（B）

A、正确 B、错误

851、状态检测防火墙检测每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。（B）

A、正确 B、错误

852、IPS虽然能主动防御，但是不能坚挺网络流量。（B）

A、正确 B、错误

853、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。（B）

A、正确 B、错误

854、审计系统进行关联分析时不需要关注日志时间。（B）

A、正确 B、错误

855、垃圾邮件一般包括商业广告、政治邮件、病毒邮件、而已欺诈邮件（网络钓鱼）等几个方面。（A）

A、正确 B、错误

856、防止网络窃听最好的方法就是给网上的信息加密，是的侦听程序无法识别这些信息模式。（A）

A、正确 B、错误

857、侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。（A）

A、正确 B、错误

858、模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。（A）

A、正确 B、错误

859、入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。（A）

A、正确 B、错误

860、VPN的主要特点是通过加密是信息安全的通过Internet传递。（A）

A、正确 B、错误

861、传输层协议使用端口号（Port）来标示和区分上层应用程序，如：Telnet协议用的是23号端口、DNS协议使用69号端口。（B）

A、正确 B、错误

862、如果Web应用对URL访问控制不当，可能造成用户直接在浏览器中输入URL，访问不该访问的页面。（A）

A、正确 B、错误

863、如果Web应用没有对攻击者的输入进行适当的编码和过滤，就用于构造数据库查询或操作系统命令时，可能导致注入漏洞。（A）

A、正确 B、错误

864、HTTP协议定义了Web浏览器向Web服务器发生Web页面请求的格式及Web页面在Internet上传输的方式。（A）

A、正确 B、错误

865、HTTP协议是文本协议，可利用回车换行做边界干扰。（A）

A、正确 B、错误

866、Init<sid>.ora文件是Oracle启动文件，任何参数的配置错误都会造成Oracle不能启动，任何参数的不合理配置都可能造成系统故障。（A）

A、正确 B、错误

867、Mysqldump是采用SQL级别的备份机制，它将数据表导成SQL脚本文件，在不同的MySQL版本之间升级时相对比较合适，这也是最常见的备份方法。（A）

A、正确 B、错误

868、Orabrute是进行远程破解Oracle密码的工具，要猜解的密码可以在password.txt中设置。（A）

A、正确 B、错误

869、Oracle的SYS账户在数据库中具有最高权限，能够做任何事情，包括启动/关闭Oracle数据库。即使SYS被锁定，也已然能够访问数据库。（A）

A、正确 B、错误

870、Oracle的若算法加密机制：两个相同的用户名和密码在两个不同的Oracle数据库机器中，将具有相同的哈希值。（A）

A、正确 B、错误

871、Oracle密码允许包含像“SELECT”，“DELETE”，“CREATE”这类的Oracle/SQL关键字。（B）

A、正确 B、错误

872、Oracle的HTTP的基本验证可选择SYS破解，因为它始终存在和有效。（A）

A、正确 B、错误

873、Oracle默认情况下，口令的传输方式是加密。（B）

A、正确 B、错误

874、Oracle数据库的归档日志不是在线日志的备份。（B）

A、正确 B、错误

875、OSI网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。（A）

A、正确 B、错误

876、OSI网络安全体系结构的五类安全服务是鉴别、访问控制、保密性、完整性、抗否认。（A）

A、正确 B、错误

877、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因。（A）

A、正确 B、错误

878、SQL Server如果设置了不恰当的数据库文件权限，可能导致敏感文件被非法删除或读取，威胁系统安全。（A）

A、正确 B、错误

879、SQL Server数据库应禁止使用除tcp/ip以外的协议，保护数据库通信安全。（A）

A、正确 B、错误

880、SQL Server应该社会自日志审核无法追踪回溯安全事件。（A）

A、正确 B、错误

881、Web服务器一般省缺不允许攻击者访问Web根目录以外的内容，内容资源不可以任意访问。(A)

882、Web攻击面不仅仅是浏览器中可见的内容。（A）

A、正确 B、错误

883、Web应用对网络通讯中包含的敏感信息进行加密，就不会被窃听。（B）

A、正确 B、错误

884、暴力猜解不能对Web应用进行攻击。（B）

A、正确 B、错误

885、在Oracle自身的配置上做限定方法是：修改$Oracle\_HOME\network\admin目录下面的SQLNET..ORA文件，类似设置如下：

Tcp\_validnode\_checking=YES

Tcp\_invited\_nodes=

(192.168.0.1,ip2,ip3•••...)。

( A )

A、正确 B、错误

886、不设置必要的日志审核，就无法追踪回溯安全事件，Oracle中若果要审计记录成功的登陆语句”SQL>audit session whenever successful;”. ( A )

A、正确 B、错误

887、对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是DNS服务器。（B）

A、正确 B、错误

888、防止XSS各种方法都有优劣之处，防范XSS的真正挑战不在于全免，而在于细致。（B）

A、正确 B、错误

889、访问控制、强制登陆、自动安全更新都属于Window2000的安全组件（B）

A、正确 B、错误

890、复杂的系统存在大量的相互引用访问，如果开发者不能有效的进行权限控制，就可能被恶意引用。（A）

A、正确 B、错误

891、攻击者可以通过SQL注入手段获取其他用户的密码。（A）

A、正确 B、错误

892、几乎所有的关系数据库系统和相应的SQL语言都面临SQL注入的潜在威胁。（A)

A、正确 B、错误

893、简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架（B）

A、正确 B、错误

894、默认可通过Web程序来远程管理Oracle10g数据库，端口是8080.（A）

A、正确 B、错误

895、如果sa是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。（A）

A、正确 B、错误

896、如果在SQL Server等领域成功并不意味这该用户已经可以访问SQL Server上的数据库。（A）

A、正确 B、错误

897、如果知道Oracle密码长度，用Rainbow表生成器来破解其密码哈希值是绝对成功的。（A）

A、正确 B、错误

898、所有操作系统、数据库、网络设备，包括一部分业务系统，均需要支持基于账号的访问控制功能。（B）

A、正确 B、错误

899、网络拓扑分析为检查是否有配置错误项泄露内部IP地址，从而推断网站系统拓扑。（A）

A、正确 B、错误

900、为Oracle数据库安全考虑，在对人共同对数据库进行维护时应依赖数据库预定义的传统角色。（B）

A、正确 B、错误

901、为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。(A)

A、正确 B、错误

902、系统类型鉴别为检查主机系统与开放服务是否存在安全漏点。（B）

A、正确 B、错误

903、系统漏洞扫描为检查目标的操作系统与应用系统信息。（B）

A、正确 B、错误

904、选择远程破解Oracle的最好账户是SYS，因为此账户永远有效。（A）

A、正确 B、错误

905、一封电子邮件可以拆分成对个IP包，每个IP包可以沿不同的路径到达目的地。（A）

A、正确 B、错误

906、一个共享文件夹。将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有读取的权限。（A）

A、正确 B、错误

907、用Sqlplus登陆到Oracle数据库，使用slesct username, password form dba\_users命令可查看数据库中的用户名和密码明文。（B）

A、正确 B、错误

908、有的Web应用登陆界面允许攻击者暴力猜解口令，在自动工具与字典表的帮助下，可以迅速找到弱密码用户。（A）

A、正确 B、错误

909、在Oracle所有版本在安装的时候都没有提示修改SYS的默认密码。（B）

A、正确 B、错误

910、在ORacle数据库安装补丁时，不需要关闭所有与数据库有关的服务。（B）

A、正确 B、错误

911、在SQL Server安装SP3补丁时不需要系统中已经安装了SP1或SP2。（B）

A、正确 B、错误

912、在SQL Server中具有sysadmin权限的用户可以通过xp\_cmdshell存储扩展以system的权限执行任意系统命令。（A）

A、正确 B、错误

913、Oracle默认配置下，每个账户如果有30次的失败登陆，此账户将被锁定。（B）

A、正确 B、错误

914、定制开发Web系统的安全度不如标准的产品。（A）

A、正确 B、错误

915、对MySQL注入攻击时，经常用到注释符号#来屏蔽剩下的内置SQL语句。（A）

A、正确 B、错误

916、一个登录名只能进入服务器，但是不能让用户访问服务器中的数据库资源。每个登录名的定义存放在msater数据库的syslogins表中。（A）

A、正确 B、错误

917、Web错误信息可能泄露服务器型号版本、数据库型号、路径、代码。（A）

A、正确 B、错误

918、Oracle的密码哈希值存储在SYS.USER$表中。可以通过像DBA USERS这类的视图来访问。（A）

A、正确 B、错误

919、产品的定制开发是应用安全中最薄弱的一环。（A）

A、正确 B、错误

920、Oracle限制了密码由英文字母，数字，#，下划线（\_），美元字符（$）构成，密码的最大长度为30字符；并不能以”$”,”#”,”\_”或任何数字开头。（A）

A、正确 B、错误

921、网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。（B）

A、正确 B、错误

922、计算机场地可以选择在公共区域人流量比较大的地方。（B）

A、正确 B、错误

923、EMC测试盒约束用户关心的信息信号的电磁发射、TEMPEST只测试盒约束系统和设备的所有电磁发射。（B）

A、正确 B、错误

924、加密传输是一种非常有效并经常使用的方法，也能解决输入和输出端的电磁信息泄露问题。（B）

A、正确 B、错误

925、出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。（B）

A、正确 B、错误

926、红区：红新号的传输通道或单元电路称为红区，反之为黑区。（A）

A、正确 B、错误

927、机房应设置相应的活在报警和灭火系统。（A）

A、正确 B、错误

928、计算机机房的建设应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。（A）

A、正确 B、错误

929、计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。（B）

A、正确 B、错误

930、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。（A）

A、正确 B、错误

931、提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。（A）

A、正确 B、错误

932、在计算机机房附近施工，不负有维护计算机信息系统安全的责任和义务。（B）

A、正确 B、错误

933、只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。（B）

A、正确 B、错误

934、主管计算机信息系统安全的公安机关和城建及规划部门，应与设施单位进行协调，在不危害用户利益的大前提下，制定措施。合理施工，做好计算机信息系统安全保护工作。（B）

A、正确 B、错误

935、防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。（A）

A、正确 B、错误

936、对于公司机密信息必须根据公司的相关规定予以适当的标识。（A）

A、正确 B、错误

937、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。（A）

A、正确 B、错误

938、如果在电话、电视会议中涉及讨论工伤机密信息，会议主持人或组织人在会议全过程中一定要确认每一个与会者是经授权参与的。（A）

A、正确 B、错误

939、为防止信息非法泄露，需要销毁存储介质时，应该批准后自行销毁。（B）

A、正确 B、错误

940、将公司的机密信息通过互联网络传送时，必须予以加密。（A）

A、正确 B、错误

941、机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。（A）

A、正确 B、错误

942、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式进行保密。（A）

A、正确 B、错误

943、“一次一密”属于序列密码的一种。（A）

A、正确 B、错误

944、3DES算法的加密过程就是用一个秘钥对待加密的数据执行三次DES算法的加密操作。（B）

A、正确 B、错误

945、AES加密算法的秘钥长度为128、192或256位。（A）

A、正确 B、错误

946、AES是一种非对称算法。（B）

A、正确 B、错误

947、DES3和RSA是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。（A）

A、正确 B、错误

948、Diffie-Hellman算法的安全性取决于离散对数计算的困难性，可以实现秘钥交换。（A）

A、正确 B、错误

949、DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。（A）

A、正确 B、错误

950、MD5是一种加密算法。（B）

A、正确 B、错误

951、PGP协议缺省的压缩算法是ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。（A）

A、正确 B、错误

952、PKI是一个用对称密码算法和技术来实现并提供安全服务的具有通用性的安全基础设施。（B）

A、正确 B、错误

953、RC4是典型的的序列密码算法。（A）

A、正确 B、错误

954、RSA算法作为主要的非对称算法，使用公钥加密的秘闻一定要采用公钥来街。（B）

A、正确 B、错误

955、安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。（A）

A、正确 B、错误

956、常见的公钥密码算法有RSA算法、Diffie-Hellman算法和EIGamal算法。（A）

A、正确 B、错误

957、当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（A）

A、正确 B、错误

958、发送方使用AH协议处理数据包，需要对整个IP的数据包计算MAC，包括IP头的所有字段和数据。（B）

A、正确 B、错误

959、分组密码的优点是错误扩展小、速度快、安全程度高。（B）

A、正确 B、错误

960、公共迷药密码体制在秘钥管理上比对称秘钥密码体制更安全。（A）

A、正确 B、错误

961、古典加密主要采用的主要方法是置换，代换。（A）

A、正确 B、错误

962、古典加密主要是对加密算法的保密，现代加密算法是公开的，主要是针对秘钥进行保密。（A）

A、正确 B、错误

963、基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。（A）

A、正确 B、错误

964、口令应在120天至少更换一次。（B）

A、正确 B、错误

965、链路加密方式适用于在广域网系统中应用。（B）

A、正确 B、错误

966、密码保管不善属于操作失误的安全隐患。（B）

A、正确 B、错误

967、日常所见的校园饭卡是利用身份认证的单因素法。（A）

A、正确 B、错误

968、身份认证要求对数据和信息来源进行验证，以确保发信人的身份。（B）

A、正确 B、错误

969、身份认证与权限控制是网络社会的管理基础。（A）

A、正确 B、错误

970、数据在传输过程中用哈希算法保证其完整性后，非法用户无法无法对数据进行任何修改。（B）

A、正确 B、错误

971、数字签名比较的是摘要结果长度是否都是128位。（B）

A、正确 B、错误

972、通信数据与文件加密是同一个概念。（B）

A、正确 B、错误

973、为AES开发的Rijndae1算法的秘钥长度是128位，分组长度也为128位。（B）

A、正确 B、错误

974、为了保证安全性，密码算法应该进行保密。（B）

A、正确 B、错误

975、文件压缩变换是一个单向加密过程。（B）

A、正确 B、错误

976、我的公钥证书不能在网络上公开，否则其他人可能冒充我的身份或伪造我的数字签名。（B）

A、正确 B、错误

977、现代加密算法可以分为对称加密算法和非对称加密。（A）

A、正确 B、错误

978、虚拟专用网VPN的关键技术主要是隧道技术、加解密技术、秘钥管理技术以及使用者与设备身份认证技术。（A）

A、正确 B、错误

979、以当前的技术来说，RSA体制是无条件安全的。（B）

A、正确 B、错误

980、在4A系统的远期建设中，应用系统自身不需要保留系统从账户信息。（B）

A、正确 B、错误

981、在MD5算法中，要先将以初始化的A、B、C、D这四个变量分别复制到a、b、c、d中。（A）

A、正确 B、错误

982、在MD5算法中要用到4个变量，分别表示A、B、C、D，均为32位长。（A）

A、正确 B、错误

983、在PKI中，注册机构RA是必要的组件。（B）

A、正确 B、错误

984、在SSL握手协议过程中，需要服务器发送自己的证书。（A）

A、正确 B、错误

985、在非对称加密过程中，加密和解密使用的是不同的秘钥。（A）

A、正确 B、错误

986、在公钥加密系统中，用公钥加密的密文可以由私钥解密，但用公钥加密的密文，不能用公钥解密。 （B）

A、正确 B、错误

987、在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一种“破解”。 （A）

A、正确 B、错误

988、账户管理的Agent不适用于在网络设备中部署。 （A）

A、正确 B、错误

989、整个PKI系统有证书服务器AS、票据许可服务器TGS、客户机和应用服务器四部分组成。 （B）

A、正确 B、错误

990、最基本的认证方式选择证书是数字证书。（B）

A、正确 B、错误

991、最小特权、纵深防御是网络安全原则之一。（A）

A、正确 B、错误

992、数字证书是由权威机构CA发行的一种权威的电子文档，是网络环境中的一种身份证。（A）

A、正确 B、错误

993、数字证书是由权威机构PKI发行的一种权威性的电子文档，是网络环境中的一种身份证。 （B）

A、正确 B、错误

994、信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段。（A）

A、正确 B、错误

995、病毒能隐藏在电脑的CMOS存储器里。（B）

A、正确 B、错误

996、对感染病毒的软盘进行浏览会导致硬盘被感染。（B）

A、正确 B、错误

997、已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（B）

A、正确 B、错误

998、重新格式化硬盘可以清楚所有病毒。（B）

A、正确 B、错误

999、专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，并根据评估结果提供评估报告。 （A）

A、正确 B、错误

1000、冒充信件回复、假装纯文字ICON、冒充微软雅虎发信、下载电子贺卡同意书、是使用的叫做字典攻击法的方法。（B）

A、正确 B、错误

1. **单项选择题**
2. Chinese Wall 模型的设计宗旨是：（A）。

A、用户只能访问哪些与已经拥有的信息不冲突的信息   
B、用户可以访问所有信息

C、用户可以访问所有已经选择的信息   
D、用户不可以访问哪些没有选择的信息

1. 安全责任分配的基本原则是：（C）。

A、“三分靠技术，七分靠管理” B、“七分靠技术，三分靠管理”

C、“谁主管，谁负责” D、防火墙技术

1. 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（B）不属于信息运行安全技术的范畴。

A、风险分析 B、审计跟踪技术 C、应急技术 D、防火墙技术

1. 从风险的观点来看，一个具有任务紧急性，核心功能性的计算机应用程序系统的开发和维护项目应该（A）。

A、内部实现 B、外部采购实现 C、合作实现 D、多来源合作实现

1. 从风险分析的观点来看，计算机系统的最主要弱点是（B）。

A、内部计算机处理 B、系统输入输出 C、通讯和网络 D、外部计算机处理

1. 从风险管理的角度，以下哪种方法不可取？（D）

A、接受风险 B、分散风险 C、转移风险 D、拖延风险

1. 当今IT的发展与安全投入，安全意识和安全手段之间形成（B）。

A、安全风险屏障 B、安全风险缺口 C、管理方式的变革 D、管理方式的缺口

1. 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（D）。

A、已买的软件 B、定做的软件 C、硬件 D、数据

1. 当一个应用系统被攻击并受到了破坏后，系统管理员从新安装和配置了此应用系统，在该系统重新上线前管理员不需查看：（C）

A、访问控制列表 B、系统服务配置情况

1. 审计记录 D、用户账户和权限的设置

10、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行（B）。

1. 逻辑隔离 B、物理隔离 C、安装防火墙 D、VLAN 划分

11、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？（D）

A、威胁、脆弱性 B、系统价值、风险

C、信息安全、系统服务安全 D、受侵害的客体、对客体造成侵害的程度业务

12、公司应明确员工的雇佣条件和考察评价的方法与程序，减少因雇佣不当而产生的安全风险。人员考察的内容不包括（B）。

A、身份考验、来自组织和个人的品格鉴定 B、家庭背景情况调查

C、学历和履历的真实性和完整性 D、学术及专业资格

13、计算机信息的实体安全包括环境安全、设备安全、（B）三个方面。

A运行安全 B、媒体安全 C、信息安全 D、人事安全

14、目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（B）

A、公安部 B、国家保密局

C、信息产业部 D、国家密码管理委员会办公室

15、目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（B）

A、GB/T 18336-2001 信息技术安全性评估准则

B、GB 17859-1999 计算机信息系统安全保护等级划分准则

C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构

D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

16、确保信息没有非授权泄密，即确保信息不泄露给非授权的个人、实体或进程，不为其所用，是指（C）。

A、完整性 B、可用性 C、保密性 D、抗抵赖性

17、如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（A）

A、自动软件管理 B、书面化制度 C、书面化方案 D、书面化标准

18、如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？（A）

A、计算风险 B、选择合适的安全措施

C、实现安全措施 D、 接受残余风险

19、软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（A）

A、软件中止和黑客入侵 B、远程监控和远程维护

C、软件中止和远程监控 D、远程维护和黑客入侵

20、 管理审计指（C）

A、保证数据接收方收到的信息与发送方发送的信息完全一致

B、防止因数据被截获而造成的泄密

C、对用户和程序使用资源的情况进行记录和审查

D、保证信息使用者都可

21、为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（A）

A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B、进行离职谈话，禁止员工账号，更改密码

C、让员工签署跨边界协议

D、列出员工在解聘前需要注意的所有责任

22、为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（D）

A、人际关系技能 B、项目管理技能 C、技术技能 D、沟通技能

23、我国的国家秘密分为几级？（A）

A、3 B、4 C、5 D、6

24、系统管理员属于（C）。

A、决策层 B、管理层

C、执行层 D、既可以划为管理层，又可以划为执行层

25、下列哪一个说法是正确的？（C）

A、风险越大，越不需要保护 B、风险越小，越需要保护

C、风险越大，越需要保护 D、越是中等风险，越需要保护

26、下面哪类访问控制模型是基于安全标签实现的？（B）

A、自主访问控制 B、强制访问控制

C、基于规则的访问控制 D、基于身份的访问控制

27、下面哪项能够提供最佳安全认证功能？（B）

A、这个人拥有什么 B、这个人是什么并且知道什么

C、这个人是什么 D、这个人知道什么

28、下面哪一个是国家推荐性标准？（A）

A、GB/T 18020-1999 应用级防火墙安全技术要求

B、SJ/T 30003-93 电子计算机机房施工及验收规范

C、GA243-2000 计算机病毒防治产品评级准则

D、ISO/IEC 15408-1999 信息技术安全性评估准则

29、下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（C）

A、对安全违规的发现和验证是进行惩戒的重要前提

B、惩戒措施的一个重要意义在于它的威慑性

C、处于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训

D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

30、下面哪一项最好地描述了风险分析的目的？（C）

A、识别用于保护资产的责任义务和规章制度

B、识别资产以及保护资产所使用的技术控制措施

C、识别资产、脆落性并计算潜在的风险

D、识别同责任义务有直接关系的威胁

31、下面哪一项最好地描述了组织机构的安全策略？（A）

A、定义了访问控制需求的总体指导方针

B、建议了如何符合标准

C、表明管理意图的高层陈述

D、表明所使用的技术控制措施的高层陈述

32、下面哪一种风险对电子商务系统来说是特殊的？（D）

A、服务中断 B、应用程序系统欺骗

C、未授权的信息泄露 D、确认信息发送错误

33、下面有关我国标准化管理和组织机构的说法错误的是？（C）

A、国家标准化管理委员会是统一管理全国标准化工作的主管机构

B、国家标准化技术委员会承担国家标准的制定和修改工作

C、全国信息安全标准化技术委员负责信息安全技术标准的审查、批准、编号和发布

D、全国信息安全标准化技术委员负责统一协调信息安全国家标准年度技术项目

34、项目管理是信息安全工程师基本理论，以下哪项对项目管理的理解是正确的？（A）

A、项目管理的基本要素是质量，进度和成本

B、项目管理的基本要素是范围，人力和沟通

C、项目管理是从项目的执行开始到项目结束的全过程进行计划、组织

D、项目管理是项目的管理者，在有限的资源约束下，运用系统的观点，方法和理论，对项目涉及的技术工作进行有效地管理

35、信息安全的金三角是（C）。

A、可靠性，保密性和完整性 B、多样性，冗余性和模化性

C、保密性，完整性和可用性 D、多样性，保密性和完整性

36、信息安全风险缺口是指（A）。

A、IT的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

37、信息安全风险应该是以下哪些因素的函数？（A）

A、信息资产的价值、面临的威胁以及自身存在的脆弱性等

B、病毒、黑客、漏洞等

C、保密信息如国家密码、商业秘密等

D、网络、系统、应用的复杂的程度

38、信息安全工程师监理的职责包括？（A）

A、质量控制，进度控制，成本控制，合同管理，信息管理和协调

B、质量控制，进度控制，成本控制，合同管理和协调

C、确定安全要求，认可设计方案，监视安全态势，建立保障证据和协调

D、确定安全要求，认可设计方案，监视安全态势和协调

39、信息安全管理最关注的是？（C）

A、外部恶意攻击 B、病毒对PC的影响

C、内部恶意攻击 D、病毒对网络的影响

40、信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（C）

A、信息的价值 B、信息的时效性

C、信息的存储方式 D、法律法规的规定

41、信息网络安全的第三个时代是（A）

A、主机时代，专网时代，多网合一时代 B、主机时代，PC时代，网络时代

C、PC时代，网络时代，信息时代 D、2001年，2002年，2003年

42、一个公司在制定信息安全体系框架时，下面哪一项是首要考虑和制定的？（A）

A、安全策略 B、安全标准 C、操作规程 D、安全基线

43、以下哪个不属于信息安全的三要素之一？（C）

A、机密性 B、完整性 C、抗抵赖性 D、可用性

44、以下哪一项安全目标在当前计算机系统安全建设中是最重要的？（C）

A、目标应该具体 B、目标应该清晰

C、目标应该是可实现的 D、目标应该进行良好的定义

45、以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（A）

A、制度和措施 B、漏洞分析

C、意外事故处理计划 D、采购计划

46、以下哪一项是对信息系统经常不能满足用户需求的最好解释？（C）

A、没有适当的质量管理工具 B、经常变化的用户需求

C、用户参与需求挖掘不够 D、项目管理能力不强

47、以下哪一种人给公司带来了最大的安全风险？（D）

A、临时工 B、咨询人员 C、以前的员工 D、当前的员工

48、以下哪种安全模型未使用针对主客体的访问控制机制？（C）

A、基于角色模型 B、自主访问控制模型

C、信息流模型 D、强制访问控制模型

49、以下哪种措施既可以起到保护的作用还能起到恢复的作用？（C）

A、对参观者进行登记 B、备份

C、实施业务持续性计划 D、口令

50、以下哪种风险被定义为合理的风险？（B）

A、最小的风险 B、可接受风险

C、残余风险 D、总风险

51、以下人员中，谁负有决定信息分类级别的责任？（B）

A、用户 B、数据所有者 C、审计员 D、安全官

52、有三种基本的鉴别的方式：你知道什么，你有什么,以及（C）。

A、你需要什么 B、你看到什么 C、你是什么 D、你做什么

53、在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（B）

A、自下而上 B、自上而下 C、上下同时开展 D、以上都不正确

54、在风险分析中，下列不属于软件资产的是（D）

A、计算机操作系统 B、网络操作系统

C、应用软件源代码 D、外来恶意代码

55、在国家标准中，属于强制性标准的是：（B）

A、GB/T XXXX-X-200X B、GB XXXX-200X

C、DBXX/T XXX-200X D、QXXX-XXX-200X

56、在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（A）

A、当信息安全事件的负面影响扩展到本组织意外时

B、只要发生了安全事件就应当公告

C、只有公众的什么财产安全受到巨大危害时才公告

D、当信息安全事件平息之后

57、在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？（A）

A、标准（Standard） B、安全策略（Security policy）

C、方针（Guideline） D、流程(Proecdure)

58、在信息安全管理工作中“符合性”的含义不包括哪一项？（C）

A、对法律法规的符合 B、对安全策略和标准的符合

C、对用户预期服务效果的符合 D、通过审计措施来验证符合情况

59、在许多组织机构中，产生总体安全性问题的主要原因是（A）。

A、缺少安全性管理 B、缺少故障管理

C、缺少风险分析 D、缺少技术控制机制

60、职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（D）

A、数据安全管理员 B、数据安全分析员

C、系统审核员 D、系统程序员

61、中国电信的岗位描述中都应明确包含安全职责，并形成正式文件记录在案，对于安全职责的描述应包括（D）。

A、落实安全政策的常规职责 B、执行具体安全程序或活动的特定职责

C、保护具体资产的特定职责 D、以上都对

62、终端安全管理目标：规范支撑系统中终端用户的行为，降低来自支撑系统终端的安全威胁，重点解决以下哪些问题？（A）。

A、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

B、终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

C、终端接入和配置管理；桌面及主机设置管理；终端防病毒管理

D、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理

63、著名的橘皮书指的是（A）。

A、可信计算机系统评估标准(TCSEC) B、信息安全技术评估标准（ITSEC）

C、美国联邦标准（FC） D、通用准则（CC）

64、资产的敏感性通常怎样进行划分？（C）

A、绝密、机密、敏感 B、机密、秘密、敏感和公开

C、绝密、机密、秘密、敏感和公开等五类

D、绝密、高度机密、秘密、敏感和公开等五类

65、重要系统关键操作操作日志保存时间至少保存（C）个月。

A、1 B、2 C、3 D、4

66、安全基线达标管理办法规定：BSS系统口令设置应遵循的内控要求是（C）

A、数字+字母 B、数字+字母+符号

C、数字+字母+字母大小写 D、数字+符号

67、不属于安全策略所涉及的方面是（D）。

A、物理安全策略 B、访问控制策略

C、信息加密策略 D、防火墙策略

68、“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（C）。

A、“普密”、“商密”两个级别 B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别

D、“一密”、“二密”，“三密”、“四密”四个级别

69、对MBOSS系统所有资产每年至少进行（A）次安全漏洞自评估。

A、1 B、2 C、3 D、4

70、下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（A）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

71、中国电信各省级公司争取在1-3年内实现CTG-MBOSS 系统安全基线“达标”（C）级以上。

A、A级 B、B级 C、C级 D、D级

72、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

73、获取支付结算、证劵交易、期货交易等网络金融服务的身份认证信息（B）组以上的可以被《中华人民共和国刑法》认为是非法获取计算机信息系统系统认定的“情节严重”。

A、5 B、10 C、-15 D、20

74、基准达标项满（B）分作为安全基线达标合格的必要条件。

A、50 B、60 C、70 D、80

75、《国家保密法》对违法人员的量刑标准是（A）。

A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑

B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑

C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑

D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

76、$HOME/.netrc文件包含下列哪种命令的自动登录信息？（C）

A、rsh B、ssh C、ftp D、rlogin

77、/etc/ftpuser文件中出现的账户的意义表示（A）。

A、该账户不可登录ftp B、该账户可以登录ftp C、没有关系 D、缺少

78、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

79、Linux系统/etc目录从功能上看相当于Windows的哪个目录？（B）

A、program files B、Windows C、system volume information D、TEMP

80、Linux系统格式化分区用哪个命令？（A）

A、fdisk B、mv C、mount D、df

81、在Unix系统中，当用ls命令列出文件属性时，如果显示-rwxrwxrwx,意思是（A）。

A、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示其他用户的访问权限

B、前三位rwx表示文件同组用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

C、前三位rwx表示文件同域用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

D、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示同域用户的访问权限

82、Linux系统通过（C）命令给其他用户发消息。

A、less B、mesg C、write D、echo to

83、Linux中，向系统中某个特定用户发送信息，用什么命令？（B）

A、wall B、write C、mesg D、net send

84、防止系统对ping请求做出回应，正确的命令是：（C）。

A、echo 0>/proc/sys/net/ipv4/icmp\_ehco\_ignore\_all

B、echo 0>/proc/sys/net/ipv4/tcp\_syncookies

C、echo 1>/proc/sys/net/ipv4/icmp\_echo\_ignore\_all

D、echo 1>/proc/sys/net/ipv4/tcp\_syncookies

85、NT/2K模型符合哪个安全级别？（B）

A、B2 B、C2 C、B1 D、C1

86、Red Flag Linux指定域名服务器位置的文件是（C）。

A、etc/hosts B、etc/networks C、etc/rosolv.conf D、/.profile

87、Solaris操作系统下，下面哪个命令可以修改/n2kuser/.profile文件的属性为所有用户可读、科协、可执行？（D）

A、chmod 744 /n2kuser/.profile B、 chmod 755 /n2kuser/.profile

C、 chmod 766 /n2kuser/.profile D、 chmod 777 /n2kuser/.profile

88、如何配置，使得用户从服务器A访问服务器B而无需输入密码？（D）

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhost文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/etc/hosts.equiv文件

89、Solaris系统使用什么命令查看已有补丁列表？（C）

A、uname –an B、showrev C、oslevel –r D、swlist –l product ‘PH??’

90、Unix系统中存放每个用户信息的文件是（D）。

A、/sys/passwd B、/sys/password C、/etc/password D、/etc/passwd

91、Unix系统中的账号文件是（A）。

A、/etc/passwd B、/etc/shadow C、/etc/group D、/etc/gshadow

92、Unix系统中如何禁止按Control-Alt-Delete关闭计算机？（B）

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

93、Unix中。可以使用下面哪一个代替Telnet，因为它能完成同样的事情并且更安全？（）

A、S-TELNET B、SSH C、FTP D、RLGON

94、Unix中，默认的共享文件系统在哪个位置？（C）

A、/sbin/ B、/usr/local/ C、/export/ D、/usr/

95、Unix中，哪个目录下运行系统工具，例如sh,cp等？（A）

A、/bin/ B、/lib/ C、/etc/ D、/

96、U盘病毒依赖于哪个文件打到自我运行的目的？（A）

A、autoron.inf B、autoexec.bat C、config.sys D、system.ini

97、Windows nt/2k中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

98、Windows 2000目录服务的基本管理单位是（D）。

A、用户 B、计算机 C、用户组 D、域

99、Windows 2000系统中哪个文件可以查看端口与服务的对应？（D）

A、c:\winnt\system\drivers\etc\services B、c:\winnt\system32\services

C、c:\winnt\system32\config\services D、c:\winnt\system32\drivers\etc\services

100、Windows NT/2000 SAM存放在（D）。

A、WINNT B、WINNT/SYSTEM32

C、WINNT/SYSTEM D、WINNT/SYSTEM32/config

101、 Windows NT/2000中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

102、Windows NT的安全标识（SID）串是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是什么？（C）

A、击键速度 B、用户网络地址 C、处理当前用户模式线程所花费CPU的时间 D、PING的响应时间

103、Windows NT和Windows 2000系统能设置为在几次无效登录后锁定账号，可以防止：（B）。

A、木马 B、暴力破解 C、IP欺骗 D、缓冲区溢出攻击

104、Windows主机推荐使用（A）格式。

A、NTFS B、FAT32 C、FAT D、Linux

105、XP当前的最新补丁是（C）。

A、SP1 B、SP2 C、SP3 D、SP4

106、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

107、当你感觉到你的Win2003运行速度明显减慢，当打开任务管理器后发现CPU使用率达到了100%，你认为你最有可能受到了（D）攻击。

A、缓冲区溢出攻击 B、木马攻击 C、暗门攻击 D、DOS攻击

108、档案权限755，对档案拥有者而言，是什么含义？（A）

A、可读，可执行，可写入 B、可读

C、可读，可执行 D、可写入

109、如何配置，使得用户从服务器A访问服务器B而无需输入密码（D）。

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhosts文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/et/hosts.equiv文件

110、要求关机后不重新启动，shutdown后面参数应该跟（C）。

A、–k B、–r C、-h D、 –c

111、一般来说，通过web运行http服务的子进程时，我们会选择（D）的用户用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

112、以下哪项技术不属于预防病毒技术的范畴？（A）

A、加密可执行程序 B、引导区保护

C、系统监控与读写控制 D、校验文件

113、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？（B）

A、缓冲区溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDos攻击

114、与另一台机器建立IPC$会话连接的命令是（D）。

A、net user [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

B、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$) user:Administrator / passwd:aaa

C、net user \192.168.0.1IPC$ D、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

115、在NT中，如果config.pol已经禁止了对注册表的访问，那么黑客能够绕过这个限制吗？怎样实现？（B）

A、不可以 B、可以通过时间服务来启动注册表编辑器

C、可以通过在本地计算机删除config.pol文件 D、可以通过poledit命令

116、在NT中，怎样使用注册表编辑器来严格限制对注册表的访问？（C）

A、HKEY\_CURRENT\_CONFIG,连接网络注册、登录密码、插入用户ID

B、HKEY\_CURRENT\_MACHINE,浏览用户的轮廓目录，选择NTUser.dat

C、HKEY\_USERS,浏览用户的轮廓目录，选择NTUser.dat

D、HKEY\_USERS,连接网络注册，登录密码，插入用户ID

117、在Solaris 8下，对于/etc/shadow文件中的一行内容如下“root:3vd4NTwk5UnLC:9038::::::”,以下说法正确的是：（E）。

A、这里的3vd4NTwk5UnLC是可逆的加密后的密码

B、这里的9038是指从1970年1月1日到现在的天数

C、这里的9038是指从1980年1月1日到现在的天数

D、这里的9038是指从1980年1月1日到最后一次修改密码的天数

E-以上都不正确

118、在Solaris 8下，对于/etc/shadow文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（A）。

A、是/etc/passwd文件格式 B、是/etc/shadow文件格式

C、既不是/etc/passwd也不是/etc/shadow文件格式

D、这个root用户没有SHELL，不可登录

E、这个用户不可登录，并不是因为没有SHELL

119、在Solaris系统中，终端会话的失败登录尝试记录在下列哪个文件里面?(D)

A、-/etc/default/login B、/etc/nologin

C、/etc/shadow D、var/adm/loginlog

120、在Windows 2000中，以下哪个进程不是基本的系统进程:(D)

A、smss. exe B、csrss. Exe C、winlogon. exe D、-conime.exe

121、在Windows 2000中可以察看开放端口情况的是:(D)。

A、nbtstat B、net C、net show D、netstat

122、在Windows 2003下netstat的哪个参数可以看到打开该端口的PID?(C)（格式到此）

A、a B、n C、o D 、p

123、在使用影子口令文件(shadowedpasswords)的Linux系统中，/etc/passwd文件和/etc/shadow文件的正确权限分别是(C)。

A、rw-r-----,-r-------- B、rw-r--r--,-r--r--r—

C、rw-r--r--,-r-------- Drw-r--rw-,-r-----r--

124、制定数据备份方案时，需要重要考虑的两个因素为适合的备份时间和(B)。

A、备份介质 B、备份的存储位置

C、备份数据量 D、恢复备份的最大允许时间

125、周期性行为，如扫描，会产生哪种处理器负荷?(A)

A、Idle Ioad B、Usage Ioad C、Traffic load D、以上都不对

126、主要由于(D)原因，使Unix易于移植

A、Unix是由机器指令书写的 B、Unix大部分由汇编少部分用C语言编写

C、Unix是用汇编语言编写的 D、Unix小部分由汇编大部分用C语言编写

127、HP-UX系统中，使用(A)命令查看系统版本、硬件配置等信息。

A、uname -a B、ifconfig C、netstat D、ps -ef

128、Linux文件权限一共10位长度，分成四段，第三段表示的内容是(C)。

A、文件类型 B、文件所有者的权限

C、文件所有者所在组的权限 D、其他用户的权限

129、在云计算虚拟化应用中，VXLAN技术处于OS工网络模型中2-3层间，它综合了2层交换的简单性与3层路由的跨域连接性。它是通过在UDP/IP上封装Mac地址而实现这一点的。在简单应用场合，vxLAN可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?(C)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

130、Linux中，什么命令可以控制口令的存活时间了(A)。

A、chage B、passwd C、chmod D、umask

131、Qfabric技术是使用市场上现成的计算和存储网元并利用行业标准的网络接口将它们连接后组建大规模的数据中心，以满足未来云计算的要求。该技术概念是哪个厂家主推的概念?(B)

A、惠普 B、uniper C、Cisco与Vmware D、博科Brocade

132、为了检测Windows系统是否有木马入侵，可以先通过()命令来查看当前的活动连接端口。

A、ipconfig B、netstat -rn C、tracert –d D、netstat -an

133、网络营业厅提供相关服务的可用性应不低于（A）。

A、99.99% B、99.9% C、99% D、98.9%

134、IRF(Intelligent Resilient Framework)是在该厂家所有数据中心交换机中实现的私有技术，是应用在网络设备控制平面的多虚拟技术。该技术属于哪个厂家?(A)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

135、Windows NT的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:(D)。

A、击键速度 B、当前用户名

C、用户网络地址 D、处理当前用户模式线程所花费CPU的时间

136、脆弱性扫描，可由系统管理员自行进行检查，原则上应不少于(B)。

A、每周一次 B、每月一次 C、每季度一次 D、每半年一次

137、下面哪一个情景属于身份验证(Authentication)过程?(A)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

138、下面哪一个情景属于授权(Authorization)过程?(B)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

139、下列哪一条与操作系统安全配置的原则不符合?(D)

A、关闭没必要的服务 B、不安装多余的组件

C、安装最新的补丁程序 D、开放更多的服务

140、关于DDoS技术，下列哪一项描述是错误的(D)。

A、一些DDoS攻击是利用系统的漏洞进行攻击的

B、黑客攻击前对目标网络进行扫描是发功DDoS攻击的一项主要攻击信息来源

C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的DDoS攻击入侵

D、DDoS攻击不对系统或网络造成任何影响

141、关于PPP协议下列说法正确的是:(C)。

A、PPP协议是物理层协议

B、PPP协议是在HDLC协议的基础上发展起来的

C、PPP协议支持的物理层可以是同步电路或异步电路

D、PPP主要由两类协议组成:链路控制协议族CLCP)和网络安全方面的验证协议族(PAP和CHAP)

142、接口被绑定在2层的zone，这个接口的接口模式是（C）。

A、NAT mode B、Route mode

C、-Transparent mode D、NAT或Route mode

143、接入控制方面，路由器对于接口的要求包括：（D）。

A、串口接入 B、局域网方式接入 C、Internet方式接入 D、VPN接入

144、局域网络标准对应OSI模型的哪几层？（C）。

A、上三层 B、只对应网络层 C、下三层 D、只对应物理层

145、拒绝服务不包括以下哪一项？（D）。

A、DDoS B、畸形报文攻击 C、Land攻击 D、ARP攻击

146、抗DDoS防护设备提供的基本安全防护功能不包括（A）。

A、对主机系统漏洞的补丁升级 B、检测DDoS攻击

C、DDoS攻击警告 D、DDoS攻击防护

147、路由器产品提供完备的安全架构以及相应的安全模块，在软、硬件层面设置重重过滤，保护路由器业务安全。其中不对的说法是：（C）。--》缺少D选项

A、路由器产品支持URPF，可以过滤大多数虚假IP泛洪攻击

B、路由器产品支持CAR功能，可以有效限制泛洪攻击

C、路由器产品不支持ACL配置功能，不能定制过滤规则

D、

148、路由器对于接入权限控制，包括：（D）。

A、根据用户账号划分使用权限 B、根据用户接口划分使用权限

C、禁止使用匿名账号 D、以上都是

149、路由器启动时默认开启了一些服务，有些服务在当前局点里并没有作用，对于这些服务：（C）。缺少D选项

A、就让他开着，也耗费不了多少资源 B、就让他开着，不会有业务去访问

C、必须关闭，防止可能的安全隐患 D、

150、设置Cisco设备的管理员账号时，应（C）。

A、多人共用一个账号 B、多人共用多个账号

C、一人对应单独账号 D、一人对应多个账号

151、什么命令关闭路由器的finger服务？（C）

A、disable finger B、no finger C、no finger service D、no service finger

152、什么是IDS？（A）

A、入侵检测系统 B、入侵防御系统 C、网络审计系统 D、主机扫描系统

153、实现资源内的细粒度授权，边界权限定义为：（B）。

A、账户 B、角色 C、权限 D、操作

154、使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）

A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

155、使用TCP 79端口的服务是：（D）。

A、telnet B、SSH C、Web D、Finger

156、使用一对一或者多对多方式的NAT转换，当所有外部IP地址均被使用后，后续的内网用户如需上网，NAT转换设备会执行什么样的动作？（C）

A、挤掉前一个用户，强制进行NAT转换 B、直接进行路由转发

C、不做NAT转换 D、将报文转移到其他NAT转换设备进行地址转换

157、私网地址用于配置本地网络、下列地址中属于私网地址的是？（C）

A、100.0.0.0 B、172.15.0.0 C、192.168.0.0 D、244.0.0.0

158、随着Internet发展的势头和防火墙的更新，防火墙的哪些功能将被取代。（D）

A、使用IP加密技术 B、日志分析工作

C、攻击检测和报警 D、对访问行为实施静态、固定的控制

159、随着安全要求的提高、技术的演进，（D）应逐步实现物理隔离，或者通过采用相当于物理隔离的技术（如MPLSVPN）实现隔离。

A、局域网 B、广域网及局域网 C、终端 D、广域网

160、通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出现崩溃，请问这种攻击属于何种攻击？（D）

A、拒绝服务（DoS）攻击 B、扫描窥探攻击

C、系统漏洞攻击 D、畸形报文攻击

161、通信领域一般要求3面隔离，即转发面、控制面、用户面实现物理隔离，或者是逻辑隔离，主要目的是在某一面受到攻击的时候，不能影响其他面。路由器的安全架构在实现上就支持：（D）

A、转发面和控制面物理隔离 B、控制面和用户面逻辑隔离

C、转发面和用户面逻辑隔离 D、以上都支持

162、网管人员常用的各种网络工具包括telnet、ftp、ssh等，分别使用的TCP端口号是（B）。

A、21、22、23 B、23、21、22 C、23、22、21 D、21、23、22

163、网络安全工作的目标包括：（D）。

A、信息机密性 B、信息完整性 C、服务可用性 D、以上都是

164、网络安全在多网合一时代的脆弱性体现在（C）。

A、网络的脆弱性 B、软件的脆弱性 C、管理的脆弱性 D、应用的脆弱性

165、应限制Juniper路由器的SSH（A），以防护通过SSH端口的DoS攻击。

A、并发连接数和1分钟内的尝试连接数 B、并发连接数

C、1分钟内的尝试连接数 D、并发连接数和3分钟内的尝试连接数

166、应用网关防火墙的逻辑位置处在OSI中的哪一层？（C）

A、传输层 B、链路层 C、应用层 D、物理层

167、应用网关防火墙在物理形式上表现为？（B）

A、网关 B、堡垒主机 C、路由 D、交换机

168、用来追踪DDoS流量的命令式：（C）

A、ip source-route B、ip cef C、ip source-track D、ip finger

169、用于保护整个网络IPS系统通常不会部署在什么位置？（D）

A、网络边界 B、网络核心 C、边界防火墙内 D、业务终端上

170、用于实现交换机端口镜像的交换机功能是：（D）

A、PERMIT LIST B、PVLAN C、VTP D、SPAN

171、有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（D）。

A、L2TP是由PPTV协议和Cisco公司的L2F组合而成

B、L2TP可用于基于Internet的远程拨号访问

C、为PPP协议的客户建立拨号连接的VPN连接

D、L2TP只能通过TCP/IP连接

172、有关PPTP（Point-to-Point Tunnel Protocol）说法正确的是（C）。

A、PPTP是Netscape提出的 B、微软从NT3.5以后对PPTP开始支持

C、PPTP可用在微软的路由和远程访问服务上 D、它是传输层上的协议

173、有一些应用，如微软Out look或MSN。它们的外观会在转化为基于Web界面的过程中丢失，此时要用到以下哪项技术：（B）

A、Web代理 B、端口转发 C、文件共享 D、网络扩展

174、预防信息篡改的主要方法不包括以下哪一项？（A）

A、使用VPN技术 B、明文加密 C、数据摘要 D、数字签名

175、域名服务系统（DNS）的功能是（A）。

A、完成域名和IP地址之间的转换 B、完成域名和网卡地址之间的转换

C、完成主机名和IP地址之间的转换 D、完成域名和电子邮件地址之间的转换

176、源IP为100.1.1.1，目的IP为100.1.1.255，这个报文属于什么攻击？（B）（假设该网段掩码为255.255.255.0）

A、LAND攻击 B、SMURF攻击 C、FRAGGLE攻击 D、WINNUKE攻击

177、在AH安全协议隧道模式中，新IP头内哪个字段无需进行数据完整性校验？（A）

A、TTL B、源IP地址 C、目的IP地址 D、源IP地址+目的IP地址

178、在C/S环境中，以下哪个是建立一个完整TCP连接的正确顺序？（D）

A、SYN，SYN/ACK，ACK B、Passive Open,Active Open,ACK,ACK

C、SYN,ACK/SYN,ACK D、Active Open/Passive Open,ACK,ACK

179、在L2TP应用场景中，用户的私有地址分配是由以下哪个组建完成？（B）

A、LAC B、LNS C、VPN Client D、用户自行配置

180、在OSI模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（A）

A、应用层 B、物理层 C、会话层 D、网络层

181、在OSI参考模型中有7个层次，提供了相应的安全服务来加强信息系统的安全性。以下哪一层提供了抗抵赖性？（B）

A、表示层 B、应用层 C、传输层 D、数据链路层

182、在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（B）

A、产生日志的数量 B、攻击减少的速度

C、较低的价格 D、假阳性的减少量

183、在安全审计的风险评估阶段，通常是按什么顺序来进行的？（A）

A、侦查阶段、渗透阶段、控制阶段 B、渗透阶段、侦查阶段、控制阶段

C、控制阶段、侦查阶段、渗透阶段 D、侦查阶段、控制阶段、渗透阶段

184、在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（D）

A、IETF 因特网工程工作小组 B、ISO 国际标准组织

C、IANA 因特网地址指派机构 D、OSI 开放系统互联

185、在传输模式IPSec应用情况中，以下哪个区域数据报文可受到加密安全保护？（D）

A、整个数据报文 B、原IP头 C、新IP头 D、传输层及上层数据报文

186、在点到点链路中，OSPF的Hello包发往以下哪个地址？（B）

A、127.0.0.1 B、224.0.0.5 C、233.0.0.1 D、255.255.255.255

187、在建立堡垒主机时，（A）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

188、在进行Sniffer监听时，系统将本地网络接口卡设置成何种侦听模式？（D）

A、unicast单播模式 B、Broadcast广播模式

C、Multicast组播模式 D、Promiscuous混杂模式

189、在零传输（Zone transfers）中DNS服务使用哪个端口？（A）

A、TCP 53 B、UDP 53 C、UDP 23 D、TCP23

190、在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（C）

A、入网访问控制 B、权限控制 C、网络检测控制 D、防火墙控制

191、在思科设备上，若要查看所有访问表的内容，可以使用的命令式（B）

A、show all access-lists B、show access-lists

C、show ip interface D、show interface

192、在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的这是对（A）。

A、可用性的攻击 B、保密性的攻击 C、完整性的攻击 D、真实性的攻击

193、在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（C）

A、报文服务拒绝 B、假冒 C、数据流分析 D、报文服务更改

194、在以下OSI七层模型中，synflooding攻击发生在哪层？（C）

A、数据链路层 B、网络层 C、传输层 D、应用层

195、在以下哪类场景中，移动用户不需要安装额外功能（L2TP）的VPDN软件？（B）

A、基于用户发起的L2TP VPN B、基于NAS发起的L2TP VPN

C、基于LNS发起的L2TP VPN D、以上都是

196、账户口令管理中4A的认证管理的英文单词为：（B）

A、Account B、Authentication C、Authorization D、Audit

197、只具有（A）和FIN标志集的数据包是公认的恶意行为迹象。

A、SYN B、date C、head D、标志位

198、主从账户在4A系统的对应关系包含：（D）

A、1 -N B、1 -1 C、N -1 D、以上全是

199、主动方式FTP服务器要使用的端口包括（A）。

A、TCP 21 TCP 20 B、TCP21 TCP大于1024的端口

C、TCP 20、TCP 大于1024端口 D、都不对

200、下列（D）因素不是影响IP电话语音质量的技术因素。

A、时延 B、抖动 C、回波 D、GK性能

201、下列安全协议中使用包括过滤技术，适合用于可信的LAN到LAN之间的VPN（内部VPN）的是（D）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

202、下列不是抵御DDoS攻击的方法有（D）。

A、加强骨干网设备监控 B、关闭不必要的服务

C、限制同时打开的Syn半连接数目 D、延长Syn半连接的time out时间

203、下列措施不能增强DNS安全的是（C）。

A、使用最新的BIND工具 B、双反向查找

C、更改DNS的端口号 D、不要让HINFO记录被外界看到

204、下列各种安全协议中使用包过滤技术，适合用于可信的LAN到LAN之间的VPN，即内部网VPN的是（）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

205、下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适？（D）

A、回应的比例 B、被动的防御 C、主动的防御 D、都不对

206、下列哪项是私有IP地址？（A）

A、10.5.42.5 B、172.76.42.5 C、172.90.42.5 D、241.16.42.5

207、下列哪一项能够提高网络的可用性？（B）

A、数据冗余 B、链路冗余 C、软件冗余 D、电源冗余

208、下列哪一种攻击方式不属于拒绝服务攻击：（A）。

A、LOphtCrack B、Synflood C、Smurf D、Ping of Death

209、下列哪一项是arp协议的基本功能？（A）

A、通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行

B、对局域网内的其他机器广播路由地址

C、过滤信息，将信息传递个数据链路层 D、将信息传递给网络层

210、最早的计算机网络与传统的通信网络最大的区别是什么？（A）

A、计算机网络采用了分组交换技术 B、计算机网络采用了电路交换技术

C、计算机网络的可靠性大大提高 D、计算机网络带宽和速度大大提高

211、以下哪个属于IPS的功能？（A）

A、检测网络攻击 B、网络流量检测 C、实时异常告警 D、以上都是

212、以下说法错误的是（C）。

A、安全是一个可用性与安全性之间的平衡过程 B、安全的三要素中包含完整性

C、可以做到绝对的安全 D、网络安全是信息安全的子集

213、以下属于4A策略管理模块可以管理的为（C）。

A、访问控制策略 B、信息加密策略 C、密码策略 D、防火墙策略

214、最早研究计算机网络的目的是什么？（B）

A、共享硬盘空间、打印机等设备 B、共享计算资源

C、直接的个人通信 D、大量的数据交换

215、防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为（C）。

A、内容过滤 B、地址转换 C、透明代理 D、内容中转

216、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）。

A、防火墙 B、CA中心 C、加密机 D、防病毒产品

217、网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（D）。

A、多重安全网关 B、防火墙 C、Vlan隔离 D、物理隔离

218、下列哪项不是Tacacs+协议的特性。（A）

A、扩展记账 B、加密整个数据包 C、使用TCP D、支持多协议

219、一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（A）

A、最小特权 B、阻塞点 C、失效保护状态 D、防御多样化

220、包过滤防火墙工作的好坏关键在于？（C）

A、防火墙的质量 B、防火墙的功能 C、防火墙的过滤规则设计 D、防火墙的日志

221、对于日常维护工作，连接路由器的协议通常使用：（B）。缺少D选项

A、TELNET，简单，容易配置 B、SSH &SSHv2 加密算法强劲，安全性好

C、TELNET配置16位长的密码，加密传输，十分安全 D、

222、BOTNET是（C）。

A、普通病毒 B、木马程序 C、僵尸网络 D、蠕虫病毒

223、监听的可能性比较低的是（B）数据链路。

A、Ethernet B、电话线 C、有线电视频道 D、无线电

224、当IPS遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（B）。

A、pass B、bypass C、watchdog D、HA

225、网络环境下的security是指（A）。

A、防黑客入侵，防病毒，窃取和敌对势力攻击

B、网络具有可靠性，可防病毒，窃密和敌对势力攻击

C、网络具有可靠性，容灾性，鲁棒性

D、网络的具有防止敌对势力攻击的能力

226、某一案例中，使用者已将无线AP的SSID广播设置为禁止，并修改了默认SSID值，但仍有未经授权的客户端接入该无线网络，这是因为（D）

A、禁止SSID广播仅在点对点的无线网络中有效

B、未经授权客户端使用了默认SSID接入

C、无线AP开启了DHCP服务

D、封装了SSID的数据包仍然会在无线AP与客户端之间传递

227、为了保护DNS的区域传送（zone transfer），应该配置防火墙以阻止（B）。

1.UDP

2.TCP

3.53

4.52

A、1,3 B、2,3 C、1,4 D、2,4

228、以下不属于代理服务技术优点的是（D）。

A、可以实现身份认证 B、内部地址的屏蔽盒转换功能

C、可以实现访问控制 D、可以防范数据驱动侵袭

229、应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（C）。

A、60% B、70% C、80% D、90%

230、TCP协议与UDP协议相比，TCP是（B），UDP是（）。

A、设置起来麻烦；很好设置 B、容易；困难

C、面向连接的；非连接的 D、不可靠的；可靠的

231、交换机转发以太网的数据基于：（B）。

A、交换机端口号 B、MAC地址 C、IP地址 D、数据类别

232、HTTP，FTP，SMTP建立在OSI模型的哪一层？（D）

A、2层-数据链路层 B、3层-网络层 C、4层-传输层 D、7层-应用层

233、网络安全的基本属性是（D）。

A、机密性 B、可用性 C、完整性 D、以上都是

234、网络安全的主要目的是保护一个组织的信息资产的（A）。

A、机密性、完整性、可用性 B、参照性、可用性、机密性、

C、可用性、完整性、参照性 D、完整性、机密性、参照性

235、DBS是采用了数据库技术的计算机系统。DBS是一个集合体，包含数据库、计算机硬件、软件和（C）。

A、系统分析员 B、程序员 C、数据库管理员 D、操作员

236、MySQL -h host -u user -p password命令的含义如下，哪些事正确的？（D）

A、-h后为host为对方主机名或IP地址 B、-u后为数据库用户名

C、-p后为密码 D、以上都对

237、Oracle当连接远程数据库或其它服务时，可以指定网络服务名，Oracle9i支持5中命名方法，请选择错误的选项。（D）

A、本地命名和目录命名 B、Oracle名称（Oracle Names）

C、主机命名和外部命名 D、DNS和内部命名

238、Oracle的数据库监听器（LISTENER）的默认通讯端口是？（A）

A、TCP 1521 B、TCP 1025 C、TCP 1251 D、TCP 1433

239、Oracle默认的用户名密码为（A）。

A、Scote/tiger B、root C、null D、rootroot

240、Oracle数据库中，物理磁盘资源包括哪些（D）。

A、控制文件 B、重做日志文件 C、数据文件 D、以上都是

241、Oracle中启用审计后，查看审计信息的语句是下面哪一个？（C）

A、select \* from SYS.AUDIT$ B、select \* from syslogins

C、select \* from SYS.AUD$ D、AUDIT SESSION

242、SMTP的端口？（A）

A、25 B、23 C、22 D、21

243、SQL Server的登录账户信息保存在哪个数据库中？（C）

A、model B、msdb C、master D、tempdb

244、SQL Sever的默认DBA账号是什么？（B）

A、administrator B、sa C、root D、SYSTEM

245、SQL Sever的默认通讯端口有哪些？（B）

A、TCP 1025 B、TCP 1433 C、UDP 1434 D、TCP 14333 E、TCP 445

246、SQL Sever中可以使用哪个存储过程调用操作系统命令，添加系统账号？（B）

A、xp\_dirtree B、xp\_cmdshell C、xp\_cmdshell D、xpdeletekey

247、SQL Sever中下面哪个存储过程可以执行系统命令？（C）

A、xp\_regread B、xp\_command C、xp\_cmdshell D、sp\_password

248、SQL的全局约束是指基于元祖的检查子句和（C）。

A、非空值约束 B、域约束子句 C、断言 D、外键子句

249、SQL数据库使用以下哪种组件来保存真实的数据？（C）

A、Schemas B、Subschemas C、Tables D、Views

250、SQL语句中，彻底删除一个表的命令是（B）。

A、delete B、drop C、clear D、remore

251、SQL语言可以（B）在宿主语言中使用，也可以独立地交互式使用。

A、-极速 B、-嵌入 C、-混合 D、-并行

252、SSL安全套接字协议所用的端口是（B）。

A、80 B、443 C、1433 D、3389

253、不属于数据库加密方式的是（D）。

A、库外加密 B、库内加密 C、硬件/软件加密 D、专用加密中间件

254、测试数据库一个月程序主要应对的风险是（B）。

A、非授权用户执行“ROLLBACK”命令 B、非授权用户执行“COMMIT”命令

C、非授权用户执行“ROLLRORWARD”命令 D、非授权用户修改数据库中的行

**255、查看Oracle 8i及更高版本数据库的版本信息的命令是（C）。----缺少CD选项**

**A、cd $Oracle\_HOME/orainst B、C-cd $Oracle\_HIME/orainst C、 D、**

256、从安全的角度来看，运行哪一项起到第一道防线的作用？（C）

A、远端服务器 B、WEB服务器 C、防火墙 D、使用安全shell程序

257、从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（B）。

A、每个分割区G有g=|G|记录，其中g=0或g>=n，且g为偶数，

B、记录必须成对地加入G或从G中删除

C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从m各分割区G1，G2，… …Gm中每一个分割区而来的，则统计信息g（G1VG2V… …VGm）是允许发布

D、记录必须不对地加入G或从G中删除

258、单个用户使用的数据库视图的描述为（A）。

A、外模式 B、概念模式 C、内模式 D、存储模式

259、对于IIS日志记录，推荐使用什么文件格式？（D）

A、Microsoft IIS日志文件格式 B、NCSA公用日志文件格式

C、ODBC日志记录格式 D、W3C扩展日志文件格式

**260、对于IIS日志文件的存放目录，下列哪项设置是最好的？（D）----缺少D选型**

**A、%WinDir%\System32\LogFiles B、C:\Inetpub\wwwroot\LogFiles**

**C、C:\LogFiles..)-F:\LogFiles D、**

261、对于IIS日志文件的访问权限，下列哪些设置是正确的？（D）

A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）

B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）

C、SYSTEM（完全控制）Administrator（完全控制）Inernet来宾账户（读取和运行） D、SYSTEM（完全控制）Administrator（完全控制）

262、对于数据库的描述一下哪项说法是正确的？（A）

A、数据和一系列规则的集合 B、一种存储数据的软件

C、一种存储数据的硬件 D、是存放人量数据的软件

263、攻击者可能利用不必要的extproc外部程序调用功能获取对系统的控制权，威胁系统安全。关闭Extproc功能需要修改TNSNAMES.ORA和LISTENER.ORA文件删除一下条目，其中有一个错误的请选择出来（A）。

A、sys\_ertproc B、icache\_extproc

C、PLSExtproc D、extproc

264、关系数据库中，实现实体之间的联系是通过表与表之间的（D）。

A、公共索引 B、公共存储

C、公共元组 D、公共属性

265、关系型数据库技术的特征由一下哪些元素确定的？（A）

A、行和列 B、节点和分支

C、Blocks和Arrows D、父类和子类

266、关于WEB应用软件系统安全，说法正确的是（D）？

A、Web应用软件的安全性仅仅与WEB应用软件本身的开发有关

B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C、黑客的攻击主要是利用黑客本身发现的新漏洞

D、以任何违反安全规定的方式使用系统都属于入侵

267、目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（D）？

A、数据库系统庞大会提供管理成本 B、数据库系统庞大会降低管理效率

C、数据的集中会降低风险的可控性 D、数据的集中会造成风险的集中

268、哪一个是PKI体系中用以对证书进行访问的协议（B）？

A、SSL B、LDAP C、CA D、IKE

269、如果一个SQL Server数据库维护人员，需要具有建立测试性的数据库的权限，那么应该指派给他哪个权限（A）？

A、Database Creators B、System Administrators

C、Server Administrators D、Security Adiministrators

270、如果以Apache 为WWW服务器，（C）是最重要的配置文件。

A、access.conf B、srm.cong C、httpd.conf D、mime.types

271、若有多个Oracle数据需要进行集中管理，那么对sysdba的管理最好选择哪种认证方式（B）？

A、系统认证 B、password文件认证方式 C、域认证方式 D、以上三种都可

272、数据库管理系统DBMS主要由哪两种部分组成？（A）

A、文件管理器和查询处理器 B、事务处理器和存储管理器

C、存储管理器和查询处理器 D、文件管理器和存储管理器

273、数据库系统与文件系统的最主要区别是（B）。

A、数据库系统复杂，而文件系统简单

B、文件系统不能解决数据冗余和数据独立性问题，而数据库系统可以解决

C、文件系统只能管理程序文件，而数据库系统能够管理各宗类型的文件

D、文件系统管理的数据量较少，而数据库系统可以管理庞大的数据量

274、为了防止电子邮件中的恶意代码，应该由（A）方式阅读电子邮件。

A、纯文本 B、网页 C、程序 D、会话

275、为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机（D）？

A、SMTP身份认证 B、逆向名字解析 C、黑名单过滤 D、内容过滤

276、为什么要对数据库进行“非规范化”处理（B）？

A、确保数据完整性 B、增加处理效率 C、防止数据重复 D、节省存储空间

277、下列不属于WEB安全性测试的范畴的是（A）？

A、数据库内容安全性 B、客户端内容安全性

C、服务器端内容安全性 D、日志功能

278、下列操作中，哪个不是SQL Server服务管理器功能（A）？

A、执行SQL查询命令 B、停止SQL Server 服务

C、暂停SQL Server服务 D、启动SQL Server服务

279、下列关于IIS的安全配置，哪些是不正确的（C）？

A、将网站内容移动到非系统驱动程序 B、重命名IUSR账户

C、禁用所有WEB服务扩展 D、创建应用程序池

280、下列哪些不是广泛使用http服务器？（D）

A、W3C B、Apache C、IIS D、IE

281、下列哪些属于WEB脚本程序编写不当造成的（C）？

A、IIS5.0 Webdav Ntdll.dll远程缓冲区一处漏洞

B、apache可以通过../../../../../../../etc/passwd方位系统文件

C、登陆页面可以用password=’a’or’a’=’a’绕过

D、数据库中的口令信息明文存放

282、下列哪种方法不能有效的防范SQL进入攻击（C）？

A、对来自客户端的输入进行完备的输入检查

B、把SQL语句替换为存储过程、预编译语句或者使用ADO命令对象

C、使用SiteKey技术

D、关掉数据库服务器或者不使用数据库

283、下列哪种工具不是WEB服务器漏洞扫描工具（B）？

A、Nikto B、Web Dumper C、paros Proxy D、Nessus

284、下列哪种攻击不是针对统计数据库的（D）？

A、小查询集合大查询集攻击 B、中值攻击 C、跟踪攻击 D、资源解析攻击

285、下列哪项中是数据库中涉及安全保密的主要问题（A）？

A、访问控制问题 B、数据的准确性问题

C、数据库的完整性问题 D、数据库的安全性问题

286、下列应用服务器中，不遵循J2EE规范的是（C）？

A、MTS B、WebLogic C、Oracle 9iApplication Server D、WebSpere

287、下面关于IIS报错信息含义的描述正确的是（B）？

A、401-找不到文件 B、403-禁止访问 C、404-权限问题 D、500-系统错误

288、下面关于Oracle进程的描述，哪项是错误的（B）？

A、运行在Windows平台上的Oracle能让每个用户组程序化地打开新的进程，这是一个安全隐患

B、在Windows平台，除了Oracle.exe进程外还有其他的独立进程

C、unix平台上有多个独立运行的进程，包括数据写进程、日志写进程、存档进程、系统监控进程、进程监控进程

D、有一个特殊的内存区域被映射为\*nix平台上的所有进程，此区域时系统全局去

289、下面哪一项是与数据库管理员（DBA）职责不相容的（C）？

A、数据管理 B、信息系统管理 C、系统安全 D、信息系统规划

290、下面选型中不属于数据库安全控制的有（D）。

A、信息流控制 B、推论控制 C、访问控制 D、隐通道控制

291、下面选型中不属于数据库安全模型的是（D）。

A、自主型安全模型 B、强制型安全模型 C、基于角色的模型 D、访问控制矩阵

292、一般来说，通过WEB运行http服务的子进程时，我们会选择（D）的用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

293、一下不是数据库的加密技术的是（D）。

A、库外加密 B、库内加密 C、硬件加密 D、固件加密

294、一下对于Oracle文件系统描述错误的是（B）？

A、\*nix下Oracle的可执行文件在$Oracle\_HOME/bin/Oracle,$Oracle\_HOME/bin也应该包含在路径环境变量内

B、Windows下Oracle的可执行文件在%Oracle\_HOME%\bin\Oracle.exe,其他

C、硬件加密 D、固件加密

295、以下几种功能中，哪个是DBMS的控制功能（A）？

A、数据定义 B、数据恢复 C、数据修改 D、数据查询

296、以下哪个安全特征和机制是SQL数据库所特有的（B）？

A、标识和鉴别 B、数据恢复 C、数据修改 D、数据查询

297、以下哪个是数据库管理员（DBA）可以行使的职责（A）？

A、系统容量规划 B、交易管理 C、审计 D、故障承受机制

298、以下哪条命令能利用“SQL注入”漏洞动用XP\_cmdshell存储过程，获得某个子目的清单？（A）

A、http://localhost/script?’:EXEC+master..XP\_cmdshell+’dir’:--

B、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’:--

C、http://localhost/script?0’:EXEC+master..XP\_cmdshell+’ dir’:--

D、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’--

299、以下哪条命令能利用“SQL”漏洞动用XP\_cmdshell存储过程，启动或停止某项服务？（B）

A、http://localhost/script?’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;-

B、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;--

C、http://localhost/script?1’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ; --

D、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ --

300、以下哪项不属于访问控制策略的实施方式？（D）

A、子模式法 B、修改查询法 C、集合法 D、验证法

301、以下哪一项是和电子邮件系统无关的？（C）

A、PEM(Privacy enhanced mail) B、PGP(Pretty good privacy)

C、X.500 D、X.400

302、以下哪种方法可以用于对付数据库的统计推论？（C）

A、信息流控制 B、共享资源矩阵 C、查询控制 D、间接存取

303、以下是对层次数据库结构的描述，请选择错误描述的选项。（C）

A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来

B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据

C、它的优点是用户不需要十分熟悉数据库结构

D、层次数据库模型的结构就像是一棵倒转的树

304、以下是对单用户数据库系统的描述，请选择错误描述的选项（C）。

A、单用户数据库系统是一种早期的最简单的数据库系统

B、在单用户系统中，整个数据库系统，包括应用程序、DBMS、数据，都装在一台计算机之间不能共享数据

C、在单用户系统中，由多个用户共用，不同计算机之间能共享数据

D、单用户数据库系统已经不适用于现在的使用，被逐步淘汰了

305、以下是对分布式结构数据库系统的描述，请选择错误描述的选项。（D）

A、分布式结构的数据库系统的数据在逻辑上是一个整体，但物理地分布在计算机网络的不同节点上，每个节点上的主机又带有多个终端用户

B、网络中的每个节点都可以独立的处理数据库中的数据，执行全局应用

C、分布式结构的数据库系统的数据分布存放给数据的处理、管理和维护带来困难

D、分布式结构的数据库系统的数据只在存放在服务器端，其他节点只进行处理和执行

306、以下是对关系数据库结构的描述，请选择错误描述的选项。（D）

A、数据存储的主要载体是表，或相关数据组

B、有一对一、一对多、多对多三种表关系

C、表关联是通过引用完整性定义的，这是通过主码和外码（主键或外键约束条件实现的）

D、缺点是不支持SQL语言

307、以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（A）

A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力

B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行DBMS功能又执行应用程序

C、在网络中把某些节点的计算机专门用于执行DBMS核心功能，这台计算机就成为数据库服务器

D、其他节点上的计算机安装DBMS外围应用开发工具和应用程序，支持用户的应用，称为客户机

308、以下是对面向对象数据库结构的描述，请选择错误描述的选项。（C）

A、它允许用对象的概念来定义与关系数据库交互

B、面向对象数据库中有两个基本的结构：对象和字面量

C、优点是程序员需要掌握与面向对象概念以及关系数据库有关的存储

D、缺点是用户必须理解面向对象概念，目前还没有统一的标准，稳定性还是一个值得关注的焦点

309、以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（D）

A、主从式结构是指一个主机带多个终端的多用户结构

B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上

C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源

D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈

311、在GRUB的配置文件grub.conf中，“timeout=-1”的含义是（C）。

A、不等待用户选择，直接启动默认的系统

B、在10秒钟内，等待用户选择要启动的系统

C、一直等待用户选择要启动的系统

D、无效

312、在Oracle中，quota可以限制用户在某个表空间上最多可使用多少字节，如果要限制data\_ts表500K，以下哪个是正确的命令？（B）

A、quo 500k in data\_ts B、quota 500K on data\_ts

C、quota data\_ts ,imit 500K D、quota data\_ts on 500K

313、在Oracle中，建表约束包括引用完整性约束、check完整性约束，还有以下三项是正确的，请排除一个错误选项。（D）

A、非空完整性约束 B、唯一完整性约束

C、主码完整性约束 D、数据角色性约束

314、在Oracle中，将scott的缺省表空间改为data2\_ts，下列哪个是正确的？（A）

A、ALTER USER scott DEFAULT TABLESPACE data2\_ts

B、ALTER DEFAULT TABLESPACE data2\_ts USER scott

C、ALTER USER scott TABLESPACE DEFAULT data2\_ts D、ALTER scott USER DEFAULT TABLESPACE data2\_ts

315、在Oracle中，将scott的资源文件改为otherprofile，下列哪个是正确的？（C）

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

316、在Oracle中，将当前系统所有角色都授予scott，除Payroll外，下列哪个是正确的？（D）

A、ALTER DEFAULT ROLLE USER　　scott ALL EXCEPT Payroll

B、ALTER USER DEFAULT ROLLE ALL EXCEPT Payroll

C、ALTER DEFAULT ROLLE ALL EXCEPT USER scott

D、ALTER USER scott DEFAULT ROLLE ALL EXCEPT Payroll

317、在Oracle中，用ALTER将scott的口令改为hello，下列哪个是正确的？（A）

A、ALTER USER scott IDENTIFIED BY hello

B、ALTER scott USER IDENTIFIED BY hello

C、ALTER USER scott IDENTIFIED AS hello

D、ALTER USER hello IDENTIFIED BY scott

318、在WEB应用软件的基本结构中，客户端的基础是（A）。

A、HTML文档 B、客户端程序

C、HTML协议 D、浏览器

319、在WEB应用软件的系统测试技术中，下面不属于安全性测试内容的是（C）。

A、客户端的内容安全性 B、服务器的内容安全性

C、数据库的内容安全性 D、Cookie安全性

320、在典型的WEB应用站点的层次结构中，“中间件”是在哪里运行的？（C）

A、浏览器客户端 B、web服务器

C、应用服务器 D、数据库服务器

321、在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（C）

A、对话管理服务 B、事务管理服务

C、资源管理服务 D、控制管理服务

322、主要用于加密机制的协议时（D）。

A、HTTP B、FTP C、TELNETD D、SSL

323、分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？（D）

A、自主性 B、可靠性 C、灵活性 D、数据备份

324、下面对Oracle的密码规则描述，哪个是错误的？（D）

A、Oracle密码必须由英文字母，数值，#，下划线(\_)，美元字符（$）构成，密码的最大长度为30字符，并不能以“$”，“#”，“\_”或任何数字卡头；密码不能包含像“SELECT”，“DELETE”，“CREATE”这类的ORACLE/SQL关键字

B、Oracle的若算法加密机制（）两个相同的用户名和密码在两台不同的ORACLE数据库机器中，将具有相同的哈希值。这些哈希值存储在SYS.USER表中，可以通过像DBA\_USE这类的试图来访问

C、Oracle默认配置下，每个中户如果有10此的失败登录，此账户将会被锁定

D、SYS账户在Oracle数据库中有最高权限，能够做任何事情，包括启动/关闭Oracle数据库，如果SYS被锁定，将不能访问数据库

325、无论是哪一种Web服务器，都会受到HTTP协议本身安全问题的困扰，这样的信息系统安全漏洞属于（C）。

A、设计型漏洞 B、开发型漏洞 C、运行型漏洞 D、以上都不是

326、SSL加密的过程包括以下步骤：（1）通过验证以后，所有数据通过密钥进行加密，使用DEC和RC4加密进行加密；（2）随后客户端随机生成一个对称密钥；（3）信息通过HASH加密，或者一次性加密（MD5SHA）进行完整性确认；（4）客户端和服务器协商建立加密通道的特定算法。正确的顺序的是（D）

A、（4）（3）（1）（2） B、（4）（1）（3）（2） C、（4）（2）（3）（1） D、（4）（2）（3）（1）

327、影响WEB系统安全的因素，不包括？（C）

A、复杂应用系统代码量大、开发人员多、难免出现疏忽

B、系统屡次升级、人员频繁变更，导致代码不一致

C、历史遗留系统、试运行系统等对个WEB系统运行于不同的服务器上

D、开发人员未经安全编码培训

328、Oracle通过修改用户密码策略可提高密码强度，以下哪个密码策略参数中文描述是错误的？（A）

A、PASSWORD\_MAX 登录超过有效次数锁定时间

B、FAILED\_LOGIN\_ATTEMPTS 最大错误登录次数

C、PASSWORD\_GRACE\_TIME 密码失效后锁定时间

D、PASSWORD\_LIFE\_TIME 口令有效时间

329、SQL Server服务有一个启动账号，默认账号是属于administrators组，现在为了安全需要创建一个新的服务启动账号，它需要哪些权限既能兼顾安全又能保证启动数据库成功，请排除一个错误的。（D）

A、数据库本地目录的读写权限 B、启动本地服务的权限

C、读取注册表的权限 D、通过API访问Windows Resource

330、作为一台运行IIS 在Internet发布站点的Windows Web服务器，下面哪项服务不是必需的？（B）

A、IIS Admin B、Net Logon

C、Performance Logs and Alerts D、World Wide Web Publishing

331、数据库中超级账户不能被锁定，其中Oracle的是（），mysql的是（），SQLServer的是（C）。

A、sa，root，sys B、admin，root，sa

C、sys，root，sa D、sys，admin，sa

332，Oracle的安全机制，是由（A）、实体权限和角色权限这三级体系结构组成的。

A、系统权限 B、索引权限 C、操作权限 D、命令控制

333、对SQL数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（B）

A、-- B、- C、-= D、-+

334、在Web页面中增加验证码功能后，下面说法正确的是（A）。

A、可以增加账号破解等自动化软件的攻击难度 B、可以防止文件包含漏洞 C、可以防止缓冲溢出 D、可以防止 浏览

335、以下破解Oracle密码哈希值的步棸，其中哪个描述是错误的？（B）

A、用Sqlplus直接登录到Oracle数据库，使用select username，password form dba\_users命令查看数据库中的用户名和密码，此时看到的密码是哈希值

B、在Cain的Cracker菜单点击导入用户名和哈希值，可直接显示用户密码明文

C、在Cain的Cracker菜单点解导入用户名和哈希值，只能通过字典破解 D、在Cain的Rainbow生成的表会占用大量的硬盘空间和内存，可是破解速度和效率很高

336、在数据库向因特网开放前，哪个步棸是可以忽略的？（B）

A、安全安装和配置操作系统和数据库系统

B、应用系统应该在内网试运行3个月

C、对应用软件如Web也没、ASP脚本等进行安全性检查

D、网络安全策略已经生效

337、如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf文件，查看是否包含如下设置，选出一个正确的（D）。

A、audit=filename B、sys=filename C、event=filename D、log=filename

338、针对一台对外提供Web服务的Windows服务器，下列关于账户权限控制，哪些项是不合理的？（C）

A、限制匿名账户对Web内容的目录写权限

B、从Everyone组中删除“从网络访问此计算机” 用户权限

C、禁用IUSR-MACHE和IWAN\_MACHINE账户

D、本地登录时必须使用Administrators账户

339、网上营业中间件如果启用了SSl，应采用不低于（C）版本的SSL，采用经国家密码管理局认可的密码算法。

A、2.0 B、2.5 C、3.0 D、3.1

340、SQL Server默认的具有DBA权限的账号是什么？（C）

A、root B、admin C、sa D、system

341、（A）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

342、（C）是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

343、《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（B）。

A、GA 163-1997 B、GA 267-2000

C、GA 243-2000 D、GB 17859-1999

344、安装了合格防雷保安器的计算机信息系统，还必须在（C）雷雨季节前对防雷保安器、保护接地装置进行一次年度检查，发现不合格时，应及时修复或更换。

A、第三年 B、第二年 C、每年 D、当年

345、使用IIalon灭火的工作原理是什么？（C）

A、降低温度 B、隔绝氧气和可燃物

C、破坏氧气和可燃物之间的化学反应 D、减少氧气

346、白炽灯、高压汞灯与可燃物、可燃结构之间的距离不应小于（C）cm。

A、30 B、40 C、50 D、60

347、被电击的人能否获救，关键在于（D）。

A、触电的方式 B、人体电阻的大小

C、触电电压的高底 D、能否尽快脱离电源和施行紧急救护

348、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）。

A、可以随意弯折 B、转弯是，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

349、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

350、长期在高频电磁场作用下，操作者会有什么不良反应？（B）

A、呼吸困难 B、神经失常 C、疲劳无力

351、触电事故中，绝大部分是由于（A）导致人身伤亡的。

A、人体接受电流遭到电击 B、烧伤 C、触电休克

352、从业人员发现直接危及人身安全的紧急情况时，例如气体灭火系统开始开启时，应（A）。

A、停止作业，立即撤离危险现场 B、继续作业

C、向上级汇报，等待上级指令

353、从业人员既是安全生产的保护对象，又是实现安全生产的（C）。

A、关键 B、保证 C、基本要素

354、低压验电笔一般适用于交、直流电压未（C）伏以下。

A、220 B、380 C、500

355、电流为（B）毫安是，称为致命电流。

A、50 B、100 C、120 D、150

356、电器的保险丝只能装在（B）上。

A、零线 B、火线 C、底线

357、电器着火是不能用（C）灭火。

A、四氧化碳或1211灭火 B、沙土 C、水

358、对不符合防雷标准、规范防雷工程专业设计方案，以下（B）应当按照审核结论进行修改并重新报批。

A、建设单位 B、防雷工程专业设计单位 C、工程施工单位

359、发现人员触电时，应（B），使之脱离电源。

A、立即用手拉开触电人员 B、用绝缘物体拨开电源或触电者 C、用铁棍拨开电源线

360、凡设在年平均雷电日大于（C）的地区的计算机信息系统，原则上均应装设计算机信息系统防雷保安器，以防止雷电电磁脉冲过电压和过电流侵入计算机信息系统设备。

A、40 B、45 C、5 D、15

361、废电池随处丢弃会造成（B）的污染。

A、白色污染 B、重金属污染 C、酸雨

362、干粉灭火器多长时间检查一次？（A）

A、半年 B、一年 C、三个月 D、两年

363、根据国家相关规定，电压（D）以下不必考虑防止电击的安全？

A、48伏 B、36伏 C、65伏 D、25伏

364、根据作业环境的不同，安全帽的颜色也不同，如在爆炸性作业场所工作宜戴（A）安全帽。

A、红色 B、黄色 C、白色

365、关于空气的正向压力，下面哪项描述是正确的？（B）

A、当门打开时，空气向内流动 B、当门打开，空气向外流动

C、当发生火灾，系统自动切断电源 D、当发生火灾，烟雾向另外一间房间流动

366、国家颁布的《安全色》标准中，表示警告、主要的颜色为（C）。

A、红色 B、蓝色 C、黄色

367、火灾中对人员威胁最大的是（B）。

A、火 B、烟气 C、可燃物

368、机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（B）m。

A、0.1 B、0.6 C、1.2 D、0.3

369、计算机电源系统的所有节点均应镀铅锡处理（B）连接。

A、热压 B、冷压 C、焊锡 D、直接

370、计算机系统接地应采用（A）。

A、专用底线 B、和大楼的钢筋专用网相连

C、大楼的各种金属管道相连 D、没必要

371、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

372、计算机系统应选用（A）电缆。

A、铜芯 B、铅芯

C、铁芯 D、没有要求

373、进行腐蚀品的装卸作业应戴（B）手套。

A、帆布 B、橡胶 C、棉布

374、人体在电磁场作用下，由于（C）将使人体受到不同程度的伤害。

A、电流 B、电压 C、棉布

375、身上着火后，下列哪种灭火方法是错误的（C）。

A、就地打滚 B、用厚重衣物覆盖压灭火苗 C、迎风快跑

376、生产经营单位必须为从业人员提供符合国家标准或（C）标准的劳动防护用品。

A、当地 B、本单位 C、行业

377、使用新设备，必须了解、掌握其安全技术特征，采取有效的安全防护措施，并对从业人员进行专门的安全生产。（B）

A、当地 B、本单位 C、行业

378.实验地点相对湿度大于75%时，则此实验环境属于易触电的环境：（A）

A、危险 B、特别危险 C、一般

379、通过人身的安全交流电流规定在(A)以下。

A、10mA B、30mA C、50mA

380、下列不属于对物理层信息窃取的是(D)

A、对存储介质的盗取 B、对监视器的窃听

C、对网络线路的窃听 D、对设备屏蔽电磁干扰

381、新、改、扩建项目的安全设施投资应当纳入(C)。

A、企业成本 B、安措经费 C、建设项目概算

382、液体表面的蒸汽与空气形成可燃气体，遇到点火源时，发生一闪即灭的现象称为(C)

A、爆炸 B、蒸发 C、闪燃

383、防雷保安器：防止(B)破坏计算机信息系统的保安装置，可分为两大类：电源

线防雷保安器（简称电源防雷保安器）和信号传输线防雷保安器（简称通道防雷保安器）。

A、直击雷 B、感应雷 C、雷暴 D、雷电电磁脉冲

384、EMC标准是为了保证(D)正常工作而制走的。

A、网络 B、媒体 C、信息 D、系统和设备

385、以下不符合防静电要求的是(B)。

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

386、以下哪些属于系统的物理故障？(A)

A、硬件故障与软件故障 B、计算机病毒

C、人为的失误 D、网络故障和设备环境故障

387、用灭火器灭火时，灭火器的喷射口应该对准火焰的(C)。

A、上部 B、中部 C、根部

388、运输、携带、邮寄计算机信息媒体进出靖的，应当如实向(A)申报。

A、海关 B、工商

C、税务 D、边防

389、在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ (B)

A、产生静电 B、计算机部件腐蚀

C、有污染物 D、B+A

390、在空气不流通的狭小地方使用二氧化碳灭火器可能造成的危险是(B)。

A中毒 B缺氧 C爆炸

391、在雷雨天不要走近高压电杆、铁塔、避雷针、远离至少(C)米以外。

A、IO米 B、15米 C、20米

392、在易燃易爆场所穿(C)最危险。

A、布鞋 B、胶鞋 C、带钉鞋

393、在遇到高压电线断落地面时，导线断落点(B)m内，禁止人员进入。

A、IO B、20 C、30

394、数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？(C)

A、30%-40% B、40%-50% C、45%-60% D、50%-70%

395、计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所

以防雷保安器必须有合理的(B)。

A、屏蔽配置 B、接地配置

C、分流配置 D、均压配置

396、计算站场地宜采用(A)蓄电池。

A、封闭式 B、半封闭式

C、开启式 D、普通任意的

397、多层的楼房中，最适合做数据中心的位置是(D)。

A、楼 B、地下室

C、顶楼 D、除以上外的任何楼层

398、计算机机房是安装计算机信息系统主体的关键场所，是(A)工作的重点，所以

对计算机机房要加强安全管理。

A、实体安全保护 B、人员管理

C、媒体安全保护 D、设备安全保护

399、区域安全，首先应考虑（B），用来识别来访问的用户的身份，并对其合法性进行验证，主要通过特殊标示符、口令、指纹等来实现。

A、来访者所持物 B、物理访问控制 C、来访者所具有的特征 D、来访者所知信息

400、在计算机房出入口处或值班室，应设置（D）和应急断电装置。

A、 电视 B、电扇 C、报警器 D、应急电话

401、下列（A）灭火器是扑救精密仪器火灾的最佳选择。

A、二氧化碳灭火剂 B、干粉灭火剂 C、泡沫灭火剂

402、电气安全主要包括人身安全、（B）安全。

A、照明 B、设备 C、电器 D、空调

403、（C）基于IDEA算法。

A、S/MIME B、SET C、PGP D、SSL

404、

405、(C)是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

406、(D)是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。

A、认证机构 B、密码 C、票据 D、数字证书

407、（D）协议主要用于加密机制。

A、HTTP B、FTP C、TELNET D、SSL

408、（A）原则保证只有发送方与接收方能访问消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

409、（D）原则允许某些用户进行特定访问。

A、保密性 B、鉴别 C、完整性 D、访问控制

410、（B）增加明文冗余度。

A、混淆 B、扩散 C、混淆与扩散 D、都不是

411、3DES加密算法的密钥长度是：（A）。

A、168 B、128 C、56 D、256

412、AES密钥长度不能是（D）。

A、128位 B、192位 C、256位 D、512位

413、AES算法是哪种算法？（A）。

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

414、AES属于哪种加密方式？（B）。

A、流加密 B、分组加密 C、异或加密 D、认证加密

415、CA指的是（A）。

A、证书授权 B、加密认证 C、虚拟专用网 D、安全套接层

416、DES经过（A）轮运算后，左右两部分合在一起经过一个末置换，输出一个64位的密文。（A）

A、16 B、8 C、32 D、4

417、DES算法是哪种算法？（A）

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

418、DES属于哪种加密方式？（B）

A、流加密 B、块加密 C、异或加密 D、认证加密

419、DNSSec中并未采用（C）。

A、数字签名技术 B、公钥加密技术 C、地址绑定技术 D、报文摘要技术

420、ECB指的是（D）。

A、密文链接模式 B、密文反馈模式 C、输出反馈模式 D、电码本模式

421、EC-DSA复杂性的程度是（D）。

A、简单 B、最简单 C、困难 D、最困难

422、EFS可以用在什么文件系统下（C）。

A、FAT16 B、FAT32 C、NTFS D、以上都可以

423、IDEA的密钥长度是多少bit？（D）。

A、56 B、64 C、96 D、128

424、Kerberos是80年代中期，麻省理工学院为Athena项目开发的一个认证服务系统，其目标是把认证、记账和（B）的功能扩展到网络环境。

A、访问控制 B、审计 C、授权 D、监控

425、Kerberos是为TCP/IP网络设计的基于（B）的可信第三方鉴别协议，负责在网络上进行仲裁及会话密钥的分配。

A、非对称密钥体系 B、对称密钥体系 C、公钥体系 D、私钥体系

426、Kerberos是一种网络认证协议。它采用的加密算法是（C）。

A、RSA B、PGP C、DES D、MD5

427、Kerberos算法是一个（B）。

A、面向访问的保护系统 B、面向票据的保护系统

C、面向列表的保护系统 D、面向门与锁的保护系统

428、Kerberos提供的最重要的安全服务是？（A）。

A、鉴别 B、机密性 C、完整性 D、可用性

429、MD5产生的散列值是多少位？（C）。

A、56 B、64 C、128 D、160

430、MD5是按每组512位为一组来处理输入的信息，经过一系列变换后，生成一个（B）为散列值。

A、64 B、128 C、256 D、512

431、MD5是以512位分组来处理输入的信息，每一分组又被划分为（A）32位子分组。

A、16个 B、32个 C、64个 D、128个

432、MD5算法将输入信息M按顺序每组（D）长度分组，即：M1，M2，...，Mn-1，Mn。

A、64位 B、128位 C、256位 D、512位

433、PKI（公共密钥基础结构）中应用的加密方式为（B）。

A、对称加密 B、非对称加密 C、HASH加密 D、单向加密

434、PKI的全称是（D）。

A、Private Key Intrusion B、Public Key Intrusion

C、Private Key Infrastructure D、Public Key Infrastructure

435、PKI无法实现（D）。

A、身份认证 B、数据的完整性 C、数据的机密性 D、权限分配

436、RC4是由RIVEST在1987年开发的一种流式的密文，就是实时地把信息加密成一个整体，它在美国一般密钥长度是128位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）。

A、64位 B、56位 C、40位 D、32位

437、RSA公钥加密系统中，他想给她发送一份邮件，并让她知道是他发出，应选用的加密秘钥是（C）。

A、他的公钥 B、她的公钥 C、他的私钥 D、她的私钥

438、RSA使用不方便的最大问题是（A）。

A、产生密钥需要强大的计算能力 B、算法中需要大数

C、算法中需要素数 D、被攻击过很多次

439、RSA算法建立的理论基础是（C）。

A、DES B、替代想组合 C、大数分解和素数检测 D、哈希函数

440、SHA-1产生的散列值是多少位？（D）。

A、56 B、64 C、128 D、160

441、按密钥的使用个数，密码系统可以分为（C）。

A、置换密码系统和易位密码系统 B、分组密码系统和序列密码系统

C、对称密码系统和非对称密码系统 D、密码系统和密码分析系统

442、充分发挥了DES和RSA两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是：（C）。

A、数字签名 B、数字指纹 C、数字信封 D、数字时间戳

443、从技术角度上看数据安全的技术特征主要包含哪几个方面？（B）。

A、数据完整性、数据的方便性、数据的可用性 B、数据的完整性、数据的保密性、数据的可用性 C、数据的稳定性、数据的保密性、数据的可用性 D、数据的方便性、数据的稳定性、数据的完整性

444、单项散列函数的安全性来自于他的（A）。

A、单向性 B、算法复杂性 C、算法的保密性 D、离散性

445、电路网关防火墙工作在OSI协议的哪一层？（A）。

A、传输层 B、链路层 C、应用层 D、物理层

446、电子邮件的机密性与真实性是通过下列哪一项实现的？（A）

A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密

B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密

C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密

D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

447、端对端加密只需要保证消息都在哪里进行加密？（A）

A、源点和目的地节点 B、经过的每一个节点

C、源点和中间经过的每一个节点 D、所有节点

448、对明文字母重新排列，并不隐藏他们的加密方法属于（C）。

A、置换密码 B、分组密码 C、易位密码 D、序列密码

449、对网络中两个相邻节点之间传输的数据进行加密保护的是（A）。

A、节点加密 B、链路加密 C、端到端加密 D、DES加密

450、发送消息和用发送方私钥加密哈希加密信息将确保消息的：（A）。

A、真实性和完整性 B、真实性和隐私 C、隐私和不可否认性 D。隐私和不可否性

451、高级加密标准AES算法中，加密回合数不可能是（D）。

A、10 B、12 C、14 D、16

452、公钥机制利用一对互相匹配的（B）进行加密，解密。

A、私钥 B、密钥 C、数字签名 D、数字证书

453、公钥加密体制中，没有公开的是（A）。

A、明文 B、密文 C、公钥 D、算法

454、公钥证书提供了一种系统的、可扩展的、统一的（A）。

A、公钥分发方案 B、实现不可否认方案

C、对称密钥分发方案 D、保证数据完整性方案

455、关于CA和数字证书的关系，以下说法不正确的是（B）。

A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由CA签发

B、数字证书一般依靠CA中心的对称密钥机制来实现

C、在电子交易中，数字证书可以用于表明参与方的身份

D、数字证书能以一种不能被假冒的方式证明证书持有人身份

456、关于数字签名说法正确的是（A）。

A、数字签名的加密方法以目前的计算机的运算能力来破解是不现实的

B、采用数字签名，不能够保证信息自签发后到收到为止没有做过任何修改（能保证信息收到后没做个任何修改）

C、采用数字签名，能够保证信息是有签名者自己签名发送的，但由于不是真实的签名，签名者容易否认（签名不容易否认）

D、用户可以采用公钥对信息加以处理，形成数字签名（需使用私钥对信息加以处理）

457、基于私有密钥体制的信息认证方法采用的算法是（D）。

A、素数检测 B、非对称算法 C、RSA算法 D、对称加密算法

458、加密技术不能实现（D）。

A、数据信息的完整性 B、基于密码技术的身份认证 C、机密文件加密 D基于IP头信息的包过滤

459、加密技术不能提供以下哪种安全服务？（D）。

A、鉴别 B、机密性 C、完整性 D可用性

460、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）。

A、对称密钥加密 B、非对称密钥加密 C、 D

461、假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（A）。

A、对称加密技术 B、分组加密技术 C、公钥加密技术 D、单项函数密码技术

462、就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。（C）

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

463、利用非对称密钥体制实现加密通信时，若A要向B发送加密信息，则该加密信息应该使用（B）。

A、A的公钥加密 B、B的公钥加密 C、A的私钥加密 D、B的私钥加密

464、利用物理设备将各类型的无法预测的输入集中起来生成随机数的设备是（A）。

A、随机数生成器 B、伪随机数生成器 C、中央处理 D、非易失存储

465、链路加密要求必须先对链路两端的加密设备进行（C）。

A、异步 B、重传 C、同步 D、备份

466、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？（C）

A、对称的公钥算法 B、非对称私钥算法 C、对称密钥算法 D、非对称密钥算法

467、密码分析的目的是什么？（A）

A、确定加密算法的强度 B、增加加密算法的代替功能

C、减少加密算法的换为功能 D、确定所使用的换位

468、请从下列各项中选出不是HASH函数算法的一项。（D）

A、MD5 B、SHA C、HMAC D、MMAC

469、如今，DES加密算法面临的问题是（A）。

A、密钥太短，已经能被现代计算机暴力破解 B、加密算法有漏洞，在数学上已被破解 C、留有后门，可能泄露部分信息 D、算法过于陈旧，已经有更好的替代方案

470、若单项散列函数的输入串有很小的变化，则输出串（A）。

A、可能有很大的变化 B、一定有很大的变化 C、可能有很小的变化 D、一定有很小的变化

471、散列算法可以做哪些事？（C）。

A、碰撞约束 B、入侵检测 C、组合散列 D、随机数生成器

472、身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（B）。

A、可信性 B、访问控制 C、完整性 D、保密性

473、数字签名常用的算法有（B）。

A、DES算法 B、RSA算法 C、Hash函数 D、AES算法

474、数字签名和随机数挑战不能防范以下哪种攻击或恶意行为？（D）。

A、伪装欺骗 B、重放攻击 C、抵赖 D、DOS攻击

475、数字签名可以解决（D）。

A、数据被泄露 B、数据被篡改 C、未经授权擅自访问 D、冒名发送数据或发送后抵赖

476、数字签名通常使用（B）方式。

A、公钥密码体系中的私钥 B、公钥密码系统中的私钥对数字摘要进行加密

C、密钥密码体系 D、公钥密码体系中公钥对数字摘要进行加密

477、数字信封是用来解决（C）。

A、公钥分发问题 B、私钥分发问题 C、对称密钥分发问题 D、数据完整性问题

478、数字证书不包括（B）。

A、签名算法 B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号 D、颁发数字证书单位的数字签名

479、数字证书的应用阶段不包括（D）。

A、证书检索 B、证书验证 C、密钥恢复 D、证书撤销

480、下列说法中错误的是（D）。

A、非对称算法也叫公开密钥算法 B、非对称算法的加密密钥和解密密钥是分离的 C、非对称算法不需要对密钥通信进行保密 D、非对称算法典型的有RSA算法、AES算法等

481、下列算法中，哪种不是对称加密算法？（C）

A、AES B、DES C、RSA D、RC5

482、下列算法中属于Hash算法的是（C）。

A、DES B、IDEA C、SHA D、RSA

483、以下对于链路加密哪项是正确的？（B）

A、消息只在源点加密，目的节点解密 B、消息在源点加密，在每一个经过的节点解密并加密 C、消息在所有经过的节点中都是加密的，但只在目的节点解密 D、消息以明文形式在节点之间传输

484、以下各种加密算法中属于单钥制加密算法的是（A）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密算法

485、以下各种加密算法中属于双钥制加密算法的是（D）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密486、以下各种算法中属于古典加密算法的是（B）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密487、以下关于CA认证中心说法正确的是（C）。

A、CA认证时使用对称密钥机制的认证方法 B、CA认证中心支负责签名，不负责证书的产生 C、CA认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份 D、CA认证中心不用保持中立，可以随便找一个用户来作为CA认证中心

488、以下关于VPN说法正确的是（B）。

A、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B、VPN指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接

C、VPN不能做到信息认证和身份认证 D、VPN只能提供身份认证、不能提供加密数据的功能

489、以下关于数字签名说法正确的是（D）。

A、数字签名是在所传输的数据后附上一段和传输数据毫无关系的数字信息

B、数字签名能够解决数据的加密传输，即安全传输问题

C、数字签名一般采用对称加密机制 D、数字签名能够解决篡改、伪造等安全性问题

490、以下密码使用方法中正确的是（D）。

A、将密码记录在日记本上以避免忘记 B、任何情况下均不得使用临时性密码

C、密码中的字母不得重复 D、不要使用全部由字母组成的密码

491、以下哪个不包含在证书中？（C）

A、密钥采取的算法 B、公钥及其参数 C、私钥及其参数 D、签发证书的CA名称

492、以下哪个选项不会破坏数据库的完整性？（A）

A、对数据库中的数据执行删除操作 B、用户操作过程中出错

C、操作系统的应用程序错误 D、DBMS或操作系统程序出错

493、以下哪项不属于数据库系统实体安全？（B）

A、环境安全 B、线路安全 C、设备安全 D、媒体安全

494、以下哪一种算法产生最长的密钥？（D）

A、Diffe-Hellman B、DES C、IDEA D、RSA

495、以下认证方式中，最为安全的是（D）。

A、用户名+密码 B、卡+密码 C、用户名+密码+验证码 D、卡+指纹

496、远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（B）

A、知道什么 B、拥有什么 C、是谁 D、双因素认证

497、在3DES算法中，密钥最高可达到多少位？（C）

A、96 B、128 C、168 D、200

498、在IPSec中，（C）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的IPSec协议、密码算法、密钥等信息。

A、ESP B、SPI C、SA D、SP

499、在IPSec中，IKE提供（B）方法供两台计算机建立。

A、解释域 B、安全关联 C、安全关系 D、选择关系

500、在RIP的MD5认证报文中，经过加密的密钥是放在哪里的？（B）

A、保温的第一个表项里 B、报文的最后一个表项里

C、报文的第二个表项里 D、报文头里

501、在非对称加密算法中，涉及到的密钥个数是？（B）

A、一个 B、两个 C、三个 D、三个以上

502、在高级加密标准AES算法中，区块大小为（A）。

A、128位 B、192位 C、256位 D、512位

503、在给定的密钥体制中，密钥与密码算法可以看成是（A）。

A、前者是可变的，后者是固定的 B、前者是固定的，后者是可变的

C、两者都是可变的 D、两者都是固定的

504、在公钥体制中，不公开的是（B）。

A、公钥 B、私钥 C、公钥和私钥 D、私钥和加密算法

505、在密码学中，需要被交换的原消息被称为什么？（D）

A、密文 B、算法 C、密码 D、明文

506、一般证书采用哪个标准？（D）

A、ISO/IEC 15408 B、ISO/IEC 17799 C、BS 7799 D、X. 509V3

507、一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（D）

A、信息的数据和时间戳 B、识别发信的计算机

C、对信息内容进行加密 D、对发送者的身份进行识别

508、在数据库中，下列哪些数据不能加密？（A）

A、索引字段 B、存放日期字段

C、存放密码的 D、存放名称字段

509、在一个网络节点中，链路加密仅在以下哪项中提供安全性？（D）

A、数据链路层 B、物理层

C、通信层 D、通信链路

510、在以下隧道协议中，属于三层隧道协议的是（D）。

A、L2F B、PPTP C、L2TP D、IPSec

511、以下哪一项是基于一个大的整数很难分解成两个素数因数？（B）

A、ECC B、RSA C、DES D、D-H

512、以下哪种数据加密技术可以在基础架构层面进行？（A）

A、IPSec B、Secure Sockets Layer

C、Transport Layer Securit D、RSA

513、目前最安全的身份认证机制是（A）。

A、一次口令机制 B、双因素法

C、基于智能卡的用户身价认证 D、身价认证的单因素法

514、当数据库由于各种原因而使其完整性遭到破坏时，必须采取以下哪项措施来恢复数据库？（C）

A、重新安装数据库 B、换一种数据库

C、使用数据库备份 D、将数据库中的数据利用工具导出，并保存

515、PGP加密算法是混合使用（B）算法和IDEA算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES B、RSA C、IDEA D、AES

516、以下哪些软件是用于加密的软件？（A）

A、PGP B、SHA C、EFS D、DES

517、如果消息接受方要确定发送方身价，则要使用（B）原则。

A、保密性 B、鉴别 C、完整性 D、访问控制

518、对于现代密码破解，（D）是最常的方法。

A、攻破算法 B、监听截获 C、信息猜测 D、暴力破解

519、非对称密码技术的缺点有哪些？（B）

A、密钥持有量减少 B、加/解密速度慢 C、耗用资源较少 D、以上都是

520、CA不能提供下列哪种证书？（D）

A、个人数字证书 B、SSL服务器证书

C、安全电子邮件证书 D、SET服务器证书

521、以下关于混合加密方式说法正确的是（B）。

A、采用公开密钥体制进行通信过程中的加解密处理

B、采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C、采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D、采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密

处理速度快的双重优点

522、果要保证（C）原则，则不能在中途修改消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

523、口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（D）

A、长期没有修改的口令 B、过短的口令

C、两个人共用的口令 D、设备供应商提供的默认的口令

524.非对称密钥的密码技术具有很多优点，其中不包括：（B）。

A、可提供数字签名、零知识证明等额外服务

B、加密/解密速度快，不需占用较多资源

C、通信双方事先不需要通过保密信道交换密钥

D、密钥持有量大大减少

525．DES是一种block（块）密文的加密算法，是把数据加密成多大的块？（B）

A、32位 B、64位 C、128位 D、256位

526．CA数字证书中不包含的信息有（C）。

A、CA的数字签名 B、证书申请者的个人信息

C、证书申请者的私钥 D、证书申请者的公钥信息

527．以下关于对称密钥加密说法正确的是（C）。

A、加密方和解密可以使用不同的算法 B、加密密钥和解密密钥可以是不同的

C、加密密钥和解密密钥必须是相同的 D、密钥的管理非常简单

528、在为计算机设置使用密码时，下面（D）密码是最安全的。

A、12345678 B、66666666

C、20061001 D、72aB@#41

529、（C）的攻击者发生在Web应用层？

A、25% B、50%

C、75% D、90%

530、“U盘破坏者”病毒（Worm.vhy）采用（B）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。

A、网上邻居 B、我的电脑

C、我的文档 D、收藏夹

531、“冲击波”病毒运行时会将自身复制到Windows目录下，并命名为（C）

A、Gsrss.exe B、msbast.exe

C、msblast.exe D、lsass.exe

532、Code Red 爆发于2001年7月，利用微软的IIS漏洞在Web服务器之间传播。针对这一漏洞，微软早在2001年三月就发布了相关的补丁。如果今天服务器仍然感染Code Red，那么属于哪个阶段的问题？（A）

A、系统管理员维护阶段的失误 B、微软公司软件的设计阶段的失误

C、最终用户使用阶段的失误 D、微软公司软件的实现阶段的失误

533、病毒的传播机制主要有哪些？（D）

A、移动存储 B、电子邮件 C、网络共享 D、以上均是

534、病毒的反静态反汇编技术都有（D）。

A、数据压缩 B、数据加密 C、感染代码 D、以上均是

535、病毒在感染计算机系统时，一般（B）感染系统的。

A、病毒程序都会在屏幕上提示，待操作者确认（允许）后

B、实在操作者不觉察的情况下

C、病毒程序会要求操作者制定存储的磁盘和文件夹后

D、在操作者为病毒制定存储的文件名以后

536、杀毒软件时提示“重新启动计算机后删除文件”其主要原因是（A）

A、文件插入了系统关键进程，杀毒时无法处理

B、文件是病毒文件，无法处理

C、由于病毒的加壳形式不同，杀毒时无法正确处理

D、文件正在运行且无法安全的结束，需要其他处理方法

537、蠕虫的目标选择算法有（D）。

A、随机性扫描 B、基于目标列表的扫描

C、顺序扫描 D、以上均是

538、网络钓鱼是指（A）

A、通过大量发送声来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息。

B、网上进行钓鱼活动

C、通过网络组织钓鱼活动，从而获得利益 D、以上都不是

539、不属于常见把入侵主机的信息发送给攻击者的方法是（D）。

A、E-MAIL B、UDP C、ICMP D、连接入侵主机

540、不属于黑客被动攻击的是（A）

A、缓冲区溢出 B、运行恶意软件 C、浏览恶意代码网页 D、打开病毒附件

541、不属于黑客前期收集信息的工具是（D）

A、Nmap B、Xscan C、Nslookup D、LC

542、常见Web攻击方法，不包括？（D）

A、利用服务器配置漏洞 B、恶意代码上传下载

C、构造恶意输入（SQL注入攻击、命令注入攻击、跨站脚本攻击）

D、业务测试

543、常用的抓包软件有（A）。

A、ethereal B、MS office C、fluxay D、netscan

544.网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（A）

A、密码加密后，不会被窃听 B、Cookie字段可以被窃听

C、报文和帧可以窃听 D、高级窃听者还可以进行ARPSpoof，中间人攻击

545、除了在代码设计开发阶段预防SQL注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（C）

A、禁止将任何高权限账号（例如sa,dba等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户

B、拒绝用户访问敏感的系统存储过程

C、禁止用户访问的数据库表 D、限制用户所能够访问的数据库表

546、防止用户被冒名所欺骗的方法是（A）。

A、对信息源发放进行身份验证 B、进行数据加密

C、对访问网络的流量进行过滤和保护 D、采用防火墙

547、给电脑设置多道口令，其中进入电脑的第一道口令是（B）。

A、系统口令 B、CMOS口令

C、文件夹口令 D、文档密码

548、攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息重新发往B称为（D）。

A、中间人攻击 B、口令猜测器和字典攻击

C、强力攻击 D、回放攻击

549、故意制作、传播计算机病毒，造成计算机信息系统不能正常运行，但如果后果不严重就无罪，可以原谅，这种说法（C）。

A、不对，对这种蓄意破坏行为不能原谅 B、即使不是故意的，后果也不很严重

C、对。我国实行成文法，根据《中华人民共和国刑法》第286条的规定，只有造成严重后果者才有罪

D、无法断定

550、关于80年代Mirros蠕虫危害的描述，哪句话是错误的？（B）

A、占用了大量的计算机处理器的时间，导致拒绝股务

B、窃取用户的机密信息，破坏计算机数据文件

C、该蠕虫利用Unix系统上的漏洞传播

D、大量的流量堵塞了网络，导致网络瘫痪

551、关于黑客注入攻击说法错误的是： (D)

A、它的主要原因是程序对用户的输入缺乏过滤

B、一般情况下防火墙对它无法防范

C、对它进行防范时要关注操作系统的版本和安全补丁

D、注入成功后可以获取部分权限

552、基于主机评估报告对主机进行加固时，第一步是（B）。

A、账号、口令策略修改 B、补丁安装

C、文件系统加固 D、日志审核增强

553、计算机病毒会对下列计算机服务造成威胁，除了（C）。

A、完整性 B、有效性

C、保密性 D、可用性

554、计算机病毒是一段可运行的程序，它一般（C）保存在磁盘中。

A、作为一个文件 B、作为一段数据

C、不作为单独文件 D、作为一段资料

555、什么方式能够从远程绕过防火墙去入侵一个网络？(D)

A、IP services\_ B、Active ports

C、Identified network topology D、Modem banks

556、输入法漏洞通过（D）端口实现的。

A、21 B、23 C、445 D、3389

557、特洛伊木马攻击的威胁类型属于（B）。

A、授权侵犯威胁 B、植入威胁

C、渗入威胁 D、旁路控制威胁

558、通常黑客扫描目标机的445端口是为了(B)。

A、利用NETBIOS SMB服务发起DOS攻击

B、发现并获得目标机上的文件及打印机共享

C、利用SMB服务确认Windows系统版本

D、利用NETBIOS服务确认Windows系统版本

559、网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？(A)

A、残余风险评估阶段 B、检查阶段

C、入侵检测系统监控阶段 D、网络异常流量临控阶段

560、网络病毒预防范阶段的主要措施是什么？(A)

A、强制补丁、网络异常流量的发现 B、强制补丁、入侵检测系统监控

C、网络异常流量的发现、入侵检测系统的监控阶段 D、缺少D选项

561、下列除了(B)以外，都是防范计算机病毒侵害的有效方法。

A、使用防病毒软件 B、机房保持卫生，经常进行消毒

C、避免外来的磁盘接触系统 D、网络使用防病毒网关设备

562、下列除了(A)以外，都是计算机病毒传

A、通过操作员接触传播 B、通过U盘接触传播

C、通过网络传播 D、通过电子播的途径邮件传播

563、下列措施中，(C)不是减少病毒的传染

和造成的损失的好办法。

A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B、外来的文件要经过病毒检测才能使用，不要使用盗版软件

C、不与外界进行任何交流，所有软件都自行开发

D、定期用抗病毒软件对系统进行查毒、杀毒

564、下列哪项是跨站脚本Cross Site Scripting攻击具体事例？（B）

A、搜索用户 B、发帖子，发消息 C、上传附件 D、下载文件

565、下列哪项为信息泄露与错误处理不当Information Leakage and Improper

Error Handlina攻击具体实例？(D)

A、不明邮件中隐藏的html链接 B、发帖子，发消息

C、上传附件 D、错误信息揭示路径

566、下面哪一项是黑客用来实施DDoS攻击的工具？(D)

A、LC5 B、Rootkit C、Icesword D、Trinoo

567、以下哪个工具可以抹去所有NT/2K配置，并将其还原到初始状态？(A)

A、Rollback. exe B、Recover. exe C、Zap. exe D、Reset. exe

568、以下哪个工具通常是系统自带任务管理器的替代？(D)

A、Regmon B、Filemon C、Autoruns D、Process explorer

569、以下哪个针对访问控制的安全措施是最容易使用和管理的？(C)

A、密码 B、加密标志 C、硬件加密 D、加密数据文件

570、以下哪项不是分布式拒绝服务攻击常用的工具？(D)

A、Trinoo B、Trinoo C、TFN D、synkill

571、以下哪项不属于针对数据库的攻击？(D)

A、特权提升 B、强力破解弱口令或默认的用户名及口令

C、SQL注入 D、利用xss漏洞攻击

572、以下哪项工具不适合用来做网络监听？(B)

A、sniffer B、Webscan C、 Windump D、 D-Iris

573、以下哪项是SYN变种攻击经常用到的工具？(B)

A、sessionIE B、synkill C、TFN D、Webscan

574、以下哪一项不是流氓软件的特征？(D)

A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装

B、通常添加驱动保护使用户难以卸载

C、通常会启动无用的程序浪费计算机的资源

D、通常会显示下流的言论

575、一个数据仓库中发生了安全性破坏。以下哪一项有助于安全调查的进行？(B)

A、访问路径 B、时戳 C、数据定义 D、数据分类

576、以下哪一项不属于恶意代码？(C)

A、病毒 B、蠕虫 C、宏 D、特洛伊木马

577、以下哪一项不属于计算机病毒的防治策略？(D)

A、防毒能力 B、查毒能力 C、杀毒能力 D、禁毒能力

578、以下哪一项是常见Web站点脆弱性扫描工具？(A)

A、Appscan B、Nmap C、Sniffer D、LC

579、以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？(A)

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将臀陆信息写入记事本

580、以下哪种符号在SQL注入攻击中经常用到？(D)

A、$\_ B、1 C、@ D、;

581、以下哪种工具能从网络上检测出网络监听软件(A)

A、sniffdet, , B、purify, , C、Dsniff D、WireShark

582、以下哪种攻击可能导致某些系统在重组IP分片的过程中宕机或者重新启动？(B)

A、分布式拒绝服务攻击 B、Ping of Death

C、NFS攻击 D、DNS缓存毒化攻击

583、下面哪部分不属于入侵的过程？(B)

A、数据采集 B、数据存储 C、数据检测 D、数据分析

584、以下对木马阐述不正确的是(A)。

A、木马可以自我复制和传播

B、有些木马可以查看目标主机的屏幕

C、有些木马可以对目标主机上的文件进行任意揉作

D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。

585、由于攻击者可以借助某种手段，避开DBMS以及应用程序而直接进入系统访问

数据，我们通常采取以下哪种方式来防范？(A)

A、数据库加密

B、修改数据库用户的密码，将之改得更为复杂

C、使用修改查询法，使用户在查询数据库时需要满足更多的条件

D、使用集合法

586、在大多数情况下，病毒侵入计算机系统以后，(D)。

A、病毒程序将立即破坏整个计算机软件系统

B、计算机系统将立即不能执行我们的各项任务

C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

587、在确定威胁的可能性时，可以不考虑以下哪项？(D)

A、威胁源 B、潜在弱点

C、现有控制措施 D、攻击所产生的负面影响

588、在以下人为的恶意攻击行为中，属于主动攻击的是(A)。

A、身份假冒 B、数据GG C、数据流分析 D、非法访问

589、下面哪一种攻击方式最常用于破解口 令？(B)

A、哄骗( spoofing) B、字典攻击(dictionary attack)

C、拒绝服务(DoS) D、WinNuk

590、针对DNS服务器发起的查询DoS攻击，属于下列哪种攻击类型？(C)

A、syn flood B、ack flood C、 udpflood D、Connection flood

591、下列哪项不是安全编码中输入验证的控制项？(D)

A、数字型的输入必须是合法的数字

B、字符型的输入中对’进行特殊处理

C、验证所有的输入点，包括Get，Post，Cookie以及其他HTTP头

D、正确使用静态查询语句，如PreDaredStatement

592、以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？(C)

A、早期的SMTP协议没有发件人认证的功能

B、网络上存在大量开放式的邮件中转服务器，导致垃圾邮件的来源难于追查

C、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因

D、Internet分布式管理的性质，导致很难控制和管理

593、以下哪种方法是防止便携式计算机机密信息泄露的最有效方法？（A）

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将登录信息写入记事本

594、以下哪种攻击属于DDoS类攻击？（A）

A、SYN变种攻击 B、smurf攻击 C、arp攻击 D、Fraggle攻击

595、URL访问控制不当不包括（D）

A、Web应用对页面权限控制不严 B、缺乏统一规范的权限控制框架

C、部分页面可以直接从URL中访问 D、使用分散登录认证

596、Web应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（A）

A、静态密码 B、短信挑战 C、指纹认证 D、图片认证

597、Web应用漏洞按类别进行排名，由多到少正确的顺序为？（A）

A、跨站脚本、注入、恶意代码、引用不当

B、注入、跨站脚本、恶意代码、引用不当

C、恶意代码、跨站脚本、注入、引用不当

D、引用不当、跨站脚本、注入、恶意代码

598、从技术角度，以下不是漏洞来源的是（D）

A、软件或协议设计时候的瑕疵 B、软件或协议实现中的弱点

C、软件本身的瑕疵 D、显示卡内存容量过低

599、（C）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A、身份假冒 B、数据篡改 C、信息窃取 D、越权访问

600、有关密码学分支的定义，下列说法中错误的是（D）

A、密码学是研究信息系统安全保密的科学，由两个相互对立、相互斗争、而且又相辅相成、相互渗透的分支科学所组成的、分别称为密码编码学和密码分析学

B、密码编码学是对密码体制、密码体制的输入输出关系进行分析、以便推出机密变量、包括明文在内的敏感数据

C、密码分析学主要研究加密信息的破译或信息的伪造

D、密码编码学主要研究对信息进行编码，实现信息的隐藏

601、与RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（C）

A、数字签名 B、鉴别机制 C、加密机制 D、数据完整性

602、以下哪项是数据库加密方法中的库外加密的缺点？（A）

A、即使访问一条数据也要对整个数据库解密 B、密钥管理比较复杂

C、加密之后不能完整的查询数据 D、密钥过于简单，容易被破解

603、以下哪项数据中涉及安全保密的最主要问题？（A）

A、访问控制问题 B、数据完整性 C、数据正确性 D、数据安全性

604、以下哪一个最好的描述了数字证书？（A）

A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，它使得黑客不能得知用户的身份

C、网站要求用户使用用户名和密码登陆的安全机制

D、伴随在线交易证明购买的收据

605、TCP SYN Flood网络攻击时利用了TCP建立连接过程需要（C）次握手的特点而完成对目标进行攻击的。

A、1 B、2 C、3 D、6

二、多项选择题（606-789）

606、COBIT度量过程的三个纬度分别是（ABC）。

A、能力 B、绩效 C、控制度 D、能力成熟度

607、IT系统内网与互联网连接检查手段有哪些？（BCD）

A、工具扫描 B、人员访谈 C、人工检查 D、文档检查

608、公司应该采取以下措施，对第三方访问进行控制。（ABCD）

A、公司应于第三发公司法人签署保密协议，并要求其第三方个人签署保密承诺，此项工作应在第三方获得网络与信息资产的访问权限之前完成

B、实行访问授权管理，未经授权，第三方不得进行任何形式的访问

C、公司应加强第三方访问的过程控制，监督其活动及操作，对其进行适当的安全宣传与培训

D、第三方人员应佩戴易于识别的标志，并在访问公司重要场所时有专人陪同

609、计算机信息系统安全的三个相辅相成，互补互通的有机组成部分是（ABD）

A、安全策略 B、安全法规 C、安全技术 D、安全管理

610、劳动合同中应包含网络与信息安全条款，这些条款规定（ACD）。

A、员工的安全责任和违约罚则

B、安全责任不可延伸至公司场所以外和正常工作时间以外

C、安全责任可延伸至公司场所以外和正常工作时间以外

D、如必要，一些安全责任应在雇佣结束后延续一段特定的时间

611、审核是网络安全工作的核心，下列应用属于主动审核的是：（CD）

A、Windows事件日志记录 B、数据库的事务日志记录

C、防火墙对访问站点的过滤 D、系统对非法链接的拒绝

612、通用准则CC实现的目标有（ABC）

A、成为统一的国际通用安全产品、系统的安全标准

B、在不同国家达成协议，相互承认产品安全等级评估

C、概述IT产品的国际通用性 D、都不是

613、系统用户账号登记表应包括（ABCD）。

A、使用者姓名、部门、职务、联系电话 B、账号权限

C、批准人、开通人 D、开通时间、到期日

614、下列情况哪些是对公司经营管理的影响为“一般”级别的互联网网络安全事件？（ABD）

A、发生未到达“预警”的一般性安全事件

B、出现新的漏洞，尚未发现利用方法或利用迹象

C、有来自境外的网络性能明显下降的报警，并且其技术原因普遍适用于我国互联网 D、出现新的蠕虫/病毒或其它恶意代码，尚未证明可能造成严重危害

615、信息安全的主要原则有（BCD）

A、认证性 B、保密性 C、可用性 D、完整性

**616、针对支撑系统，除业务关联性、对业务网络的影响，资产价值主要体现在（ACD）几个方面。 缺少D选项**

**A、业务收益的影响 B、设备购买成本 C、面向客户的重要程度 D、**

617、IT系统病毒泛滥的主要原因有哪些？（ABCD）

A、主机和终端防病毒软件缺乏统一管理

B、主机和终端防病毒软件没有设置为自动更新或更新周期较长

C、防病毒服务器没有及时更新放病毒库

D、缺乏防病毒应急处理流程和方案

618、IT系统病毒防护评估检查对象包括哪些内容？（ABCD）

A、防病毒服务器 B、重要应用Windows主机

C、Windows终端 D、主机管理员

619、互联网连接防火墙设备的安全策略配置要求包括哪几点（ABCD）。

A、远程登录是否禁止telnet方式 B、最后一条策略是否是拒绝一切流量

C、是否存在允许any to any的策略

D、是否设置了管理IP，设备只能从管理IP登录维护

620、《安全基线标准》在安全管理层面主要围绕哪几部分考评安全基线？（ABC）

A、组织架构管理 B、人员安全管理 C、运维安全管理 D、制度安全管理

621、IT系统维护人员权限原则包括（ACD）。

A、工作相关 B、最大授权 C、最小授权 D、权限制约

622、安全系统加固手册中关于造成系统异常中断的各方面因素，主要包括哪三方面（ABD）

A、人为原因 B、环境原因 C、生产原因 D、设备原因

623、IT系统维护人员权限原则包括（ACD）

A、工作相关 B、最大授权 C、最小授权 D、权限制约

624、计算当前Linux系统中所有用户的数量，可以使用（ABC）命令

A、wc -l /etc/passwd B、wc -l</etc/passwd

C、cat/etc/passwd|wc -l D、cat/etc/passwd>wc -l

625、Solarid系统中，攻击者在系统中增加账户会改变哪些文件？（AB）

A、shadow B、passwd C、inetd,conf D、hosts

626、Syn Flood攻击的现象有以下哪些？（ABC）

A、大量连接处于SYN\_RCVD状态 B、正常网络访问受阻

C、系统资源使用率高

627、UNIX安全审计的主要技术手段有哪些？（ABCDEF）

A、文件完整性审计 B、用户、弱口令审计 C、安全补丁审计

D、端口审计 E、进程审计 F、系统日志审计

628、Unix系统提供备份工具有（ABCD）

A、cp：可以完成把某一目录内容拷贝到另一目录

B、tar：可以创建、把文件添加到或从一个tar档案中解开文件

C、cpio：把文件拷贝进或拷贝出一个cpio档案或tar档案

D、dump：用来恢复整个文件系统或提取单个文件

629、操作系统应利用安全工具提供以下哪些访问控制功能？（ABC）

A、验证用户身份，必要的话，还应进行终端或物理地点识别

B、记录所有系统访问日志

C、必要时，应能限制用户连接时间 D、都不对

630、从哪些地方可以看到遗留痕迹？（ABCD）

A、回收站 B、最近使用过的文件 C、注册表 D、文件最后更改的时间戳631、

632、关于Windows活动目录说法正确的是（ABD）。

A、活动目录是采用分层结构来存储网络对象信息的一种网络管理体系

B、活动目录可以提供存储目录数据和网络用户级管理员使用这些数据的方法

C、利用活动目录来实现域内计算机的分布式管理

D、活动目录与域紧密结合构成与目录林和域目录树，使大型网络中庞大、复杂的网络管理、控制、访问变得简单，使网络管理效率更高

633、建立堡垒主机的一般原则是（AC）。

A、最简化原则 B、复杂化原则 C、预防原则 D、网络隔离原则

634、逻辑空间主要包括哪些部分？（ABDE）

A、TABLESPACES B、SEGMENTS C、DATAFILE

D、EXTENTS E、BLOCK

635、哪些属于Windows日志？（ABCD）

A、AppEvent.Evt B、SecEvent.Evt C、SysEvent.Evt D、W3C扩展日志

636、如何设置listener口令？（ACDE）

A、以Oracle用户运行lsnrctl命令 B、set log\_file

C、change\_password D、set password E、save\_config

637、审计启动其日志有哪两种存放方式？（BD）

A、NONE B、OS C、TRUE D、SYS.AUD$

638、生产服务器通常都是UNIX平台，资产价值最高，不直接连接外部网络，主要的安全需求是（ABD）

A、访问控制 B、账号口令 C、数据过滤 D、权限管理和补丁管理

639、使用md5sum工具对文件签名，以下说法正确的是？（ADE）

A、md5sum对任何签名结果是定长的16字节

B、md5sum对文件签名具有不可抵赖性

C、md5sum是对文件进行加密运算得出签名，不同文件结果几乎不相同

D、md5sum是对文件进行哈希运算得出签名，不同文件结果几乎不相同

E、md5sum对文件签名时，与文件的日期和时间无关

640、为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有（ABCD）

A、口令/账号加密 B、定期更换口令

C、限制对口令文件的访问 D、设置复杂的、具有一定位数的口令

641、文件系统是构成Linux基础，Linux中常用文件系统有（ABD）？

A、ext3 B、ext2 C、hfs D、reiserfs

642、下列关于UNIX下日志说法正确的是（AC）

A、wtmp记录每一次用户登录和注销的历史信息

B、acct记录每个用户使用过的命令

C、sulog记录su命令的使用情况

D、acct记录当前登录的每个用户

643、下列哪些操作可以看到自启动项目？（ABD）

A、注册表 B、开始菜单 C、任务管理器 D、msconfig

644、下列哪些命令行可用于查看当前进程？（ABC）

A、Ps -ef B、Strings -f/proc/[0-9]\*/cmdline

C、Ls -al /proc/[0-9]\*/exe D、Cat/etc/inetd.conf

645、下面操作系统中，哪些是UNIX操作系统？（CD）

A、Red-hat Linux B、Novell Netware C、Free BSD D、SCO Unix

646、严格的口令策略应当包含哪些要素（ABC）

A、满足一定的长度，比如8位以上 B、同时包含数字，字母和特殊字符

C、系统强制要求定期更改口令 D、用户可以设置空口令

647、在Solaris 8 下，使用ps -ef命令列出进程中有一行如下“root 1331 0 00:01:00? 0:00 /usr/sbin/inetd -s -t”，以下说法正确的是（ABE）

A、参数-t是trace，记录包括IP和PORT等信息

B、参数-t对于UDP服务无效 C、进程启动的时间不能确定

D、进程已经运行了1分钟 E、进程的父进程号是1

648、在Solaris 8 下，以下说法正确的是：（AB）

A、/etc/rc2.d里S开头的文件在系统缺省安装的缺省级别会自动运行

B、/etc/rc3.d里S开头的文件在系统缺省安装的缺省级别会自动运行

C、/etc/init.d里的文件在系统启动任何级别时会自动运行

D、init 0是进入单用户级别 E、init 6命令会运行所有级别的rc目录下以S开头的文件

649、在Solaris 8 下，以下说法正确的是：（BC）

A、PATH环境变量最后带有“.”，会使当前目录的命令比其他目录的命令有限执行

B、可以修改/etc/inittab里ttymon的参数，使得登录的SHELL在无输入时自动退出

C、在使用/bin/ksh时，可以设置TMOUT值，使得登录的SHELL在无输入时自动退出

D、在/etc/login中，可以设置TIMEOUT值，使得登录的SHELL在无输入时自动退出

E、tar xvf命令的意思是以tar格式解开输入，并且保持文件属性等参数不变

650、在配置Apache访问控制时，Allow和Deny指令可以允许或拒绝来自特定主机名或主机名地址的访问。那么下列哪些配置是不正确的？（AD）

A、Order allow,deny Allow from 192.101.205

B、B、Order deny,allow Deny from all Allow from example

C、C、Order deny,allow Deny from 192.101.205

D、D、Order allow,deny Deny from 192.101.205 Allow from all

651、造成操作系统安全漏洞的原因是（ABC）。

A、不安全的编程语言 B、不安全的编程习惯

C、考虑不周的架构设计 D、人为的恶意破坏

652、针对Linux主机，一般的加固手段包括（ABC）。

A、打补丁 B、关闭不必要的服务 C、限制访问主机 D、切断网络

653、做系统快照，查看端口信息的方式有（AD）。

A、netstat -an B、net share C、net use D、用taskinfo来查看连接情况

654、网厅安全解决方案主要从哪几个方面对网厅安全进行建议和指导？（ABCD）

A、安全管理 B、安全防护 C、安全运维 D、灾备/恢复

655、IT系统软件设计中应当考虑并执行安全审计功能，详细记录访问信息的活动，包括（ABCD）。

A、记录的活动以是否有数据的修改、应用程序的异常关闭、异常删除触发

B、应用系统应当配置单独的审计数据库，审计记录应单独存放，并设置严格的边界访问控制，只有安全管理人员才能够看到审计记录

C、信息系统的审计功能包括：事件日期、时间、发起者信息、类型、描述和结果

D、应用系统的审计进程为后台处理，与应用系统运行同步进行，并且对于审计进程应当涉及相应的守护进程，一旦出现异常停止系统可重新启动审计进程，从而保障审计的“完整性”

656、IPSec的配置步骤包括：（ABCD）

A、防火墙基本配置 B、定义保护数据流和域间规则

C、配置IPSec安全提议 D、配置IKEPeer

657、Juniper路由器在配置SSH访问时应注意如下（ABCD）细节。

A、建立允许访问的SSH-ADDRESSES过滤器

B、确保只允许来自内部接口的授权用户访问

C、针对SSH进行限速以保护路由引擎

D、过滤器应用在loopback接口

658、对于使用RPF反向地址验证，以下说法错误的是：（BCD）。

A、对称路由可以使用 B、非对称路由可以使用

C、有些情况不可以使用，但与对称或非对称路由无关

D、在任何情况下都可以使用

659、防病毒服务升级检查包括如下几项内容？（ABC）

A、检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决

B、在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本

C、对重要的服务器，定期抽查防病毒客户端的病毒库升级情况

660、防范DOS攻击的方法主要有（ABCD）。

A、安装Dos检测系统 B、对黑洞路由表里的地址进行过滤

C、及时打好补丁 D、正确配置TCP/IP参数

661、防火墙trust域中的客户机通过nat访问untrust中的服务器的ftp服务，已经允许客户机访问服务器的tcp21端口，但只能登陆到服务器，却无法下载文件，以下解决办法中可能的是：（ABC）

A、修改trust untrust域间双向的默认访问策略为允许

B、FTP工作方式为port模式时，修改untrust trust域间in方向的默认访问策略为允许 C、在trust untrust域间配置中启用detect ftp

D、FTP工作方式为passive模式时，修改untrust trust域间in方向的默认访问策略为允许

662、防火墙不能防止以下哪些攻击？（ABD）

A、内部网络用户的攻击 B、传送已感染病毒的软件和文件

C、外部网络用户的IP地址欺骗 D、数据驱动型的攻击

663、防火墙常见的集中工作模式有（ABC）。

A、路由 B、NAT C、透明 D、旁路

664、防火墙的缺陷主要有（ABCD）。

A、限制有用的网络服务 B、无法防护内部网络用户的攻击

C、不能防备新的网络安全问题 D、不能完全防止传送已感染病毒的软件或文件

665、防火墙的日志管理应遵循如下原则：（BC）

A、本地保存日志 B、本地保存日志并把日志保存到日志服务器上

C、保持时钟的同步 D、在日志服务器保存日志

666、防火墙的特征是（ABCD）。

A、保护脆弱和有缺陷的网络服务 B、加强对网络系统的访问控制

C、加强隐私，隐藏内部网络结构 D、对网络存取和访问进行监控审计

667、防火墙的主要功能有哪些？（ABCD）

A、过滤进、出网络的数据 B、管理进、出网络的访问行为

C、封堵某些禁止的业务，对网络攻击进行检测和报警

D、记录通过防火墙的信息内容和活动

668、防火墙的作用主要有（ABCD）。

A、实现一个公司的安全策略 B、创建一个阻塞点

C、记录Internet活动 D、限制网络暴露

669、防火墙技术，涉及到（ABCD）。

A、计算机网络技术 B、密码技术 C、软件技术 D、安全操作系统

670、防火墙可以部署在下列位置：（ABCD）。

A、安全域边界 B、服务器区域边界

C、可信网络区域和不可信网络区域之间 D、根据网络特点设计方案

671、防火墙配置时应确保（ABCD）服务不开放。

A、Rlogin B、NNTP C、Finger D、NFS

672、启用Cisco设备的访问控制列表，可以起到如下作用（ABC）。

A、过滤恶意和垃圾路由信息 B、控制网络的垃圾信息流

C、控制未授权的远程访问 D、防止DDoS攻击

673、如果Cisco设备的VTY需要远程访问，则需要配置（ABCD）。

A、至少8位含数字、大小写、特写字符的密码 B、远程连接的并发数目

C、访问控制列表 D、超市退出

674、如果需要配置Cisco路由器禁止从网络启动和自动从网络下载初始配置文件，配置命令包括（AB）。

A、no boot network B、no service config C、no boot config D、no service network

675、入侵检测的内容主要包括：（BC）。

A、独占资源、恶意使用 B、试图闯入或成功闯入、冒充其他用户

C、安全审计 D、违反安全策略、合法用户的泄露

676、入侵检测系统包括以下哪些类型？（AC）

A、主机入侵检测系统 B、链路状态入侵检测系统

C、网络入侵检测系统 D、数据包过滤入侵检测系统

677、随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器（sniffer）来监听整个子网的办法不再可行。可选择解决的办法有（ABCD）。

A、使用交换机的核心芯片上的一个调试的端口

B、把入侵检测系统放在交换机内部或防火墙等数据流的关键入口

C、采用分解器（tap）

D、使用以透明网桥模式接入的入侵检测系统

678、通常要求把路由器的日志存储在专用日志服务器上，假设把Cisco路由器日志存储在192.168.0.100的syslog服务器上，需要在路由器侧配置的操作时：（ABCD）。

A、使用Router(config)# logging on启用日志：使用Router(config)# logging trap information将记录日志级别设定为“information”

B、使用Routee(config)# logging192.168.0.100将记录日志类型设定为“local6”

C、使用(config)# logging facility local6将日志发送到192.168.0.100

D、使用(config)# logging sourceinterface loopback0设定日志发送源loopback0

679、通过SSL VPN接入企业内部的应用，其优势体现在哪些方面：（ABCD）。

A、应用代理 B、穿越NAT和防火墙设备

C、完善的资源访问控制 D、抵御外部攻击

680、网络地址端口转换（NAPT）与普通地址转换有什么区别？（AD）

A、经过NAPT转换后，对于外网用户，所有报文都来自于同一个IP地址

B、NAT只支持应用层的协议地址转换

C、NAPT只支持网络层的协议地址转换

D、NAT支持网络层的协议地址转换

681、网络攻击的类型包括以下哪几种？（ABCD）

A、窃取口令 B、系统漏洞和后门 C、协议缺陷 D、拒绝服务

682、网络面临的典型威胁包括（ABCD）。

A、未经授权的访问 B、信息在传送过程中被截获、篡改

C、黑客攻击 D、滥用和误用

683、网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，该类病毒程序大规模爆发后，会对相关网络造成拒绝服务攻击，为了防止受到网络蠕虫的侵害，应当注意对（ACD）及时进行升级更新。

A、计算机操作系统 B、计算机硬件 C、文字处理软件 D、应用软件

684、下列关于NAT地址转换的说法中哪些事正确的：（ABCD）。

A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

B、地址转换可以按照用户的需要，在局域网内向外提供FTP、WWW、Telnet等服务

C、有些应用层协议在数据中携带IP地址信息，对它们作NAT时还要修改上层数据中的IP地址信息

D、对于某些非TCP、UDP的协议（如ICMP、PPTP），作上层NAT时，会对它们的特征参数（如ICMP的id参数）进行转换。

685、下列哪两项正确描述了由WPA定义的无线安全标准？（BC）

A、使用公开密钥的认证方法 B、当客户端连接的时候都要进行动态密钥交换

C、包含PSK认证 D、定制了一个经常更换的静态的加密密钥来增强安全性

686、下列配置中，可以增强无线AP（access point）安全性的有（ABCD）。

A、禁止SSID广播 B、禁用DHCP服务

C、采用WPA2-PSK加密认证 D、启用MAC地址接入过滤

687、下面可以攻击状态检测的防火墙方法有：（ABD）

A、协议隧道攻击 B、利用FTP-pasv绕过防火墙认证的攻击

C、ip欺骗攻击 D、反弹木马攻击

688、下面什么路由协议不可以为HSRP的扩充：（ABC）

A、SNMP B、CDP C、HTTP D、VRRP

689、下面什么协议有MD5认证：（ABC）

A、BGP B、OSPF C、EIGER D、RIPversion 1

690、下面是网络安全技术的有：（ABC）

A、防火墙 B、防病毒 C、PKI D、UPS

691、选购一个防火墙时应该考虑的因素有：（ABCD）

A、网络受威胁的程度 B、可能受到的潜在损失

C、站点是否有经验丰富的管理员 D、未来扩展的需要

692、一台路由器的安全快照需要保存如下哪些信息？（AB）

A、当前的配置--running-config B、当前的开放端口列表

C、当前的路由表 D、当前的CPU状态

693、以下对于包过滤防火墙的描述正确的有（ACD）。

A、难以防范黑客攻击 B、处理速度非常慢

C、不支持应用层协议 D、不能处理新的安全威胁

694、以下对于代理防火墙的描述正确的有（ABCD）。

A、能够理解应用层上的协议 B、时延较高，吞吐量低

C、能做复杂一些的访问控制，并做精细的认证和审核 D、可伸缩性较差

695、以下关于L2TP VPN配置注意事项的说法中正确的有：（ABC）

A、L2TP的LNS端必须配置虚拟接口模板（Virtual-Template）的IP地址，该虚拟接口模板需要加入域

B、防火墙缺省需要进行隧道的认证。如果不配置认证，需要undo tunnel authentication命令

C、为了使L2TP拨号上来的用户分配的地址不能喝内网用户的地址在同一个网段

D、LNS端不允许配置多个L2TP-Group

1. 以下哪几项关于安全审计和安全审计系统的描述是正确的？（CD）

A、对入侵和攻击行为只能起到威慑作用

B、安全审计不能有助于提高系统的抗抵赖性

C、安全审计是对系统记录和活动的独立审查和检验

D、安全审计系统可提供侦破辅助和取证功能

697、以下哪些属于网络欺骗方式？（ABCD）

A、IP欺骗 B、ARP欺骗 C、DNS欺骗 D、Web欺骗

698、以下哪些是防火墙规范管理需要的？（ABCD）

A、需要配置两个防火墙管理员 B、物理访问防火墙必须严密地控制

C、系统软件、配置数据文件在更改后必须进行备份

D、通过厂商指导发布的硬件和软件的bug和防火墙软件升级版

699、以下硬件安装维护重要安全提示正确的有：（ABCD）

A、不要在雷雨天气进行故障处理 B、保持故障处理区域的干净、干燥

C、上防静电手套或防静电腕带再执行安装和更换操作

D、在使用和操作设备时，需要按照正确的操作流程来操作

700、以下属于DTE(Data Terminal Equipment)数据终端设备的有（AB）

A、路由器 B、PC C、交换机 D、HUB

701、在防火墙的“访问控制”应用中，内网、外网、DMZ三者的访问关系为：（ABD）

A、内网可以访问外网 B、内网可以访问DMZ区

C、DMZ区可以访问内网 D、外网可以访问DMZ区

702、关于GRE校验和验证技术，当本端配置了校验和而对端没有配置校验和时，以下叙述正确的有（BC）。

A、本端对接收报文检查校验和 B、对端对接收报文检查校验和

C、本端对发送报文计算校验和 D、对端对发送报文计算校验和

703、配置PPP链路层协议时，链路层协议状态始终不能转为Up状态的处理建议：（ABCD）

A、PPP链路两端的接口上配置的参数和验证方式都必须一致，LCP检查才能成功

B、如果LCP协商失败，请检查LCP配置协商参数

C、请检查验证方式配置是否正确。因为LCP协商中，包含验证方式的协商。因为LCP协商中，包含验证方式的协商。验证方式协商失败也会导致LCP协商失败

D、接口试图下先执行shutdown命令将接口关闭，再执行undo shutdown命令重启接口

704、对DNSSEC的描述正确的有（AC）。

A、为DNS数据提供来源验证，即保证数据来自正确的名称服务器

B、DNSSEC可防御DNS Query Flood攻击

C、为域名数据提供完整性验证，即保证数据在传输的过程中没有被篡改

D、实施DNSSEC后，只需升级软件系统，对网络、服务器等硬件设备不需考虑

705、MySQL安装程序会给出三种选择，用户可以根据自身的需要选择一种适合的安装方式，以下哪些是正确的？（ABD）

A、Typical（典型安装） B、Compact(最小安装)

C、Full(全部安装) D、Custom(选择安装)

706、MySQL中用DROP语句可删除数据库和数据表，以下哪句是正确的语法？（ABCD）

A、DROP TABLE table\_name1 B、DROP TABLE table\_name1,table\_name2

C、DROP TABLE IF EXISTS table\_name1 D、DROP DATABASE DB name1

707、Oracle 7.2之前的数据库连接用户名和密码在网络传输时是不进行加密的，为了要和旧版本兼容Oracle数据库9.02存在DBLINK\_ENCRYPT\_LOGIN参数用来调节数据库连接时用户名和密码的加密特性，以下说法正确的是：（ACD）。

A、DBLINK\_ENCRYPT\_LOGIN为TRUE时，数据库连接加密用户名和密码

B、DBLINK\_ENCRYPT\_LOGIN时，数据库连接不加密用户名和密码

C、DBLINK\_ENCRYPT\_LOGIN为FALSE时，如果加密的数据库连接失败，会尝试不加密的连接

D、DBLINK\_ENCRYPT\_LOGIN为TRUE时，加密的数据库连接失败，也不会尝试不加密的连接

708、Oracle实例主要由哪两部分组成：（AC）

A、内存 B、Share pool buffer C、后台进程 D、pmon和smon

709、Oracle中如何设置audit trail审计，正确的说法是：（ABD）

A、在init.ora文件中设置“audit\_trail = true”或者“audit\_trail = db”

B、以SYSDBA身份使用AUDIT ALL ON SYS.AUD$ BY ACCESS，语句对audit trail审计

C、Oracle不支持对audit trail的审计

D、在设置audit trail审计前，要保证已经打开Oracle的审计机制

710、SQL Server的登录认证种类有以下哪些？（ACD）

A、Windows认证模式 B、双因子认证模式

C、混合认证模式 D、SQL Server认证

711、SQL Server的取消权限的操作有以下哪些？（ABC）

A、在“详细信息”窗格中右击要授予/拒绝/取消其权限的用户定义的角色

B、单击“属性”命令在“名称”下单击“权限”单击列出全部对象

C、选择在每个对象上授予拒绝或废除的权限，选中标志表示授予权限，X表示拒绝权限，空框表示废除权限，只列出适用于该对象的权限

D、回到“数据库用户属性”对话框中，再点击“确定”按钮，所有的设置就完成了

712、SQL Server中ALTER DATABASE可以提供以下哪些功能选项？（ABCD）

A、更改数据库名称 B、文件组名称 C、数据文件 D、日志文件的逻辑名称

713、SQL Server中关于实例的描述，请选择正确的答案。（ABD）

A、如果安装选择“默认”的实例名称。这时本SQL Server的名称将和Windows 2000服务器的名称相同

B、SQL Server可以在同一台服务器上安装多个实例

C、SQL Server只能在一台服务器上安装一个实例

D、实例各有一套不为其他实例共享的系统及用户数据库，所以各实例的运行是独立的。

714、SQL Server中使用企业管理器从数据库中删除数据或日志文件的步骤如下，正确的步骤是？（ABCD）

A、展开服务器组，然后展开服务器

B、展开“数据库”文件夹，右击要从中删除数据或日志文件的数据库，然后单击“属性”命令

C、若要删除数据文件，单击“常规”选项卡。若要删除日志文件，单击“事务日志”选项卡

D、在“文件名”列户，单击要删除的文件名旁边的箭头，再点DELETE键，文件名旁出现十字光标，表明将删除此文件

715、参数REMOTE\_LOGIN\_PASSWORDFILE在Oracle数据库实例的初始化参数文件中，此参数控制着密码文件的使用及其状态，以下说法正确的是：（ABCD）

A、NONE：只是Oracle系统不使用密码文件，不允许远程管理数据库

B、EXCLUSIVE：指示只有一个数据库实例可以使用密码文件

C、SHARED：指示可有多个数据库实例可以使用密码文件

D、以上说法都正确

716、关于SQL Server 2000中的SQL账号、角色，下面说法正确的是：（ABC）

A、PUBLIC,guest为缺省的账号 B、guest不能从master数据库清除

C、可以通过删除guest账号的角色，从而消弱guest可能带来的安全隐患

D、SQL Server角色的权限是不可以修改的

717、连接MySQL后选择需要的数据库DB\_NAME？以下哪些方法是对的（AC）

A、连接后用USE DB\_NAME选择数据库

B、连接后用SET DB\_NAME选择数据库

C、用mysql -h host -u user -p DB\_NAME连接数据库

D、用mysql -h host -u user -p -T DB\_NAME连接数据库

718、如果数据库不需要远程访问，可以禁止远程tcp/ip连接，以增强安全性。可选择的有效方法：（AC）

A、用防火墙封堵数据库侦听端口避免远程连接 B、禁止tcp/ip协议的使用

C、在mysqld服务器中参数中添加 --skip-networking启动参数来使mysql

D、在/etc/my.cnf下添加remoteConnnect=disable

719、以下哪些MySQL中GRANT语句的权限指定符？（ABCDEF）

A、ALTER B、CREATE C、DELETE

D、UPLOAD E、DROP F、INSERT

720、用THC组织的Oracle的工具，通过sniffer方式抓取数据库的认证信息可有效破解Oracle密码，以下哪些数据是必须获取的？（ABC）

A、AUTH\_SESSKEY B、AUTH\_PASSWORD C、用户名 D、实例名

721、在Oracle 9数据库可以通过配置$Oracle\_HOME\network\admin\sqlnet.ora文件实现数据库层次的基于TCP协议和地址的访问控制。下面说法正确的是：（ABCD）

A、首先需要配置TCP,VALIDNODE\_CHECKING=yes启用节点检查功能

B、其次配置TCP.INVITED\_NODES=192.168.0.12，192.168.0.33将会允许地址是192.168.0网段的12和33的主机访问

C、然后配置TCP.EXCLUDED\_NONES=192.168.0.123将会禁止地址是192.168.0网段的123的主机访问

D、要以上配置生效必须重启lsnrctl监听器

722、在SQL Server 2000中，如果想查询当前数据库服务器软件的版本，可以使用下面哪些方式（ABCD）

A、在查询分析器中通过如下语句查询SELECT ServerPROPERTY(‘productversion’),ServerPROPERTY(‘productlevel’),ServerPROPERTY(‘edition’)

B、在命令行下，用SQL Server自带的管理工具osql连接进入数据库，输入select@@version

C、企业管理器查看服务器属性 D、在SQL Server服务管理器里面查看“关于”

723、在SQL Server 2000中一些无用的存储过程，这些存储过程极容易被攻击者利用，攻击数据库系统。下面的存储过程哪些可以用来执行执行系统命令或修改注册表？（ABC）

A、xp\_cmdshell B、xp\_regwrite C、xp\_regdeletekey D、select \* from master

724、在SQL Server中创建数据库，如下哪些描述是正确的？（ABCD）

A、创建数据库的权限默认授权sysadmin和dbcreator固定服务器角色的成员，但是它仍可以授予其他用户

B、创建数据库的用户将成为该数据库的所有者

C、在一个服务器上，最多可以创建32,767个数据库

D、数据库名称必须遵循标示符规则

725、在对SQL Server 2000的相关文件、目录进行安全配置时，下面可以采用的措施是：（ABCD）

A、删除缺省安装时的例子样本库

B、将存放数据的库文件，配置权限为administrators组、system和启动SQL Server服务的用户账号及DBA组具有完全控制权限

C、对SQL Server安装目录，去除everyone的所有控制权限

D、将数据库数据相关的文件，保存在非系统盘的NTFS独立分区

726、sybase数据库文件系统需要哪些裸设备？（ABCD）

A、master B、proce C、data D、log

727、Oracle支持哪些加密方式？（ABCD）

A、DES B、RC4\_256 C、RC4\_40 D、DES40

728、SQL Server用事件探测器可以帮助排除故障和解决问题，创建跟踪的步骤如下哪些是正确的？（ABCD）

A、从“模板名称”下拉菜单为你创建跟踪选择一个模板

B、“事件探查器”主界面打开后，从“文件”菜单选择“新跟踪”

C、在“跟踪名称”文本框中输入你想要为这个跟踪创建的跟踪名称

D、修改这些默认的选项设置。通过点击“显示全部事件”和“显示全部列”复选框来查看其他的选项。

729、最重要的电磁场干扰源是：（BCD）

A、电源周波干扰 B、雷电电磁脉冲LEMP

C、电网操作过电压SEMP D、静电放电ESD

730、雷电侵入计算机信息系统的途径主要有：（ABD）

A、信息传输通道线侵入 B、电源馈线侵入 C、建筑物 D、地电位反击

731、电信生产其机房作业，是由专门的值机员、机务员来完成，作业内容是：固定电话、无线电话、电报、载波、短波、微波、卫星和电力等电信通信设备，使设备出去良好状态，保证其正常运行。（ABCD）

A、安装 B、值守 C、维护 D、检修

732、对计算机系统有影响的腐蚀性气体大体有如下几种：（ABCD）

A、二氧化硫 B、氢化硫 C、臭氧 D、一氧化碳

733、防火工作的基本措施有：（ABCD）

A、加强对人员的教育管理 B、加强对可燃物的管理

C、加强对物的管理 D、加强对火源、电源的管理

734、会导致电磁泄漏的有（ABCDE）

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

E、信号处理电

735、火灾自动报警、自动灭火系统部署应注意（ABCD）。

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、具有自动和手动两种触发装置

736、计算机场地安全测试包括（ABCD）。

A、温度，湿度，尘埃 B、照度，噪声，电磁场干扰环境场强

C、接地电阻，电压、频率 D、波形失真率，腐蚀性气体的分析方法

737、计算机信息系统设备处于不同雷电活动地区，其雷电电磁场强度有很大差异，根据这一差异，将被防护空间分为下列哪些防护区？（ABCD）

A、直击雷非防护区（LPZOA） B、直击雷防护区（LPZOB）

C、第一防护区（LPZI） D、后续防护区（LPZ2,3...等）

738、静电的危害有（ABCD）。

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

739、灭火的基本方法有（ABCD）。

A、冷却法 B、隔离法 C、窒息法 D、抑制

740、实体安全技术包括（ABD）。

A、环境安全 B、设备安全 C、人员安全 D、媒体安全

741、使用配有计算机的仪器设备时，不应该做的有：（ABCD）

A、更改登机密码和系统设置

B、自行安装软件

C、玩各种电脑游戏

D、将获得的图像、数据等资料存储在未予指定的硬盘分区上

742、硬件设备的使用管理包括（ABCD）。

A、严格按硬件设备的操作使用规程进行操作

B、建立设备使用情况日志，并登记使用过程

C、建立硬件设备故障情况登记表

D、坚持对设备进行例行维护和保养

743、预防静电的措施有（ABCD）。

A、接地 B、不使用或安装产生静电的设备

C、不在产生静电场所穿脱工作服 D、作业人员穿防静电鞋

744、在实验室中引起火灾的通常原因包括：（ABCD）

A、明火 B、电器保养不良

C、仪器设备在不使用时未关闭电源 D、使用易燃物品时粗心大意

745、直击雷：直接击在（ABCD）并产生电效应、热效应和机械力的雷电放电。

A、建筑物 B、构建物 C、地面突进物 D、大地或设备

746、员工区域安全守则包括：（ABCD）

A、非工作时间，员工进入或离开办公区域，应在值班人员处登记

B、外来人员进入办公区域或机房，相关员工必须全程陪同

C、将物品带入/带出公司，要遵守公司相关的规定及流程

D、参加会议时遵守会前、会中、会后的保密流程

747、机房出入控制措施包括：（ABCD）

A、机房接待前台须核查弄清业务系统安全区域的来访者的身份，并记录其进入和离开安全区域的日期与时间

B、机房须告知进入安全区的来访者，该区域的安全要求和紧急情况下的行动步骤

C、可采用强制性控制措施，对来访者的访问行为进行授权和验证

D、要求所有进出机房人员佩带易于辨识的标识

748、为了减小雷电损失，可以采取的措施有（ACD）

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

749、安全要求可以分解为（ABCDE）。

A、可控性 B、保密性 C、可用性 D、完整性 E、不可否认性

750、HASH加密使用复杂的数字算法来实现有效的加密，其算法包括（ABC）

A、MD2 B、MD4 C、MD5 D、Cost256

751、利用密码技术，可以实现网络安全所要求的。（ABCD）

A、数据保密性 B、数据完整性 C、数据可用性 D、身份验证

752、一个密码体系一般分为以下哪几个部分？（ABCD）

A、明文 B、加密密钥和解密密钥

C、密文 D、加密算法和解密算法

753、公钥密码体质的应用主要在于。（AC）

A、数字签名 B、加密 C、密钥管理 D、哈希函数

754、目前基于对称密钥体制的算法主要有。（BC）

A、RSA B、DES C、AES D、DSA

755、使用esp协议时，可以使用的加密运算是。（ABC）

A、DES B、3DES C、AES D、RSA

756、数字签名的作用是。（ACD）

A、确定一个人的身份 B、保密性

C、肯定是该人自己的签字 D、使该人与文件内容发生关系

757、以下属于对称加密算法的是：（ABD）

A、DES B、3DES C、SHA-1 D、RC4 E、MD5

758、在加密过程中，必须用到的三个主要元素是（ABC）

A、所传输的信息（明文） B、加密 钥匙（Encryption Key）

C、加密函数 D、传输信道

759、账号口令管理办法适用于所有和DSMP系统、智能网系统、彩铃平台相关的（ACD）

A、系统管理员 B、操作系统

C、操作维护人员 D、所有上述系统中存在的账号和口令

760、为保证密码安全，我们应采取的正确措施有（ABC）

A、不使用生日做密码 B、不使用少于5为的密码

C、不适应纯数字密码 D、将密码设的非常复杂并保证20位以上

761、公司在使用数据签名技术时，除充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名外，还应注意（ABCD）

A、采取保护公钥完整性的安全措施，例如使用公约证书

B、确定签名算法的类型、属性以及所用密钥长度

C、用于数字签名的密钥应不同于用来加密内容的密钥

D、符合有关数字签名的法律法规，必要时，应在合同或协议中规定使用数字签名的相 关事宜

762、相对于对称加密算法，非对称密钥加密算法（ACD）

A、加密数据的速率较低

B、更适合于现有网络中对所传输数据（明文）的加解密处理

C、安全性更好 D、加密和解密的密钥不同

763、一个典型的PKI应用系统包括（ABCD）实体

A、认证机构CA B、册机构RA C、证书及CRL目录库 D、用户端软件

764、加密的强度主要取决于（ABD）

A、算法的强度 B、密钥的保密性 C、明文的长度 D、密钥的强度

765、一下对于对称密钥加密说法正确的是（BCD）

A、对称加密算法的密钥易于管理 B、加解密双方使用同样的密钥

C、DES算法属于对称加密算法 D、相对于非对称加密算法，加解密处理速度比较快

766、在通信过程中，只采用数字签名可以解决（ABC）等问题

A、数据完整性 B、数据的抵抗赖性 C、数据的篡改 D、数据的保密性

767、对称密钥算法体系包括：（ABCDE）

A、明文(plaintext)：原始消息或数据，作为算法的输入

B、加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换

C、秘密密钥(secret key)：秘密密钥也是算法输入，算法进行的具体替换和转换取决于 这个密钥

D、密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对 于一个给定的消息，两个不同的密钥会产生两个不同的密文

、.解密算法(decryption algorithm)：本质上是加密算法的执行。它使用密文和统一密钥 产生原始明文

768、一下对于混合加密方式说法正确的是。（BCD）

A、 使用公开密钥密码体制对要传输的信息（明文）进行加解密处理

B、使用对称加密算法对要传输的信息（明文）进行加解密处理

C、使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信

D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的

769、电信的网页防篡改技术有（ABC）

A、外挂轮询技术 B、核心内嵌技术

C、时间触发技术 D、安装防病毒软件

770、病毒发展的趋势是？（ABC）

A、 范围更广 B、度更快 C、方式更多

771、病毒自启动方式一般有（ABC）

A、 修改注册表 B、将自身添加为服务

C、将自身添加到启动文件夹 D、修改系统配置文件

772、常见Web攻击方法有一下哪种？（ABCD）

A、SQL Injection B、Cookie欺骗 C、跨站脚本攻击

D、信息泄露漏洞 E、文件腹泻脚本存在的安全隐患

F、 GOOGLE HACKING

773、宏病毒感染一下哪些类型的文件？（ABCDEF）

A、DOC B、EXE C、XLS D、DOT

774、木马传播包括一下哪些途径：（ACD）

A、通过电子邮件的附件传播 B、通过下载文件传播

C、通过网页传播 D、通过聊天工具传播

775、目前最好的防病毒软件能做到的是（ABCD）

A、检查计算机是否感染病毒，消除已感染的任何病毒

B、杜绝病毒对计算的侵害

C、查出计算机已感染的已知病毒，消除其中的一部分

D、检查计算机是否染有已知病毒，并作相应处理

776、通用的DoS攻击手段有哪些？（CD）

A、 SYN Attack B、ICMP Flood C、UDP Flood

D、Ping of Death E、Tear Drop F、Ip Spoofing

777、以下关于蠕虫的描述正确的有：（ABCDEF）

A、 蠕虫具有自动利用网络传播的特点，在传播的同时，造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪

B、 隐藏式蠕虫的基本特征，通过在主机上隐藏，使得用户不容易发现它的存在

C、蠕虫需要传播受感染的宿主文件来进行复制

D、蠕虫的传染能力主要是针对计算机内的文件系统。

778、以下哪几种扫描检测技术属于被动式的检测技术？（AB）

A、 基于应用的检测技术 B、基于主动的检测技术

C、基于目标的漏洞检测技术 D、基于网络的检测技术

779、以下是检查磁盘与文件是否被病毒感染的有效方法：（BC）

A、 检查磁盘目录中是否有病毒文件 B、用抗病毒软件检查磁盘的各个文件

C、用放大镜检查磁盘编码是否有霉变现象 D、检查文件的长度是否无故变化

780、造成计算机不安全的因素有（BD）等多种。

A、 技术原因 B、自然原因 C、认为原因 D、管理原因

781、嗅探技术有哪些特点？（ABCD）

A、间接性 B、.直接性 C、隐蔽性 D、开放性

782、一个恶意的攻击者必须具备哪几点？（ABC）

A、 方法 B、机会 C、动机 D、运气

783、对于DOS网络攻击，可以采用以下哪些措施来缓解主机系统被攻击进程。（ACD）

A、缩短SYN Timeout时间和设置SYN Cookie B、增加网络带宽

C、在系统之前增加负载均衡设备 D、在防火墙上设置ACL或黑客路由

784、利用Bind/DNS漏洞攻击的分类主要有（ACD）

A、 拒绝服务 B、匿名登录 C、.缓冲区溢出

D、DNS缓存中毒 E、病毒或后门攻击

785、常见Web攻击方法有一下哪种？（ABCD）

A、 SQL Injection B、 Cookie欺骗 C、 跨站脚本攻击 D、信息泄露漏洞

786、黑客所使用的入侵技术主要包括（ABCDE）

A、协议漏洞渗透 B、密码分析还原 C、应用漏洞分析与渗透

D、拒绝服务攻击 E、病毒或后门攻击

787、主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有（ABC）

A、针对入侵者采取措施 B、修正系统

C、收集更详细的信息 D、入侵追踪

788、下面哪些漏洞属于网络服务类安全漏洞：（BC）

A、Windows 2000中文版输入法漏洞 B、IS Web服务存在的IDQ远程溢出漏洞

C、RPC DCOM服务漏洞 D、Web服务asp脚本漏洞

789、系统感染病毒后的现象有哪些？（ABCD）

A、系统错误或系统崩溃 B、系统反应慢，网络拥塞

C、陌生的进程或服务 D、陌生的自启动

**三、判断题：（790-1000）**

790、TCSEC将信息安全风机防护等级一共分为7个安全等级：D、C1、C2、B1、B2、B3、 A。(A)

A、正确 B、错误

791、通用标准v2版（CC）的安全等级是以EAL来表示的。（A）

A、正确 B、错误

792、一个企业的信息安全组织能否顺利开展工作（定期安全评估、日志安全巡检、定期安全审核、应急演练等），主要取决于公司领导对信息安全工作的认识程度和支持力度。（A）

A、正确 B、错误

793、在信息安全领域，CIA通常是指：保密性、完整性和可用性。（A）

A、正确 B、错误

794、信息安全是永远是相对的，并且需要不断持续关注和改进，永远没有一劳永逸的安全

防护措施。（A）

A、正确 B、错误

795、在信息安全领域，CIA通常是指：保密性、完整性和非抵赖性。（B）

A、正确 B、错误

796、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

797、信息安全的威胁主体包括内部人员、准内部人员、外部人员、系统自身等方面。（B）

A、正确 B、错误误

798、互联网网络安全事件根据危害和紧急程度分为一般、预警、报警、紧急、重大五种。 （B）

A、正确 B、错误

799、安全审计是从管理和技术两个方面检查公司的安全策略和控制措施的执行情况，发现安全隐患的过程。（A）

A、正确 B、错误

800、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

801、计算机系统安全是指应用系统具备访问控制机制，数据不被泄露、丢失、篡改等。（B）

A、正确 B、错误

802、主机加固完成后，一般可以有效保证主机的安全性增强。（A）

A、正确 B、错误

803、黑客在进行信息收集时，通常利用Windows的IPC漏洞可以获得系统用户的列表的信 息。（A）

A、正确 B、错误

804、Solaris系统中一般需要确认ROOT账号只能本地登录，这样有助于安全增强。（A）

A、正确 B、错误

805、HP-UX系统加固中在设置ROOT环境变量不能有相对路径设置。（A）

A、正确 B、错误

806、屏幕保护的木马是需要分大小写。（B）

A、正确 B、错误

807、安全审计就是日志的记录。（B）

A、正确 B、错误误

808、HP-UX系统加固中在设置通用用户环境变量不能有相对路径设置。（A）

A、正确 B、错误

809、AIX系统加固时，对系统配置一般需要自编脚本完成。（A）

A、正确 B、错误

810、Windows NT中用户登录域的口令是以明文方式传输的。（B）

A、正确 B、错误

811、操作系统普通用户账号审批记录应编号、留档。（A）

A、正确 B、错误

812、计算机病毒是计算机系统中自动产生的。（B）

A、正确 B、错误

813、主机系统加固时根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。（A）

A、正确 B、错误

814、4A系统的建设能够减轻账户管理员的维护工作。（A）

A、正确 B、错误

815、4A系统的接入管理可以管理到用户无力访问的接入。（B）

A、正确 B、错误

816、Cisco路由器可以使用enable password命令为特权模式的进入设置强壮的密码。（B）

A、正确 B、错误

817、Cisco设备的AUX端口默认是启用的。（A）

A、正确 B、错误

818、DHCP可以向终端提供IP地址、网关、DNS服务器地址等参数。（A）

A、正确 B、错误误

819、Inbound方向的NAT使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际IP地址。（B）

A、正确 B、错误

820、IPS设备即使不出现故障，它仍然是一个潜在的网络瓶颈，需要强大的网络结构来配合。（A）

A、正确 B、错误

821、IPS的过滤器规则不能自由定义。（B）

A、正确 B、错误

822、IPS的某些功能和防火墙类似。（A）

A、正确 B、错误

823、IPS和IDS都是主动防御系统。（B）

A、正确 B、错误

824、NAT是一种网络地址翻译的技术，它能是的多台没有合法地址的计算机共享一个合法的IP地址访问Internet。（A）

A、正确 B、错误

825、Netscreen的ROOT管理员具有的最高权限，为了避免ROOT管理员密码被窃取后造成威胁，应该限制ROOT只能通过CONSOLE接口访问设备，而不能远程登录。(A)

A、正确 B、错误

826、Netscreen防火墙的外网口应禁止PING测试，内网口可以不限制。（B）

A、正确 B、错误

827、OSI是开放的信息安全的缩写。（B）

A、正确 B、错误

828、OSI七层模型中，传输层数据成为段（Segment），主要是用来建立主机端到端连接，包括TCP和UDP连接。（A）

A、正确 B、错误

829、OSI中会话层不提供机密性服务。（A）

A、正确 B、错误

830、SSH使用TCP 79端口的服务。（B）

A、正确 B、错误

831、TCP/IP模型从下至上分为四层：物理层，数据链路层，网络层和应用层。（B）

A、正确 B、错误

832、TCP/IP模型与OSI参考模型的不同点在于TCP/IP把表示层和会话层都归于应用层，所以TCP/IP模型从下至上分为五层：物理层，数据链路层，网络层，传输层和应用层。 （A）

A、正确 B、错误

833、TCP/IP协议体系结构中，IP层对应OSI/RM模型的网络层。（A）

A、正确 B、错误

834、默认情况下需要关闭Cisco设备的Small TCP/UDP服务。（A）

A、正确 B、错误

835、缺省情况下，防火墙工作模式为路由模式，切换工作模式后可直接进行进一步配置。（B）

A、正确 B、错误

836、入侵检测具有对操作系统的校验管理，判断是否有破坏安全的用户活动。（A）

A、正确 B、错误

837、入侵检测可以处理数据包级的攻击。（B）

A、正确 B、错误

838、入侵检测系统不能弥补由于系统提供信息的质量或完整性的问题。（A）

A、正确 B、错误

839、入侵检测系统能够检测到用户的对主机、数据库的网络操作行为。（B）

A、正确 B、错误

840、入侵检测系统是一种对计算机系统或网络事件进行检测并分析这个入侵事件特征的过程。（A）

A、正确 B、错误

841、统计分析的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。（B）

A、正确 B、错误

842、统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。（A）

A、正确 B、错误

843、透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决IP地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的IP的地址。（A）

A、正确 B、错误

844、完整性分析的缺点是一般以批处理方式实现，不用于实时响应。（A）

A、正确 B、错误

845、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（B）

A、正确 B、错误

846、网络边界的Cisco路由器应关闭CDP服务。（A）

A、正确 B、错误

847、网络边界Cisco设备的CDP协议可以开放。（B）

A、正确 B、错误

848、网络层的防护手段（防火墙，SSL，IDS，加固）可以组织或检测到应用层攻击。（B）

A、正确 B、错误

849、针对不同的攻击行为，IPS只需要一个过滤器就足够了。（B）

A、正确 B、错误

850、主机型IDS其数据采集部分当然位于其所检测的网络上。（B）

A、正确 B、错误

851、状态检测防火墙检测每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。（B）

A、正确 B、错误

852、IPS虽然能主动防御，但是不能坚挺网络流量。（B）

A、正确 B、错误

853、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。（B）

A、正确 B、错误

854、审计系统进行关联分析时不需要关注日志时间。（B）

A、正确 B、错误

855、垃圾邮件一般包括商业广告、政治邮件、病毒邮件、而已欺诈邮件（网络钓鱼）等几个方面。（A）

A、正确 B、错误

856、防止网络窃听最好的方法就是给网上的信息加密，是的侦听程序无法识别这些信息模式。（A）

A、正确 B、错误

857、侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。（A）

A、正确 B、错误

858、模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。（A）

A、正确 B、错误

859、入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。（A）

A、正确 B、错误

860、VPN的主要特点是通过加密是信息安全的通过Internet传递。（A）

A、正确 B、错误

861、传输层协议使用端口号（Port）来标示和区分上层应用程序，如：Telnet协议用的是23号端口、DNS协议使用69号端口。（B）

A、正确 B、错误

862、如果Web应用对URL访问控制不当，可能造成用户直接在浏览器中输入URL，访问不该访问的页面。（A）

A、正确 B、错误

863、如果Web应用没有对攻击者的输入进行适当的编码和过滤，就用于构造数据库查询或操作系统命令时，可能导致注入漏洞。（A）

A、正确 B、错误

864、HTTP协议定义了Web浏览器向Web服务器发生Web页面请求的格式及Web页面在Internet上传输的方式。（A）

A、正确 B、错误

865、HTTP协议是文本协议，可利用回车换行做边界干扰。（A）

A、正确 B、错误

866、Init<sid>.ora文件是Oracle启动文件，任何参数的配置错误都会造成Oracle不能启动，任何参数的不合理配置都可能造成系统故障。（A）

A、正确 B、错误

867、Mysqldump是采用SQL级别的备份机制，它将数据表导成SQL脚本文件，在不同的MySQL版本之间升级时相对比较合适，这也是最常见的备份方法。（A）

A、正确 B、错误

868、Orabrute是进行远程破解Oracle密码的工具，要猜解的密码可以在password.txt中设置。（A）

A、正确 B、错误

869、Oracle的SYS账户在数据库中具有最高权限，能够做任何事情，包括启动/关闭Oracle数据库。即使SYS被锁定，也已然能够访问数据库。（A）

A、正确 B、错误

870、Oracle的若算法加密机制：两个相同的用户名和密码在两个不同的Oracle数据库机器中，将具有相同的哈希值。（A）

A、正确 B、错误

871、Oracle密码允许包含像“SELECT”，“DELETE”，“CREATE”这类的Oracle/SQL关键字。（B）

A、正确 B、错误

872、Oracle的HTTP的基本验证可选择SYS破解，因为它始终存在和有效。（A）

A、正确 B、错误

873、Oracle默认情况下，口令的传输方式是加密。（B）

A、正确 B、错误

874、Oracle数据库的归档日志不是在线日志的备份。（B）

A、正确 B、错误

875、OSI网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。（A）

A、正确 B、错误

876、OSI网络安全体系结构的五类安全服务是鉴别、访问控制、保密性、完整性、抗否认。（A）

A、正确 B、错误

877、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因。（A）

A、正确 B、错误

878、SQL Server如果设置了不恰当的数据库文件权限，可能导致敏感文件被非法删除或读取，威胁系统安全。（A）

A、正确 B、错误

879、SQL Server数据库应禁止使用除tcp/ip以外的协议，保护数据库通信安全。（A）

A、正确 B、错误

880、SQL Server应该社会自日志审核无法追踪回溯安全事件。（A）

A、正确 B、错误

881、Web服务器一般省缺不允许攻击者访问Web根目录以外的内容，内容资源不可以任意访问。(A)

882、Web攻击面不仅仅是浏览器中可见的内容。（A）

A、正确 B、错误

883、Web应用对网络通讯中包含的敏感信息进行加密，就不会被窃听。（B）

A、正确 B、错误

884、暴力猜解不能对Web应用进行攻击。（B）

A、正确 B、错误

885、在Oracle自身的配置上做限定方法是：修改$Oracle\_HOME\network\admin目录下面的SQLNET..ORA文件，类似设置如下：

Tcp\_validnode\_checking=YES

Tcp\_invited\_nodes=

(192.168.0.1,ip2,ip3•••...)。

( A )

A、正确 B、错误

886、不设置必要的日志审核，就无法追踪回溯安全事件，Oracle中若果要审计记录成功的登陆语句”SQL>audit session whenever successful;”. ( A )

A、正确 B、错误

887、对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是DNS服务器。（B）

A、正确 B、错误

888、防止XSS各种方法都有优劣之处，防范XSS的真正挑战不在于全免，而在于细致。（B）

A、正确 B、错误

889、访问控制、强制登陆、自动安全更新都属于Window2000的安全组件（B）

A、正确 B、错误

890、复杂的系统存在大量的相互引用访问，如果开发者不能有效的进行权限控制，就可能被恶意引用。（A）

A、正确 B、错误

891、攻击者可以通过SQL注入手段获取其他用户的密码。（A）

A、正确 B、错误

892、几乎所有的关系数据库系统和相应的SQL语言都面临SQL注入的潜在威胁。（A)

A、正确 B、错误

893、简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架（B）

A、正确 B、错误

894、默认可通过Web程序来远程管理Oracle10g数据库，端口是8080.（A）

A、正确 B、错误

895、如果sa是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。（A）

A、正确 B、错误

896、如果在SQL Server等领域成功并不意味这该用户已经可以访问SQL Server上的数据库。（A）

A、正确 B、错误

897、如果知道Oracle密码长度，用Rainbow表生成器来破解其密码哈希值是绝对成功的。（A）

A、正确 B、错误

898、所有操作系统、数据库、网络设备，包括一部分业务系统，均需要支持基于账号的访问控制功能。（B）

A、正确 B、错误

899、网络拓扑分析为检查是否有配置错误项泄露内部IP地址，从而推断网站系统拓扑。（A）

A、正确 B、错误

900、为Oracle数据库安全考虑，在对人共同对数据库进行维护时应依赖数据库预定义的传统角色。（B）

A、正确 B、错误

901、为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。(A)

A、正确 B、错误

902、系统类型鉴别为检查主机系统与开放服务是否存在安全漏点。（B）

A、正确 B、错误

903、系统漏洞扫描为检查目标的操作系统与应用系统信息。（B）

A、正确 B、错误

904、选择远程破解Oracle的最好账户是SYS，因为此账户永远有效。（A）

A、正确 B、错误

905、一封电子邮件可以拆分成对个IP包，每个IP包可以沿不同的路径到达目的地。（A）

A、正确 B、错误

906、一个共享文件夹。将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有读取的权限。（A）

A、正确 B、错误

907、用Sqlplus登陆到Oracle数据库，使用slesct username, password form dba\_users命令可查看数据库中的用户名和密码明文。（B）

A、正确 B、错误

908、有的Web应用登陆界面允许攻击者暴力猜解口令，在自动工具与字典表的帮助下，可以迅速找到弱密码用户。（A）

A、正确 B、错误

909、在Oracle所有版本在安装的时候都没有提示修改SYS的默认密码。（B）

A、正确 B、错误

910、在ORacle数据库安装补丁时，不需要关闭所有与数据库有关的服务。（B）

A、正确 B、错误

911、在SQL Server安装SP3补丁时不需要系统中已经安装了SP1或SP2。（B）

A、正确 B、错误

912、在SQL Server中具有sysadmin权限的用户可以通过xp\_cmdshell存储扩展以system的权限执行任意系统命令。（A）

A、正确 B、错误

913、Oracle默认配置下，每个账户如果有30次的失败登陆，此账户将被锁定。（B）

A、正确 B、错误

914、定制开发Web系统的安全度不如标准的产品。（A）

A、正确 B、错误

915、对MySQL注入攻击时，经常用到注释符号#来屏蔽剩下的内置SQL语句。（A）

A、正确 B、错误

916、一个登录名只能进入服务器，但是不能让用户访问服务器中的数据库资源。每个登录名的定义存放在msater数据库的syslogins表中。（A）

A、正确 B、错误

917、Web错误信息可能泄露服务器型号版本、数据库型号、路径、代码。（A）

A、正确 B、错误

918、Oracle的密码哈希值存储在SYS.USER$表中。可以通过像DBA USERS这类的视图来访问。（A）

A、正确 B、错误

919、产品的定制开发是应用安全中最薄弱的一环。（A）

A、正确 B、错误

920、Oracle限制了密码由英文字母，数字，#，下划线（\_），美元字符（$）构成，密码的最大长度为30字符；并不能以”$”,”#”,”\_”或任何数字开头。（A）

A、正确 B、错误

921、网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。（B）

A、正确 B、错误

922、计算机场地可以选择在公共区域人流量比较大的地方。（B）

A、正确 B、错误

923、EMC测试盒约束用户关心的信息信号的电磁发射、TEMPEST只测试盒约束系统和设备的所有电磁发射。（B）

A、正确 B、错误

924、加密传输是一种非常有效并经常使用的方法，也能解决输入和输出端的电磁信息泄露问题。（B）

A、正确 B、错误

925、出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。（B）

A、正确 B、错误

926、红区：红新号的传输通道或单元电路称为红区，反之为黑区。（A）

A、正确 B、错误

927、机房应设置相应的活在报警和灭火系统。（A）

A、正确 B、错误

928、计算机机房的建设应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。（A）

A、正确 B、错误

929、计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。（B）

A、正确 B、错误

930、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。（A）

A、正确 B、错误

931、提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。（A）

A、正确 B、错误

932、在计算机机房附近施工，不负有维护计算机信息系统安全的责任和义务。（B）

A、正确 B、错误

933、只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。（B）

A、正确 B、错误

934、主管计算机信息系统安全的公安机关和城建及规划部门，应与设施单位进行协调，在不危害用户利益的大前提下，制定措施。合理施工，做好计算机信息系统安全保护工作。（B）

A、正确 B、错误

935、防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。（A）

A、正确 B、错误

936、对于公司机密信息必须根据公司的相关规定予以适当的标识。（A）

A、正确 B、错误

937、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。（A）

A、正确 B、错误

938、如果在电话、电视会议中涉及讨论工伤机密信息，会议主持人或组织人在会议全过程中一定要确认每一个与会者是经授权参与的。（A）

A、正确 B、错误

939、为防止信息非法泄露，需要销毁存储介质时，应该批准后自行销毁。（B）

A、正确 B、错误

940、将公司的机密信息通过互联网络传送时，必须予以加密。（A）

A、正确 B、错误

941、机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。（A）

A、正确 B、错误

942、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式进行保密。（A）

A、正确 B、错误

943、“一次一密”属于序列密码的一种。（A）

A、正确 B、错误

944、3DES算法的加密过程就是用一个秘钥对待加密的数据执行三次DES算法的加密操作。（B）

A、正确 B、错误

945、AES加密算法的秘钥长度为128、192或256位。（A）

A、正确 B、错误

946、AES是一种非对称算法。（B）

A、正确 B、错误

947、DES3和RSA是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。（A）

A、正确 B、错误

948、Diffie-Hellman算法的安全性取决于离散对数计算的困难性，可以实现秘钥交换。（A）

A、正确 B、错误

949、DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。（A）

A、正确 B、错误

950、MD5是一种加密算法。（B）

A、正确 B、错误

951、PGP协议缺省的压缩算法是ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。（A）

A、正确 B、错误

952、PKI是一个用对称密码算法和技术来实现并提供安全服务的具有通用性的安全基础设施。（B）

A、正确 B、错误

953、RC4是典型的的序列密码算法。（A）

A、正确 B、错误

954、RSA算法作为主要的非对称算法，使用公钥加密的秘闻一定要采用公钥来街。（B）

A、正确 B、错误

955、安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。（A）

A、正确 B、错误

956、常见的公钥密码算法有RSA算法、Diffie-Hellman算法和EIGamal算法。（A）

A、正确 B、错误

957、当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（A）

A、正确 B、错误

958、发送方使用AH协议处理数据包，需要对整个IP的数据包计算MAC，包括IP头的所有字段和数据。（B）

A、正确 B、错误

959、分组密码的优点是错误扩展小、速度快、安全程度高。（B）

A、正确 B、错误

960、公共迷药密码体制在秘钥管理上比对称秘钥密码体制更安全。（A）

A、正确 B、错误

961、古典加密主要采用的主要方法是置换，代换。（A）

A、正确 B、错误

962、古典加密主要是对加密算法的保密，现代加密算法是公开的，主要是针对秘钥进行保密。（A）

A、正确 B、错误

963、基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。（A）

A、正确 B、错误

964、口令应在120天至少更换一次。（B）

A、正确 B、错误

965、链路加密方式适用于在广域网系统中应用。（B）

A、正确 B、错误

966、密码保管不善属于操作失误的安全隐患。（B）

A、正确 B、错误

967、日常所见的校园饭卡是利用身份认证的单因素法。（A）

A、正确 B、错误

968、身份认证要求对数据和信息来源进行验证，以确保发信人的身份。（B）

A、正确 B、错误

969、身份认证与权限控制是网络社会的管理基础。（A）

A、正确 B、错误

970、数据在传输过程中用哈希算法保证其完整性后，非法用户无法无法对数据进行任何修改。（B）

A、正确 B、错误

971、数字签名比较的是摘要结果长度是否都是128位。（B）

A、正确 B、错误

972、通信数据与文件加密是同一个概念。（B）

A、正确 B、错误

973、为AES开发的Rijndae1算法的秘钥长度是128位，分组长度也为128位。（B）

A、正确 B、错误

974、为了保证安全性，密码算法应该进行保密。（B）

A、正确 B、错误

975、文件压缩变换是一个单向加密过程。（B）

A、正确 B、错误

976、我的公钥证书不能在网络上公开，否则其他人可能冒充我的身份或伪造我的数字签名。（B）

A、正确 B、错误

977、现代加密算法可以分为对称加密算法和非对称加密。（A）

A、正确 B、错误

978、虚拟专用网VPN的关键技术主要是隧道技术、加解密技术、秘钥管理技术以及使用者与设备身份认证技术。（A）

A、正确 B、错误

979、以当前的技术来说，RSA体制是无条件安全的。（B）

A、正确 B、错误

980、在4A系统的远期建设中，应用系统自身不需要保留系统从账户信息。（B）

A、正确 B、错误

981、在MD5算法中，要先将以初始化的A、B、C、D这四个变量分别复制到a、b、c、d中。（A）

A、正确 B、错误

982、在MD5算法中要用到4个变量，分别表示A、B、C、D，均为32位长。（A）

A、正确 B、错误

983、在PKI中，注册机构RA是必要的组件。（B）

A、正确 B、错误

984、在SSL握手协议过程中，需要服务器发送自己的证书。（A）

A、正确 B、错误

985、在非对称加密过程中，加密和解密使用的是不同的秘钥。（A）

A、正确 B、错误

986、在公钥加密系统中，用公钥加密的密文可以由私钥解密，但用公钥加密的密文，不能用公钥解密。 （B）

A、正确 B、错误

987、在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一种“破解”。 （A）

A、正确 B、错误

988、账户管理的Agent不适用于在网络设备中部署。 （A）

A、正确 B、错误

989、整个PKI系统有证书服务器AS、票据许可服务器TGS、客户机和应用服务器四部分组成。 （B）

A、正确 B、错误

990、最基本的认证方式选择证书是数字证书。（B）

A、正确 B、错误

991、最小特权、纵深防御是网络安全原则之一。（A）

A、正确 B、错误

992、数字证书是由权威机构CA发行的一种权威的电子文档，是网络环境中的一种身份证。（A）

A、正确 B、错误

993、数字证书是由权威机构PKI发行的一种权威性的电子文档，是网络环境中的一种身份证。 （B）

A、正确 B、错误

994、信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段。（A）

A、正确 B、错误

995、病毒能隐藏在电脑的CMOS存储器里。（B）

A、正确 B、错误

996、对感染病毒的软盘进行浏览会导致硬盘被感染。（B）

A、正确 B、错误

997、已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（B）

A、正确 B、错误

998、重新格式化硬盘可以清楚所有病毒。（B）

A、正确 B、错误

999、专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，并根据评估结果提供评估报告。 （A）

A、正确 B、错误

1000、冒充信件回复、假装纯文字ICON、冒充微软雅虎发信、下载电子贺卡同意书、是使用的叫做字典攻击法的方法。（B）

A、正确 B、错误

1. 1单项选择题（1-605）
2. Chinese Wall 模型的设计宗旨是：（A）。

A、用户只能访问哪些与已经拥有的信息不冲突的信息 B、用户可以访问所有信息

C、用户可以访问所有已经选择的信息 D、用户不可以访问哪些没有选择的信息

1. 安全责任分配的基本原则是：（C）。

A、“三分靠技术，七分靠管理” B、“七分靠技术，三分靠管理”

C、“谁主管，谁负责” D、防火墙技术

1. 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（B）不属于信息运行安全技术的范畴。

A、风险分析 B、审计跟踪技术 C、应急技术 D、防火墙技术

1. 从风险的观点来看，一个具有任务紧急性，核心功能性的计算机应用程序系统的开发和维护项目应该（A）。

A、内部实现 B、外部采购实现 C、合作实现 D、多来源合作实现

1. 从风险分析的观点来看，计算机系统的最主要弱点是（B）。

A、内部计算机处理 B、系统输入输出 C、通讯和网络 D、外部计算机处理

1. 从风险管理的角度，以下哪种方法不可取？（D）

A、接受风险 B、分散风险 C、转移风险 D、拖延风险

1. 当今IT的发展与安全投入，安全意识和安全手段之间形成（B）。

A、安全风险屏障 B、安全风险缺口 C、管理方式的变革 D、管理方式的缺口

1. 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（D）。

A、已买的软件 B、定做的软件 C、硬件 D、数据

1. 当一个应用系统被攻击并受到了破坏后，系统管理员从新安装和配置了此应用系统，在该系统重新上线前管理员不需查看：（C）

A、访问控制列表 B、系统服务配置情况

1. 审计记录 D、用户账户和权限的设置

10、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行（B）。

1. 逻辑隔离 B、物理隔离 C、安装防火墙 D、VLAN 划分

11、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？（D）

A、威胁、脆弱性 B、系统价值、风险

C、信息安全、系统服务安全 D、受侵害的客体、对客体造成侵害的程度业务

12、公司应明确员工的雇佣条件和考察评价的方法与程序，减少因雇佣不当而产生的安全风险。人员考察的内容不包括（B）。

A、身份考验、来自组织和个人的品格鉴定 B、家庭背景情况调查

C、学历和履历的真实性和完整性 D、学术及专业资格

13、计算机信息的实体安全包括环境安全、设备安全、（B）三个方面。

A运行安全 B、媒体安全 C、信息安全 D、人事安全

14、目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（B）

A、公安部 B、国家保密局

C、信息产业部 D、国家密码管理委员会办公室

15、目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（B）

A、GB/T 18336-2001 信息技术安全性评估准则

B、GB 17859-1999 计算机信息系统安全保护等级划分准则

C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构

D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

16、确保信息没有非授权泄密，即确保信息不泄露给非授权的个人、实体或进程，不为其所用，是指（C）。

A、完整性 B、可用性 C、保密性 D、抗抵赖性

17、如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（A）

A、自动软件管理 B、书面化制度 C、书面化方案 D、书面化标准

18、如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？（A）

A、计算风险 B、选择合适的安全措施

C、实现安全措施 D、 接受残余风险

19、软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（A）

A、软件中止和黑客入侵 B、远程监控和远程维护

C、软件中止和远程监控 D、远程维护和黑客入侵

20、 管理审计指（C）

A、保证数据接收方收到的信息与发送方发送的信息完全一致

B、防止因数据被截获而造成的泄密

C、对用户和程序使用资源的情况进行记录和审查

D、保证信息使用者都可

21、为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（A）

A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B、进行离职谈话，禁止员工账号，更改密码

C、让员工签署跨边界协议

D、列出员工在解聘前需要注意的所有责任

22、为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（D）

A、人际关系技能 B、项目管理技能 C、技术技能 D、沟通技能

23、我国的国家秘密分为几级？（A）

A、3 B、4 C、5 D、6

24、系统管理员属于（C）。

A、决策层 B、管理层

C、执行层 D、既可以划为管理层，又可以划为执行层

25、下列哪一个说法是正确的？（C）

A、风险越大，越不需要保护 B、风险越小，越需要保护

C、风险越大，越需要保护 D、越是中等风险，越需要保护

26、下面哪类访问控制模型是基于安全标签实现的？（B）

A、自主访问控制 B、强制访问控制

C、基于规则的访问控制 D、基于身份的访问控制

27、下面哪项能够提供最佳安全认证功能？（B）

A、这个人拥有什么 B、这个人是什么并且知道什么

C、这个人是什么 D、这个人知道什么

28、下面哪一个是国家推荐性标准？（A）

A、GB/T 18020-1999 应用级防火墙安全技术要求

B、SJ/T 30003-93 电子计算机机房施工及验收规范

C、GA243-2000 计算机病毒防治产品评级准则

D、ISO/IEC 15408-1999 信息技术安全性评估准则

29、下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（C）

A、对安全违规的发现和验证是进行惩戒的重要前提

B、惩戒措施的一个重要意义在于它的威慑性

C、处于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训

D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

30、下面哪一项最好地描述了风险分析的目的？（C）

A、识别用于保护资产的责任义务和规章制度

B、识别资产以及保护资产所使用的技术控制措施

C、识别资产、脆落性并计算潜在的风险

D、识别同责任义务有直接关系的威胁

31、下面哪一项最好地描述了组织机构的安全策略？（A）

A、定义了访问控制需求的总体指导方针

B、建议了如何符合标准

C、表明管理意图的高层陈述

D、表明所使用的技术控制措施的高层陈述

32、下面哪一种风险对电子商务系统来说是特殊的？（D）

A、服务中断 B、应用程序系统欺骗

C、未授权的信息泄露 D、确认信息发送错误

33、下面有关我国标准化管理和组织机构的说法错误的是？（C）

A、国家标准化管理委员会是统一管理全国标准化工作的主管机构

B、国家标准化技术委员会承担国家标准的制定和修改工作

C、全国信息安全标准化技术委员负责信息安全技术标准的审查、批准、编号和发布

D、全国信息安全标准化技术委员负责统一协调信息安全国家标准年度技术项目

34、项目管理是信息安全工程师基本理论，以下哪项对项目管理的理解是正确的？（A）

A、项目管理的基本要素是质量，进度和成本

B、项目管理的基本要素是范围，人力和沟通

C、项目管理是从项目的执行开始到项目结束的全过程进行计划、组织

D、项目管理是项目的管理者，在有限的资源约束下，运用系统的观点，方法和理论，对项目涉及的技术工作进行有效地管理

35、信息安全的金三角是（C）。

A、可靠性，保密性和完整性 B、多样性，冗余性和模化性

C、保密性，完整性和可用性 D、多样性，保密性和完整性

36、信息安全风险缺口是指（A）。

A、IT的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

37、信息安全风险应该是以下哪些因素的函数？（A）

A、信息资产的价值、面临的威胁以及自身存在的脆弱性等

B、病毒、黑客、漏洞等

C、保密信息如国家密码、商业秘密等

D、网络、系统、应用的复杂的程度

38、信息安全工程师监理的职责包括？（A）

A、质量控制，进度控制，成本控制，合同管理，信息管理和协调

B、质量控制，进度控制，成本控制，合同管理和协调

C、确定安全要求，认可设计方案，监视安全态势，建立保障证据和协调

D、确定安全要求，认可设计方案，监视安全态势和协调

39、信息安全管理最关注的是？（C）

A、外部恶意攻击 B、病毒对PC的影响

C、内部恶意攻击 D、病毒对网络的影响

40、信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（C）

A、信息的价值 B、信息的时效性

C、信息的存储方式 D、法律法规的规定

41、信息网络安全的第三个时代是（A）

A、主机时代，专网时代，多网合一时代 B、主机时代，PC时代，网络时代

C、PC时代，网络时代，信息时代 D、2001年，2002年，2003年

42、一个公司在制定信息安全体系框架时，下面哪一项是首要考虑和制定的？（A）

A、安全策略 B、安全标准 C、操作规程 D、安全基线

43、以下哪个不属于信息安全的三要素之一？（C）

A、机密性 B、完整性 C、抗抵赖性 D、可用性

44、以下哪一项安全目标在当前计算机系统安全建设中是最重要的？（C）

A、目标应该具体 B、目标应该清晰

C、目标应该是可实现的 D、目标应该进行良好的定义

45、以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（A）

A、制度和措施 B、漏洞分析

C、意外事故处理计划 D、采购计划

46、以下哪一项是对信息系统经常不能满足用户需求的最好解释？（C）

A、没有适当的质量管理工具 B、经常变化的用户需求

C、用户参与需求挖掘不够 D、项目管理能力不强

47、以下哪一种人给公司带来了最大的安全风险？（D）

A、临时工 B、咨询人员 C、以前的员工 D、当前的员工

48、以下哪种安全模型未使用针对主客体的访问控制机制？（C）

A、基于角色模型 B、自主访问控制模型

C、信息流模型 D、强制访问控制模型

49、以下哪种措施既可以起到保护的作用还能起到恢复的作用？（C）

A、对参观者进行登记 B、备份

C、实施业务持续性计划 D、口令

50、以下哪种风险被定义为合理的风险？（B）

A、最小的风险 B、可接受风险

C、残余风险 D、总风险

51、以下人员中，谁负有决定信息分类级别的责任？（B）

A、用户 B、数据所有者 C、审计员 D、安全官

52、有三种基本的鉴别的方式：你知道什么，你有什么,以及（C）。

A、你需要什么 B、你看到什么 C、你是什么 D、你做什么

53、在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（B）

A、自下而上 B、自上而下 C、上下同时开展 D、以上都不正确

54、在风险分析中，下列不属于软件资产的是（D）

A、计算机操作系统 B、网络操作系统

C、应用软件源代码 D、外来恶意代码

55、在国家标准中，属于强制性标准的是：（B）

A、GB/T XXXX-X-200X B、GB XXXX-200X

C、DBXX/T XXX-200X D、QXXX-XXX-200X

56、在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（A）

A、当信息安全事件的负面影响扩展到本组织意外时

B、只要发生了安全事件就应当公告

C、只有公众的什么财产安全受到巨大危害时才公告

D、当信息安全事件平息之后

57、在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？（A）

A、标准（Standard） B、安全策略（Security policy）

C、方针（Guideline） D、流程(Proecdure)

58、在信息安全管理工作中“符合性”的含义不包括哪一项？（C）

A、对法律法规的符合 B、对安全策略和标准的符合

C、对用户预期服务效果的符合 D、通过审计措施来验证符合情况

59、在许多组织机构中，产生总体安全性问题的主要原因是（A）。

A、缺少安全性管理 B、缺少故障管理

C、缺少风险分析 D、缺少技术控制机制

60、职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（D）

A、数据安全管理员 B、数据安全分析员

C、系统审核员 D、系统程序员

61、中国电信的岗位描述中都应明确包含安全职责，并形成正式文件记录在案，对于安全职责的描述应包括（D）。

A、落实安全政策的常规职责 B、执行具体安全程序或活动的特定职责

C、保护具体资产的特定职责 D、以上都对

62、终端安全管理目标：规范支撑系统中终端用户的行为，降低来自支撑系统终端的安全威胁，重点解决以下哪些问题？（A）。

A、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

B、终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

C、终端接入和配置管理；桌面及主机设置管理；终端防病毒管理

D、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理

63、著名的橘皮书指的是（A）。

A、可信计算机系统评估标准(TCSEC) B、信息安全技术评估标准（ITSEC）

C、美国联邦标准（FC） D、通用准则（CC）

64、资产的敏感性通常怎样进行划分？（C）

A、绝密、机密、敏感 B、机密、秘密、敏感和公开

C、绝密、机密、秘密、敏感和公开等五类

D、绝密、高度机密、秘密、敏感和公开等五类

65、重要系统关键操作操作日志保存时间至少保存（C）个月。

A、1 B、2 C、3 D、4

66、安全基线达标管理办法规定：BSS系统口令设置应遵循的内控要求是（C）

A、数字+字母 B、数字+字母+符号

C、数字+字母+字母大小写 D、数字+符号

67、不属于安全策略所涉及的方面是（D）。

A、物理安全策略 B、访问控制策略

C、信息加密策略 D、防火墙策略

68、“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（C）。

A、“普密”、“商密”两个级别 B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别

D、“一密”、“二密”，“三密”、“四密”四个级别

69、对MBOSS系统所有资产每年至少进行（A）次安全漏洞自评估。

A、1 B、2 C、3 D、4

70、下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（A）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

71、中国电信各省级公司争取在1-3年内实现CTG-MBOSS 系统安全基线“达标”（C）级以上。

A、A级 B、B级 C、C级 D、D级

72、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

73、获取支付结算、证劵交易、期货交易等网络金融服务的身份认证信息（B）组以上的可以被《中华人民共和国刑法》认为是非法获取计算机信息系统系统认定的“情节严重”。

A、5 B、10 C、-15 D、20

74、基准达标项满（B）分作为安全基线达标合格的必要条件。

A、50 B、60 C、70 D、80

75、《国家保密法》对违法人员的量刑标准是（A）。

A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑

B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑

C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑

D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

76、$HOME/.netrc文件包含下列哪种命令的自动登录信息？（C）

A、rsh B、ssh C、ftp D、rlogin

77、/etc/ftpuser文件中出现的账户的意义表示（A）。

A、该账户不可登录ftp B、该账户可以登录ftp C、没有关系 D、缺少

78、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

79、Linux系统/etc目录从功能上看相当于Windows的哪个目录？（B）

A、program files B、Windows C、system volume information D、TEMP

80、Linux系统格式化分区用哪个命令？（A）

A、fdisk B、mv C、mount D、df

81、在Unix系统中，当用ls命令列出文件属性时，如果显示-rwxrwxrwx,意思是（A）。

A、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示其他用户的访问权限

B、前三位rwx表示文件同组用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

C、前三位rwx表示文件同域用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

D、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示同域用户的访问权限

82、Linux系统通过（C）命令给其他用户发消息。

A、less B、mesg C、write D、echo to

83、Linux中，向系统中某个特定用户发送信息，用什么命令？（B）

A、wall B、write C、mesg D、net send

84、防止系统对ping请求做出回应，正确的命令是：（C）。

A、echo 0>/proc/sys/net/ipv4/icmp\_ehco\_ignore\_all

B、echo 0>/proc/sys/net/ipv4/tcp\_syncookies

C、echo 1>/proc/sys/net/ipv4/icmp\_echo\_ignore\_all

D、echo 1>/proc/sys/net/ipv4/tcp\_syncookies

85、NT/2K模型符合哪个安全级别？（B）

A、B2 B、C2 C、B1 D、C1

86、Red Flag Linux指定域名服务器位置的文件是（C）。

A、etc/hosts B、etc/networks C、etc/rosolv.conf D、/.profile

87、Solaris操作系统下，下面哪个命令可以修改/n2kuser/.profile文件的属性为所有用户可读、科协、可执行？（D）

A、chmod 744 /n2kuser/.profile B、 chmod 755 /n2kuser/.profile

C、 chmod 766 /n2kuser/.profile D、 chmod 777 /n2kuser/.profile

88、如何配置，使得用户从服务器A访问服务器B而无需输入密码？（D）

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhost文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/etc/hosts.equiv文件

89、Solaris系统使用什么命令查看已有补丁列表？（C）

A、uname –an B、showrev C、oslevel –r D、swlist –l product ‘PH??’

90、Unix系统中存放每个用户信息的文件是（D）。

A、/sys/passwd B、/sys/password C、/etc/password D、/etc/passwd

91、Unix系统中的账号文件是（A）。

A、/etc/passwd B、/etc/shadow C、/etc/group D、/etc/gshadow

92、Unix系统中如何禁止按Control-Alt-Delete关闭计算机？（B）

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

93、Unix中。可以使用下面哪一个代替Telnet，因为它能完成同样的事情并且更安全？（）

A、S-TELNET B、SSH C、FTP D、RLGON

94、Unix中，默认的共享文件系统在哪个位置？（C）

A、/sbin/ B、/usr/local/ C、/export/ D、/usr/

95、Unix中，哪个目录下运行系统工具，例如sh,cp等？（A）

A、/bin/ B、/lib/ C、/etc/ D、/

96、U盘病毒依赖于哪个文件打到自我运行的目的？（A）

A、autoron.inf B、autoexec.bat C、config.sys D、system.ini

97、Windows nt/2k中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

98、Windows 2000目录服务的基本管理单位是（D）。

A、用户 B、计算机 C、用户组 D、域

99、Windows 2000系统中哪个文件可以查看端口与服务的对应？（D）

A、c:\winnt\system\drivers\etc\services B、c:\winnt\system32\services

C、c:\winnt\system32\config\services D、c:\winnt\system32\drivers\etc\services

100、Windows NT/2000 SAM存放在（D）。

A、WINNT B、WINNT/SYSTEM32

C、WINNT/SYSTEM D、WINNT/SYSTEM32/config

101、 Windows NT/2000中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

102、Windows NT的安全标识（SID）串是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是什么？（C）

A、击键速度 B、用户网络地址 C、处理当前用户模式线程所花费CPU的时间 D、PING的响应时间

103、Windows NT和Windows 2000系统能设置为在几次无效登录后锁定账号，可以防止：（B）。

A、木马 B、暴力破解 C、IP欺骗 D、缓冲区溢出攻击

104、Windows主机推荐使用（A）格式。

A、NTFS B、FAT32 C、FAT D、Linux

105、XP当前的最新补丁是（C）。

A、SP1 B、SP2 C、SP3 D、SP4

106、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

107、当你感觉到你的Win2003运行速度明显减慢，当打开任务管理器后发现CPU使用率达到了100%，你认为你最有可能受到了（D）攻击。

A、缓冲区溢出攻击 B、木马攻击 C、暗门攻击 D、DOS攻击

108、档案权限755，对档案拥有者而言，是什么含义？（A）

A、可读，可执行，可写入 B、可读

C、可读，可执行 D、可写入

109、如何配置，使得用户从服务器A访问服务器B而无需输入密码（D）。

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhosts文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/et/hosts.equiv文件

110、要求关机后不重新启动，shutdown后面参数应该跟（C）。

A、–k B、–r C、-h D、 –c

111、一般来说，通过web运行http服务的子进程时，我们会选择（D）的用户用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

112、以下哪项技术不属于预防病毒技术的范畴？（A）

A、加密可执行程序 B、引导区保护

C、系统监控与读写控制 D、校验文件

113、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？（B）

A、缓冲区溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDos攻击

114、与另一台机器建立IPC$会话连接的命令是（D）。

A、net user [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

B、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$) user:Administrator / passwd:aaa

C、net user \192.168.0.1IPC$ D、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

115、在NT中，如果config.pol已经禁止了对注册表的访问，那么黑客能够绕过这个限制吗？怎样实现？（B）

A、不可以 B、可以通过时间服务来启动注册表编辑器

C、可以通过在本地计算机删除config.pol文件 D、可以通过poledit命令

116、在NT中，怎样使用注册表编辑器来严格限制对注册表的访问？（C）

A、HKEY\_CURRENT\_CONFIG,连接网络注册、登录密码、插入用户ID

B、HKEY\_CURRENT\_MACHINE,浏览用户的轮廓目录，选择NTUser.dat

C、HKEY\_USERS,浏览用户的轮廓目录，选择NTUser.dat

D、HKEY\_USERS,连接网络注册，登录密码，插入用户ID

117、在Solaris 8下，对于/etc/shadow文件中的一行内容如下“root:3vd4NTwk5UnLC:9038::::::”,以下说法正确的是：（E）。

A、这里的3vd4NTwk5UnLC是可逆的加密后的密码

B、这里的9038是指从1970年1月1日到现在的天数

C、这里的9038是指从1980年1月1日到现在的天数

D、这里的9038是指从1980年1月1日到最后一次修改密码的天数

E-以上都不正确

118、在Solaris 8下，对于/etc/shadow文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（A）。

A、是/etc/passwd文件格式 B、是/etc/shadow文件格式

C、既不是/etc/passwd也不是/etc/shadow文件格式

D、这个root用户没有SHELL，不可登录

E、这个用户不可登录，并不是因为没有SHELL

119、在Solaris系统中，终端会话的失败登录尝试记录在下列哪个文件里面?(D)

A、-/etc/default/login B、/etc/nologin

C、/etc/shadow D、var/adm/loginlog

120、在Windows 2000中，以下哪个进程不是基本的系统进程:(D)

A、smss. exe B、csrss. Exe C、winlogon. exe D、-conime.exe

121、在Windows 2000中可以察看开放端口情况的是:(D)。

A、nbtstat B、net C、net show D、netstat

122.、在Windows 2003下netstat的哪个参数可以看到打开该端口的PID?(C)（格式到此）

A、a B、n C、o D 、p

123.、在使用影子口令文件(shadowedpasswords)的Linux系统中，/etc/passwd文件和/etc/shadow文件的正确权限分别是(C)。

A、rw-r-----,-r-------- B、rw-r--r--,-r--r--r—

C、rw-r--r--,-r-------- Drw-r--rw-,-r-----r--

124.、制定数据备份方案时，需要重要考虑的两个因素为适合的备份时间和(B)。

A、备份介质 B、备份的存储位置

C、备份数据量 D、恢复备份的最大允许时间

125.、周期性行为，如扫描，会产生哪种处理器负荷?(A)

A、Idle Ioad B、Usage Ioad C、Traffic load D、以上都不对

126、主要由于(D)原因，使Unix易于移植

A、Unix是由机器指令书写的 B、Unix大部分由汇编少部分用C语言编写

C、Unix是用汇编语言编写的 D、Unix小部分由汇编大部分用C语言编写

127.、HP-UX系统中，使用(A)命令查看系统版本、硬件配置等信息。

A、uname -a B、ifconfig C、netstat D、ps -ef

128.、Linux文件权限一共10位长度，分成四段，第三段表示的内容是(C)。

A、文件类型 B、文件所有者的权限

C、文件所有者所在组的权限 D、其他用户的权限

129、在云计算虚拟化应用中，VXLAN技术处于OS工网络模型中2-3层间，它综合了2层交换的简单性与3层路由的跨域连接性。它是通过在UDP/IP上封装Mac地址而实现这一点的。在简单应用场合，vxLAN可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?(C)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

130.、Linux中，什么命令可以控制口令的存活时间了(A)。

A、chage B、passwd C、chmod D、umask

131.、Qfabric技术是使用市场上现成的计算和存储网元并利用行业标准的网络接口将它们连接后组建大规模的数据中心，以满足未来云计算的要求。该技术概念是哪个厂家主推的概念?(B)

A、惠普 B、uniper C、Cisco与Vmware D、博科Brocade

132、为了检测Windows系统是否有木马入侵，可以先通过()命令来查看当前的活动连接端口。

A、ipconfig B、netstat -rn C、tracert –d D、netstat -an

133、网络营业厅提供相关服务的可用性应不低于（A）。

A、99.99% B、99.9% C、99% D、98.9%

134.、IRF(Intelligent Resilient Framework)是在该厂家所有数据中心交换机中实现的私有技术，是应用在网络设备控制平面的多虚拟技术。该技术属于哪个厂家?(A)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

135.、Windows NT的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:(D)。

A、击键速度 B、当前用户名

C、用户网络地址 D、处理当前用户模式线程所花费CPU的时间

136、脆弱性扫描，可由系统管理员自行进行检查，原则上应不少于(B)。

A、每周一次 B、每月一次 C、每季度一次 D、每半年一次

137、下面哪一个情景属于身份验证(Authentication)过程?(A)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

138、下面哪一个情景属于授权(Authorization)过程?(B)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

139、下列哪一条与操作系统安全配置的原则不符合?(D)

A、关闭没必要的服务 B、不安装多余的组件

C、安装最新的补丁程序 D、开放更多的服务

140、关于DDoS技术，下列哪一项描述是错误的(D)。

A、一些DDoS攻击是利用系统的漏洞进行攻击的

B、黑客攻击前对目标网络进行扫描是发功DDoS攻击的一项主要攻击信息来源

C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的DDoS攻击入侵

D、DDoS攻击不对系统或网络造成任何影响

141、关于PPP协议下列说法正确的是:(C)。

A、PPP协议是物理层协议

B、PPP协议是在HDLC协议的基础上发展起来的

C、PPP协议支持的物理层可以是同步电路或异步电路

D、PPP主要由两类协议组成:链路控制协议族CLCP)和网络安全方面的验证协议族(PAP和CHAP)

142、接口被绑定在2层的zone，这个接口的接口模式是（C）。

A、NAT mode B、Route mode

C、-Transparent mode D、NAT或Route mode

143、接入控制方面，路由器对于接口的要求包括：（D）。

A、串口接入 B、局域网方式接入 C、Internet方式接入 D、VPN接入

144、局域网络标准对应OSI模型的哪几层？（C）。

A、上三层 B、只对应网络层 C、下三层 D、只对应物理层

145、拒绝服务不包括以下哪一项？（D）。

A、DDoS B、畸形报文攻击 C、Land攻击 D、ARP攻击

146、抗DDoS防护设备提供的基本安全防护功能不包括（A）。

A、对主机系统漏洞的补丁升级 B、检测DDoS攻击

C、DDoS攻击警告 D、DDoS攻击防护

147、路由器产品提供完备的安全架构以及相应的安全模块，在软、硬件层面设置重重过滤，保护路由器业务安全。其中不对的说法是：（C）。--》缺少D选项

A、路由器产品支持URPF，可以过滤大多数虚假IP泛洪攻击

B、路由器产品支持CAR功能，可以有效限制泛洪攻击

C、路由器产品不支持ACL配置功能，不能定制过滤规则

D、

148、路由器对于接入权限控制，包括：（D）。

A、根据用户账号划分使用权限 B、根据用户接口划分使用权限

C、禁止使用匿名账号 D、以上都是

149、路由器启动时默认开启了一些服务，有些服务在当前局点里并没有作用，对于这些服务：（C）。缺少D选项

A、就让他开着，也耗费不了多少资源 B、就让他开着，不会有业务去访问

C、必须关闭，防止可能的安全隐患 D、

150、设置Cisco设备的管理员账号时，应（C）。

A、多人共用一个账号 B、多人共用多个账号

C、一人对应单独账号 D、一人对应多个账号

151、什么命令关闭路由器的finger服务？（C）

A、disable finger B、no finger C、no finger service D、no service finger

152、什么是IDS？（A）

A、入侵检测系统 B、入侵防御系统 C、网络审计系统 D、主机扫描系统

153、实现资源内的细粒度授权，边界权限定义为：（B）。

A、账户 B、角色 C、权限 D、操作

154、使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）

A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

155、使用TCP 79端口的服务是：（D）。

A、telnet B、SSH C、Web D、Finger

156、使用一对一或者多对多方式的NAT转换，当所有外部IP地址均被使用后，后续的内网用户如需上网，NAT转换设备会执行什么样的动作？（C）

A、挤掉前一个用户，强制进行NAT转换 B、直接进行路由转发

C、不做NAT转换 D、将报文转移到其他NAT转换设备进行地址转换

157、私网地址用于配置本地网络、下列地址中属于私网地址的是？（C）

A、100.0.0.0 B、172.15.0.0 C、192.168.0.0 D、244.0.0.0

158、随着Internet发展的势头和防火墙的更新，防火墙的哪些功能将被取代。（D）

A、使用IP加密技术 B、日志分析工作

C、攻击检测和报警 D、对访问行为实施静态、固定的控制

159、随着安全要求的提高、技术的演进，（D）应逐步实现物理隔离，或者通过采用相当于物理隔离的技术（如MPLSVPN）实现隔离。

A、局域网 B、广域网及局域网 C、终端 D、广域网

160、通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出现崩溃，请问这种攻击属于何种攻击？（D）

A、拒绝服务（DoS）攻击 B、扫描窥探攻击

C、系统漏洞攻击 D、畸形报文攻击

161、通信领域一般要求3面隔离，即转发面、控制面、用户面实现物理隔离，或者是逻辑隔离，主要目的是在某一面受到攻击的时候，不能影响其他面。路由器的安全架构在实现上就支持：（D）

A、转发面和控制面物理隔离 B、控制面和用户面逻辑隔离

C、转发面和用户面逻辑隔离 D、以上都支持

162、网管人员常用的各种网络工具包括telnet、ftp、ssh等，分别使用的TCP端口号是（B）。

A、21、22、23 B、23、21、22 C、23、22、21 D、21、23、22

163、网络安全工作的目标包括：（D）。

A、信息机密性 B、信息完整性 C、服务可用性 D、以上都是

164、网络安全在多网合一时代的脆弱性体现在（C）。

A、网络的脆弱性 B、软件的脆弱性 C、管理的脆弱性 D、应用的脆弱性

165、应限制Juniper路由器的SSH（A），以防护通过SSH端口的DoS攻击。

A、并发连接数和1分钟内的尝试连接数 B、并发连接数

C、1分钟内的尝试连接数 D、并发连接数和3分钟内的尝试连接数

166、应用网关防火墙的逻辑位置处在OSI中的哪一层？（C）

A、传输层 B、链路层 C、应用层 D、物理层

167、应用网关防火墙在物理形式上表现为？（B）

A、网关 B、堡垒主机 C、路由 D、交换机

168、用来追踪DDoS流量的命令式：（C）

A、ip source-route B、ip cef C、ip source-track D、ip finger

169、用于保护整个网络IPS系统通常不会部署在什么位置？（D）

A、网络边界 B、网络核心 C、边界防火墙内 D、业务终端上

170、用于实现交换机端口镜像的交换机功能是：（D）

A、PERMIT LIST B、PVLAN C、VTP D、SPAN

171、有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（D）。

A、L2TP是由PPTV协议和Cisco公司的L2F组合而成

B、L2TP可用于基于Internet的远程拨号访问

C、为PPP协议的客户建立拨号连接的VPN连接

D、L2TP只能通过TCP/IP连接

172、有关PPTP（Point-to-Point Tunnel Protocol）说法正确的是（C）。

A、PPTP是Netscape提出的 B、微软从NT3.5以后对PPTP开始支持

C、PPTP可用在微软的路由和远程访问服务上 D、它是传输层上的协议

173、有一些应用，如微软Out look或MSN。它们的外观会在转化为基于Web界面的过程中丢失，此时要用到以下哪项技术：（B）

A、Web代理 B、端口转发 C、文件共享 D、网络扩展

174、预防信息篡改的主要方法不包括以下哪一项？（A）

A、使用VPN技术 B、明文加密 C、数据摘要 D、数字签名

175、域名服务系统（DNS）的功能是（A）。

A、完成域名和IP地址之间的转换 B、完成域名和网卡地址之间的转换

C、完成主机名和IP地址之间的转换 D、完成域名和电子邮件地址之间的转换

176、源IP为100.1.1.1，目的IP为100.1.1.255，这个报文属于什么攻击？（B）（假设该网段掩码为255.255.255.0）

A、LAND攻击 B、SMURF攻击 C、FRAGGLE攻击 D、WINNUKE攻击

177、在AH安全协议隧道模式中，新IP头内哪个字段无需进行数据完整性校验？（A）

A、TTL B、源IP地址 C、目的IP地址 D、源IP地址+目的IP地址

178、在C/S环境中，以下哪个是建立一个完整TCP连接的正确顺序？（D）

A、SYN，SYN/ACK，ACK B、Passive Open,Active Open,ACK,ACK

C、SYN,ACK/SYN,ACK D、Active Open/Passive Open,ACK,ACK

179、在L2TP应用场景中，用户的私有地址分配是由以下哪个组建完成？（B）

A、LAC B、LNS C、VPN Client D、用户自行配置

180、在OSI模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（A）

A、应用层 B、物理层 C、会话层 D、网络层

181、在OSI参考模型中有7个层次，提供了相应的安全服务来加强信息系统的安全性。以下哪一层提供了抗抵赖性？（B）

A、表示层 B、应用层 C、传输层 D、数据链路层

182、在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（B）

A、产生日志的数量 B、攻击减少的速度

C、较低的价格 D、假阳性的减少量

183、在安全审计的风险评估阶段，通常是按什么顺序来进行的？（A）

A、侦查阶段、渗透阶段、控制阶段 B、渗透阶段、侦查阶段、控制阶段

C、控制阶段、侦查阶段、渗透阶段 D、侦查阶段、控制阶段、渗透阶段

184、在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（D）

A、IETF 因特网工程工作小组 B、ISO 国际标准组织

C、IANA 因特网地址指派机构 D、OSI 开放系统互联

185、在传输模式IPSec应用情况中，以下哪个区域数据报文可受到加密安全保护？（D）

A、整个数据报文 B、原IP头 C、新IP头 D、传输层及上层数据报文

186、在点到点链路中，OSPF的Hello包发往以下哪个地址？（B）

A、127.0.0.1 B、224.0.0.5 C、233.0.0.1 D、255.255.255.255

187、在建立堡垒主机时，（A）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

188、在进行Sniffer监听时，系统将本地网络接口卡设置成何种侦听模式？（D）

A、unicast单播模式 B、Broadcast广播模式

C、Multicast组播模式 D、Promiscuous混杂模式

189、在零传输（Zone transfers）中DNS服务使用哪个端口？（A）

A、TCP 53 B、UDP 53 C、UDP 23 D、TCP23

190、在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（C）

A、入网访问控制 B、权限控制 C、网络检测控制 D、防火墙控制

191、在思科设备上，若要查看所有访问表的内容，可以使用的命令式（B）

A、show all access-lists B、show access-lists

C、show ip interface D、show interface

192、在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的这是对（A）。

A、可用性的攻击 B、保密性的攻击 C、完整性的攻击 D、真实性的攻击

193、在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（C）

A、报文服务拒绝 B、假冒 C、数据流分析 D、报文服务更改

194、在以下OSI七层模型中，synflooding攻击发生在哪层？（C）

A、数据链路层 B、网络层 C、传输层 D、应用层

195、在以下哪类场景中，移动用户不需要安装额外功能（L2TP）的VPDN软件？（B）

A、基于用户发起的L2TP VPN B、基于NAS发起的L2TP VPN

C、基于LNS发起的L2TP VPN D、以上都是

196、账户口令管理中4A的认证管理的英文单词为：（B）

A、Account B、Authentication C、Authorization D、Audit

197、只具有（A）和FIN标志集的数据包是公认的恶意行为迹象。

A、SYN B、date C、head D、标志位

198、主从账户在4A系统的对应关系包含：（D）

A、1 -N B、1 -1 C、N -1 D、以上全是

199、主动方式FTP服务器要使用的端口包括（A）。

A、TCP 21 TCP 20 B、TCP21 TCP大于1024的端口

C、TCP 20、TCP 大于1024端口 D、都不对

200、下列（D）因素不是影响IP电话语音质量的技术因素。

A、时延 B、抖动 C、回波 D、GK性能

201、下列安全协议中使用包括过滤技术，适合用于可信的LAN到LAN之间的VPN（内部VPN）的是（D）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

202、下列不是抵御DDoS攻击的方法有（D）。

A、加强骨干网设备监控 B、关闭不必要的服务

C、限制同时打开的Syn半连接数目 D、延长Syn半连接的time out时间

203、下列措施不能增强DNS安全的是（C）。

A、使用最新的BIND工具 B、双反向查找

C、更改DNS的端口号 D、不要让HINFO记录被外界看到

204、下列各种安全协议中使用包过滤技术，适合用于可信的LAN到LAN之间的VPN，即内部网VPN的是（）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

205、下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适？（D）

A、回应的比例 B、被动的防御 C、主动的防御 D、都不对

206、下列哪项是私有IP地址？（A）

A、10.5.42.5 B、172.76.42.5 C、172.90.42.5 D、241.16.42.5

207、下列哪一项能够提高网络的可用性？（B）

A、数据冗余 B、链路冗余 C、软件冗余 D、电源冗余

208、下列哪一种攻击方式不属于拒绝服务攻击：（A）。

A、LOphtCrack B、Synflood C、Smurf D、Ping of Death

209、下列哪一项是arp协议的基本功能？（A）

A、通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行

B、对局域网内的其他机器广播路由地址

C、过滤信息，将信息传递个数据链路层 D、将信息传递给网络层

210、最早的计算机网络与传统的通信网络最大的区别是什么？（A）

A、计算机网络采用了分组交换技术 B、计算机网络采用了电路交换技术

C、计算机网络的可靠性大大提高 D、计算机网络带宽和速度大大提高

211、以下哪个属于IPS的功能？（A）

A、检测网络攻击 B、网络流量检测 C、实时异常告警 D、以上都是

212、以下说法错误的是（C）。

A、安全是一个可用性与安全性之间的平衡过程 B、安全的三要素中包含完整性

C、可以做到绝对的安全 D、网络安全是信息安全的子集

213、以下属于4A策略管理模块可以管理的为（C）。

A、访问控制策略 B、信息加密策略 C、密码策略 D、防火墙策略

214、最早研究计算机网络的目的是什么？（B）

A、共享硬盘空间、打印机等设备 B、共享计算资源

C、直接的个人通信 D、大量的数据交换

215、防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为（C）。

A、内容过滤 B、地址转换 C、透明代理 D、内容中转

216、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）。

A、防火墙 B、CA中心 C、加密机 D、防病毒产品

217、网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（D）。

A、多重安全网关 B、防火墙 C、Vlan隔离 D、物理隔离

218、下列哪项不是Tacacs+协议的特性。（A）

A、扩展记账 B、加密整个数据包 C、使用TCP D、支持多协议

219、一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（A）

A、最小特权 B、阻塞点 C、失效保护状态 D、防御多样化

220、包过滤防火墙工作的好坏关键在于？（C）

A、防火墙的质量 B、防火墙的功能 C、防火墙的过滤规则设计 D、防火墙的日志

221、对于日常维护工作，连接路由器的协议通常使用：（B）。缺少D选项

A、TELNET，简单，容易配置 B、SSH &SSHv2 加密算法强劲，安全性好

C、TELNET配置16位长的密码，加密传输，十分安全 D、

222、BOTNET是（C）。

A、普通病毒 B、木马程序 C、僵尸网络 D、蠕虫病毒

223、监听的可能性比较低的是（B）数据链路。

A、Ethernet B、电话线 C、有线电视频道 D、无线电

224、当IPS遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（B）。

A、pass B、bypass C、watchdog D、HA

225、网络环境下的security是指（A）。

A、防黑客入侵，防病毒，窃取和敌对势力攻击

B、网络具有可靠性，可防病毒，窃密和敌对势力攻击

C、网络具有可靠性，容灾性，鲁棒性

D、网络的具有防止敌对势力攻击的能力

226、某一案例中，使用者已将无线AP的SSID广播设置为禁止，并修改了默认SSID值，但仍有未经授权的客户端接入该无线网络，这是因为（D）

A、禁止SSID广播仅在点对点的无线网络中有效

B、未经授权客户端使用了默认SSID接入

C、无线AP开启了DHCP服务

D、封装了SSID的数据包仍然会在无线AP与客户端之间传递

227、为了保护DNS的区域传送（zone transfer），应该配置防火墙以阻止（B）。

1.UDP

2.TCP

3.53

4.52

A、1,3 B、2,3 C、1,4 D、2,4

228、以下不属于代理服务技术优点的是（D）。

A、可以实现身份认证 B、内部地址的屏蔽盒转换功能

C、可以实现访问控制 D、可以防范数据驱动侵袭

229、应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（C）。

A、60% B、70% C、80% D、90%

230、TCP协议与UDP协议相比，TCP是（B），UDP是（）。

A、设置起来麻烦；很好设置 B、容易；困难

C、面向连接的；非连接的 D、不可靠的；可靠的

231、交换机转发以太网的数据基于：（B）。

A、交换机端口号 B、MAC地址 C、IP地址 D、数据类别

232、HTTP，FTP，SMTP建立在OSI模型的哪一层？（D）

A、2层-数据链路层 B、3层-网络层 C、4层-传输层 D、7层-应用层

233、网络安全的基本属性是（D）。

A、机密性 B、可用性 C、完整性 D、以上都是

234、网络安全的主要目的是保护一个组织的信息资产的（A）。

A、机密性、完整性、可用性 B、参照性、可用性、机密性、

C、可用性、完整性、参照性 D、完整性、机密性、参照性

235、DBS是采用了数据库技术的计算机系统。DBS是一个集合体，包含数据库、计算机硬件、软件和（C）。

A、系统分析员 B、程序员 C、数据库管理员 D、操作员

236、MySQL -h host -u user -p password命令的含义如下，哪些事正确的？（D）

A、-h后为host为对方主机名或IP地址 B、-u后为数据库用户名

C、-p后为密码 D、以上都对

237、Oracle当连接远程数据库或其它服务时，可以指定网络服务名，Oracle9i支持5中命名方法，请选择错误的选项。（D）

A、本地命名和目录命名 B、Oracle名称（Oracle Names）

C、主机命名和外部命名 D、DNS和内部命名

238、Oracle的数据库监听器（LISTENER）的默认通讯端口是？（A）

A、TCP 1521 B、TCP 1025 C、TCP 1251 D、TCP 1433

239、Oracle默认的用户名密码为（A）。

A、Scote/tiger B、root C、null D、rootroot

240、Oracle数据库中，物理磁盘资源包括哪些（D）。

A、控制文件 B、重做日志文件 C、数据文件 D、以上都是

241、Oracle中启用审计后，查看审计信息的语句是下面哪一个？（C）

A、select \* from SYS.AUDIT$ B、select \* from syslogins

C、select \* from SYS.AUD$ D、AUDIT SESSION

242、SMTP的端口？（A）

A、25 B、23 C、22 D、21

243、SQL Server的登录账户信息保存在哪个数据库中？（C）

A、model B、msdb C、master D、tempdb

244、SQL Sever的默认DBA账号是什么？（B）

A、administrator B、sa C、root D、SYSTEM

245、SQL Sever的默认通讯端口有哪些？（B）

A、TCP 1025 B、TCP 1433 C、UDP 1434 D、TCP 14333 E、TCP 445

246、SQL Sever中可以使用哪个存储过程调用操作系统命令，添加系统账号？（B）

A、xp\_dirtree B、xp\_cmdshell C、xp\_cmdshell D、xpdeletekey

247、SQL Sever中下面哪个存储过程可以执行系统命令？（C）

A、xp\_regread B、xp\_command C、xp\_cmdshell D、sp\_password

248、SQL的全局约束是指基于元祖的检查子句和（C）。

A、非空值约束 B、域约束子句 C、断言 D、外键子句

249、SQL数据库使用以下哪种组件来保存真实的数据？（C）

A、Schemas B、Subschemas C、Tables D、Views

250、SQL语句中，彻底删除一个表的命令是（B）。

A、delete B、drop C、clear D、remore

251、SQL语言可以（B）在宿主语言中使用，也可以独立地交互式使用。

A、-极速 B、-嵌入 C、-混合 D、-并行

252、SSL安全套接字协议所用的端口是（B）。

A、80 B、443 C、1433 D、3389

253、不属于数据库加密方式的是（D）。

A、库外加密 B、库内加密 C、硬件/软件加密 D、专用加密中间件

254、测试数据库一个月程序主要应对的风险是（B）。

A、非授权用户执行“ROLLBACK”命令 B、非授权用户执行“COMMIT”命令

C、非授权用户执行“ROLLRORWARD”命令 D、非授权用户修改数据库中的行

**255、查看Oracle 8i及更高版本数据库的版本信息的命令是（C）。----缺少CD选项**

**A、cd $Oracle\_HOME/orainst B、C-cd $Oracle\_HIME/orainst C、 D、**

256、从安全的角度来看，运行哪一项起到第一道防线的作用？（C）

A、远端服务器 B、WEB服务器 C、防火墙 D、使用安全shell程序

257、从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（B）。

A、每个分割区G有g=|G|记录，其中g=0或g>=n，且g为偶数，

B、记录必须成对地加入G或从G中删除

C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从m各分割区G1，G2，… …Gm中每一个分割区而来的，则统计信息g（G1VG2V… …VGm）是允许发布

D、记录必须不对地加入G或从G中删除

258、单个用户使用的数据库视图的描述为（A）。

A、外模式 B、概念模式 C、内模式 D、存储模式

259、对于IIS日志记录，推荐使用什么文件格式？（D）

A、Microsoft IIS日志文件格式 B、NCSA公用日志文件格式

C、ODBC日志记录格式 D、W3C扩展日志文件格式

**260、对于IIS日志文件的存放目录，下列哪项设置是最好的？（D）----缺少D选型**

**A、%WinDir%\System32\LogFiles B、C:\Inetpub\wwwroot\LogFiles**

**C、C:\LogFiles..)-F:\LogFiles D、**

261、对于IIS日志文件的访问权限，下列哪些设置是正确的？（D）

A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）

B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）

C、SYSTEM（完全控制）Administrator（完全控制）Inernet来宾账户（读取和运行） D、SYSTEM（完全控制）Administrator（完全控制）

262、对于数据库的描述一下哪项说法是正确的？（A）

A、数据和一系列规则的集合 B、一种存储数据的软件

C、一种存储数据的硬件 D、是存放人量数据的软件

263、攻击者可能利用不必要的extproc外部程序调用功能获取对系统的控制权，威胁系统安全。关闭Extproc功能需要修改TNSNAMES.ORA和LISTENER.ORA文件删除一下条目，其中有一个错误的请选择出来（A）。

A、sys\_ertproc B、icache\_extproc

C、PLSExtproc D、extproc

264、关系数据库中，实现实体之间的联系是通过表与表之间的（D）。

A、公共索引 B、公共存储

C、公共元组 D、公共属性

265、关系型数据库技术的特征由一下哪些元素确定的？（A）

A、行和列 B、节点和分支

C、Blocks和Arrows D、父类和子类

266、关于WEB应用软件系统安全，说法正确的是（D）？

A、Web应用软件的安全性仅仅与WEB应用软件本身的开发有关

B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C、黑客的攻击主要是利用黑客本身发现的新漏洞

D、以任何违反安全规定的方式使用系统都属于入侵

267、目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（D）？

A、数据库系统庞大会提供管理成本 B、数据库系统庞大会降低管理效率

C、数据的集中会降低风险的可控性 D、数据的集中会造成风险的集中

268、哪一个是PKI体系中用以对证书进行访问的协议（B）？

A、SSL B、LDAP C、CA D、IKE

269、如果一个SQL Server数据库维护人员，需要具有建立测试性的数据库的权限，那么应该指派给他哪个权限（A）？

A、Database Creators B、System Administrators

C、Server Administrators D、Security Adiministrators

270、如果以Apache 为WWW服务器，（C）是最重要的配置文件。

A、access.conf B、srm.cong C、httpd.conf D、mime.types

271、若有多个Oracle数据需要进行集中管理，那么对sysdba的管理最好选择哪种认证方式（B）？

A、系统认证 B、password文件认证方式 C、域认证方式 D、以上三种都可

272、数据库管理系统DBMS主要由哪两种部分组成？（A）

A、文件管理器和查询处理器 B、事务处理器和存储管理器

C、存储管理器和查询处理器 D、文件管理器和存储管理器

273、数据库系统与文件系统的最主要区别是（B）。

A、数据库系统复杂，而文件系统简单

B、文件系统不能解决数据冗余和数据独立性问题，而数据库系统可以解决

C、文件系统只能管理程序文件，而数据库系统能够管理各宗类型的文件

D、文件系统管理的数据量较少，而数据库系统可以管理庞大的数据量

274、为了防止电子邮件中的恶意代码，应该由（A）方式阅读电子邮件。

A、纯文本 B、网页 C、程序 D、会话

275、为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机（D）？

A、SMTP身份认证 B、逆向名字解析 C、黑名单过滤 D、内容过滤

276、为什么要对数据库进行“非规范化”处理（B）？

A、确保数据完整性 B、增加处理效率 C、防止数据重复 D、节省存储空间

277、下列不属于WEB安全性测试的范畴的是（A）？

A、数据库内容安全性 B、客户端内容安全性

C、服务器端内容安全性 D、日志功能

278、下列操作中，哪个不是SQL Server服务管理器功能（A）？

A、执行SQL查询命令 B、停止SQL Server 服务

C、暂停SQL Server服务 D、启动SQL Server服务

279、下列关于IIS的安全配置，哪些是不正确的（C）？

A、将网站内容移动到非系统驱动程序 B、重命名IUSR账户

C、禁用所有WEB服务扩展 D、创建应用程序池

280、下列哪些不是广泛使用http服务器？（D）

A、W3C B、Apache C、IIS D、IE

281、下列哪些属于WEB脚本程序编写不当造成的（C）？

A、IIS5.0 Webdav Ntdll.dll远程缓冲区一处漏洞

B、apache可以通过../../../../../../../etc/passwd方位系统文件

C、登陆页面可以用password=’a’or’a’=’a’绕过

D、数据库中的口令信息明文存放

282、下列哪种方法不能有效的防范SQL进入攻击（C）？

A、对来自客户端的输入进行完备的输入检查

B、把SQL语句替换为存储过程、预编译语句或者使用ADO命令对象

C、使用SiteKey技术

D、关掉数据库服务器或者不使用数据库

283、下列哪种工具不是WEB服务器漏洞扫描工具（B）？

A、Nikto B、Web Dumper C、paros Proxy D、Nessus

284、下列哪种攻击不是针对统计数据库的（D）？

A、小查询集合大查询集攻击 B、中值攻击 C、跟踪攻击 D、资源解析攻击

285、下列哪项中是数据库中涉及安全保密的主要问题（A）？

A、访问控制问题 B、数据的准确性问题

C、数据库的完整性问题 D、数据库的安全性问题

286、下列应用服务器中，不遵循J2EE规范的是（C）？

A、MTS B、WebLogic C、Oracle 9iApplication Server D、WebSpere

287、下面关于IIS报错信息含义的描述正确的是（B）？

A、401-找不到文件 B、403-禁止访问 C、404-权限问题 D、500-系统错误

288、下面关于Oracle进程的描述，哪项是错误的（B）？

A、运行在Windows平台上的Oracle能让每个用户组程序化地打开新的进程，这是一个安全隐患

B、在Windows平台，除了Oracle.exe进程外还有其他的独立进程

C、unix平台上有多个独立运行的进程，包括数据写进程、日志写进程、存档进程、系统监控进程、进程监控进程

D、有一个特殊的内存区域被映射为\*nix平台上的所有进程，此区域时系统全局去

289、下面哪一项是与数据库管理员（DBA）职责不相容的（C）？

A、数据管理 B、信息系统管理 C、系统安全 D、信息系统规划

290、下面选型中不属于数据库安全控制的有（D）。

A、信息流控制 B、推论控制 C、访问控制 D、隐通道控制

291、下面选型中不属于数据库安全模型的是（D）。

A、自主型安全模型 B、强制型安全模型 C、基于角色的模型 D、访问控制矩阵

292、一般来说，通过WEB运行http服务的子进程时，我们会选择（D）的用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

293、一下不是数据库的加密技术的是（D）。

A、库外加密 B、库内加密 C、硬件加密 D、固件加密

294、一下对于Oracle文件系统描述错误的是（B）？

A、\*nix下Oracle的可执行文件在$Oracle\_HOME/bin/Oracle,$Oracle\_HOME/bin也应该包含在路径环境变量内

B、Windows下Oracle的可执行文件在%Oracle\_HOME%\bin\Oracle.exe,其他

C、硬件加密 D、固件加密

295、以下几种功能中，哪个是DBMS的控制功能（A）？

A、数据定义 B、数据恢复 C、数据修改 D、数据查询

296、以下哪个安全特征和机制是SQL数据库所特有的（B）？

A、标识和鉴别 B、数据恢复 C、数据修改 D、数据查询

297、以下哪个是数据库管理员（DBA）可以行使的职责（A）？

A、系统容量规划 B、交易管理 C、审计 D、故障承受机制

298、以下哪条命令能利用“SQL注入”漏洞动用XP\_cmdshell存储过程，获得某个子目的清单？（A）

A、http://localhost/script?’:EXEC+master..XP\_cmdshell+’dir’:--

B、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’:--

C、http://localhost/script?0’:EXEC+master..XP\_cmdshell+’ dir’:--

D、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’--

299、以下哪条命令能利用“SQL”漏洞动用XP\_cmdshell存储过程，启动或停止某项服务？（B）

A、http://localhost/script?’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;-

B、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;--

C、http://localhost/script?1’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ; --

D、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ --

300、以下哪项不属于访问控制策略的实施方式？（D）

A、子模式法 B、修改查询法 C、集合法 D、验证法

301、以下哪一项是和电子邮件系统无关的？（）

A、PEM(Privacy enhanced mail) B、PGP(Pretty good privacy)

C、X.500 D、X.400

302、以下哪种方法可以用于对付数据库的统计推论？（C）

A、信息流控制 B、共享资源矩阵 C、查询控制 D、间接存取

303、以下是对层次数据库结构的描述，请选择错误描述的选项。（C）

A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来

B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据

C、它的优点是用户不需要十分熟悉数据库结构

D、层次数据库模型的结构就像是一棵倒转的树

304、以下是对单用户数据库系统的描述，请选择错误描述的选项（C）。

A、单用户数据库系统是一种早期的最简单的数据库系统

B、在单用户系统中，整个数据库系统，包括应用程序、DBMS、数据，都装在一台计算机之间不能共享数据

C、在单用户系统中，由多个用户共用，不同计算机之间能共享数据

D、单用户数据库系统已经不适用于现在的使用，被逐步淘汰了

305、以下是对分布式结构数据库系统的描述，请选择错误描述的选项。（D）

A、分布式结构的数据库系统的数据在逻辑上是一个整体，但物理地分布在计算机网络的不同节点上，每个节点上的主机又带有多个终端用户

B、网络中的每个节点都可以独立的处理数据库中的数据，执行全局应用

C、分布式结构的数据库系统的数据分布存放给数据的处理、管理和维护带来困难

D、分布式结构的数据库系统的数据只在存放在服务器端，其他节点只进行处理和执行

306、以下是对关系数据库结构的描述，请选择错误描述的选项。（D）

A、数据存储的主要载体是表，或相关数据组

B、有一对一、一对多、多对多三种表关系

C、表关联是通过引用完整性定义的，这是通过主码和外码（主键或外键约束条件实现的）

D、缺点是不支持SQL语言

307、以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（A）

A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力

B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行DBMS功能又执行应用程序

C、在网络中把某些节点的计算机专门用于执行DBMS核心功能，这台计算机就成为数据库服务器

D、其他节点上的计算机安装DBMS外围应用开发工具和应用程序，支持用户的应用，称为客户机

308、以下是对面向对象数据库结构的描述，请选择错误描述的选项。（C）

A、它允许用对象的概念来定义与关系数据库交互

B、面向对象数据库中有两个基本的结构：对象和字面量

C、优点是程序员需要掌握与面向对象概念以及关系数据库有关的存储

D、缺点是用户必须理解面向对象概念，目前还没有统一的标准，稳定性还是一个值得关注的焦点

309、以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（D）

A、主从式结构是指一个主机带多个终端的多用户结构

B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上

C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源

D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈

311、在GRUB的配置文件grub.conf中，“timeout=-1”的含义是（C）。

A、不等待用户选择，直接启动默认的系统

B、在10秒钟内，等待用户选择要启动的系统

C、一直等待用户选择要启动的系统

D、无效

312、在Oracle中，quota可以限制用户在某个表空间上最多可使用多少字节，如果要限制data\_ts表500K，以下哪个是正确的命令？（B）

A、quo 500k in data\_ts B、quota 500K on data\_ts

C、quota data\_ts ,imit 500K D、quota data\_ts on 500K

313、在Oracle中，建表约束包括引用完整性约束、check完整性约束，还有以下三项是正确的，请排除一个错误选项。（D）

A、非空完整性约束 B、唯一完整性约束

C、主码完整性约束 D、数据角色性约束

314、在Oracle中，将scott的缺省表空间改为data2\_ts，下列哪个是正确的？（A）

A、ALTER USER scott DEFAULT TABLESPACE data2\_ts

B、ALTER DEFAULT TABLESPACE data2\_ts USER scott

C、ALTER USER scott TABLESPACE DEFAULT data2\_ts D、ALTER scott USER DEFAULT TABLESPACE data2\_ts

315、在Oracle中，将scott的资源文件改为otherprofile，下列哪个是正确的？（C）

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

316、在Oracle中，将当前系统所有角色都授予scott，除Payroll外，下列哪个是正确的？（D）

A、ALTER DEFAULT ROLLE USER　　scott ALL EXCEPT Payroll

B、ALTER USER DEFAULT ROLLE ALL EXCEPT Payroll

C、ALTER DEFAULT ROLLE ALL EXCEPT USER scott

D、ALTER USER scott DEFAULT ROLLE ALL EXCEPT Payroll

317、在Oracle中，用ALTER将scott的口令改为hello，下列哪个是正确的？（A）

A、ALTER USER scott IDENTIFIED BY hello

B、ALTER scott USER IDENTIFIED BY hello

C、ALTER USER scott IDENTIFIED AS hello

D、ALTER USER hello IDENTIFIED BY scott

318、在WEB应用软件的基本结构中，客户端的基础是（A）。

A、HTML文档 B、客户端程序

C、HTML协议 D、浏览器

319、在WEB应用软件的系统测试技术中，下面不属于安全性测试内容的是（C）。

A、客户端的内容安全性 B、服务器的内容安全性

C、数据库的内容安全性 D、Cookie安全性

320、在典型的WEB应用站点的层次结构中，“中间件”是在哪里运行的？（C）

A、浏览器客户端 B、web服务器

C、应用服务器 D、数据库服务器

321、在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（C）

A、对话管理服务 B、事务管理服务

C、资源管理服务 D、控制管理服务

322、主要用于加密机制的协议时（D）。

A、HTTP B、FTP C、TELNETD D、SSL

323、分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？（D）

A、自主性 B、可靠性 C、灵活性 D、数据备份

324、下面对Oracle的密码规则描述，哪个是错误的？（D）

A、Oracle密码必须由英文字母，数值，#，下划线(\_)，美元字符（$）构成，密码的最大长度为30字符，并不能以“$”，“#”，“\_”或任何数字卡头；密码不能包含像“SELECT”，“DELETE”，“CREATE”这类的ORACLE/SQL关键字

B、Oracle的若算法加密机制（）两个相同的用户名和密码在两台不同的ORACLE数据库机器中，将具有相同的哈希值。这些哈希值存储在SYS.USER表中，可以通过像DBA\_USE这类的试图来访问

C、Oracle默认配置下，每个中户如果有10此的失败登录，此账户将会被锁定

D、SYS账户在Oracle数据库中有最高权限，能够做任何事情，包括启动/关闭Oracle数据库，如果SYS被锁定，将不能访问数据库

325、无论是哪一种Web服务器，都会受到HTTP协议本身安全问题的困扰，这样的信息系统安全漏洞属于（C）。

A、设计型漏洞 B、开发型漏洞 C、运行型漏洞 D、以上都不是

326、SSL加密的过程包括以下步骤：（1）通过验证以后，所有数据通过密钥进行加密，使用DEC和RC4加密进行加密；（2）随后客户端随机生成一个对称密钥；（3）信息通过HASH加密，或者一次性加密（MD5SHA）进行完整性确认；（4）客户端和服务器协商建立加密通道的特定算法。正确的顺序的是（D）

A、（4）（3）（1）（2） B、（4）（1）（3）（2） C、（4）（2）（3）（1） D、（4）（2）（3）（1）

327、影响WEB系统安全的因素，不包括？（C）

A、复杂应用系统代码量大、开发人员多、难免出现疏忽

B、系统屡次升级、人员频繁变更，导致代码不一致

C、历史遗留系统、试运行系统等对个WEB系统运行于不同的服务器上

D、开发人员未经安全编码培训

328、Oracle通过修改用户密码策略可提高密码强度，以下哪个密码策略参数中文描述是错误的？（A）

A、PASSWORD\_MAX 登录超过有效次数锁定时间

B、FAILED\_LOGIN\_ATTEMPTS 最大错误登录次数

C、PASSWORD\_GRACE\_TIME 密码失效后锁定时间

D、PASSWORD\_LIFE\_TIME 口令有效时间

329、SQL Server服务有一个启动账号，默认账号是属于administrators组，现在为了安全需要创建一个新的服务启动账号，它需要哪些权限既能兼顾安全又能保证启动数据库成功，请排除一个错误的。（D）

A、数据库本地目录的读写权限 B、启动本地服务的权限

C、读取注册表的权限 D、通过API访问Windows Resource

330、作为一台运行IIS 在Internet发布站点的Windows Web服务器，下面哪项服务不是必需的？（B）

A、IIS Admin B、Net Logon

C、Performance Logs and Alerts D、World Wide Web Publishing

331、数据库中超级账户不能被锁定，其中Oracle的是（），mysql的是（），SQLServer的是（C）。

A、sa，root，sys B、admin，root，sa

C、sys，root，sa D、sys，admin，sa

332，Oracle的安全机制，是由（A）、实体权限和角色权限这三级体系结构组成的。

A、系统权限 B、索引权限 C、操作权限 D、命令控制

333、对SQL数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（B）

A、-- B、- C、-= D、-+

334、在Web页面中增加验证码功能后，下面说法正确的是（A）。

A、可以增加账号破解等自动化软件的攻击难度 B、可以防止文件包含漏洞 C、可以防止缓冲溢出 D、可以防止 浏览

335、以下破解Oracle密码哈希值的步棸，其中哪个描述是错误的？（B）

A、用Sqlplus直接登录到Oracle数据库，使用select username，password form dba\_users命令查看数据库中的用户名和密码，此时看到的密码是哈希值

B、在Cain的Cracker菜单点击导入用户名和哈希值，可直接显示用户密码明文

C、在Cain的Cracker菜单点解导入用户名和哈希值，只能通过字典破解 D、在Cain的Rainbow生成的表会占用大量的硬盘空间和内存，可是破解速度和效率很高

336、在数据库向因特网开放前，哪个步棸是可以忽略的？（B）

A、安全安装和配置操作系统和数据库系统

B、应用系统应该在内网试运行3个月

C、对应用软件如Web也没、ASP脚本等进行安全性检查

D、网络安全策略已经生效

337、如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf文件，查看是否包含如下设置，选出一个正确的（D）。

A、audit=filename B、sys=filename C、event=filename D、log=filename

338、针对一台对外提供Web服务的Windows服务器，下列关于账户权限控制，哪些项是不合理的？（C）

A、限制匿名账户对Web内容的目录写权限

B、从Everyone组中删除“从网络访问此计算机” 用户权限

C、禁用IUSR-MACHE和IWAN\_MACHINE账户

D、本地登录时必须使用Administrators账户

339、网上营业中间件如果启用了SSl，应采用不低于（C）版本的SSL，采用经国家密码管理局认可的密码算法。

A、2.0 B、2.5 C、3.0 D、3.1

340、SQL Server默认的具有DBA权限的账号是什么？（C）

A、root B、admin C、sa D、system

341、（A）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

342、（C）是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

343、《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（B）。

A、GA 163-1997 B、GA 267-2000

C、GA 243-2000 D、GB 17859-1999

344、安装了合格防雷保安器的计算机信息系统，还必须在（C）雷雨季节前对防雷保安器、保护接地装置进行一次年度检查，发现不合格时，应及时修复或更换。

A、第三年 B、第二年 C、每年 D、当年

345、使用IIalon灭火的工作原理是什么？（C）

A、降低温度 B、隔绝氧气和可燃物

C、破坏氧气和可燃物之间的化学反应 D、减少氧气

346、白炽灯、高压汞灯与可燃物、可燃结构之间的距离不应小于（C）cm。

A、30 B、40 C、50 D、60

347、被电击的人能否获救，关键在于（D）。

A、触电的方式 B、人体电阻的大小

C、触电电压的高底 D、能否尽快脱离电源和施行紧急救护

348、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）。

A、可以随意弯折 B、转弯是，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

349、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

350、长期在高频电磁场作用下，操作者会有什么不良反应？（B）

A、呼吸困难 B、神经失常 C、疲劳无力

351、触电事故中，绝大部分是由于（A）导致人身伤亡的。

A、人体接受电流遭到电击 B、烧伤 C、触电休克

352、从业人员发现直接危及人身安全的紧急情况时，例如气体灭火系统开始开启时，应（A）。

A、停止作业，立即撤离危险现场 B、继续作业

C、向上级汇报，等待上级指令

353、从业人员既是安全生产的保护对象，又是实现安全生产的（C）。

A、关键 B、保证 C、基本要素

354、低压验电笔一般适用于交、直流电压未（C）伏以下。

A、220 B、380 C、500

355、电流为（B）毫安是，称为致命电流。

A、50 B、100 C、120 D、150

356、电器的保险丝只能装在（B）上。

A、零线 B、火线 C、底线

357、电器着火是不能用（C）灭火。

A、四氧化碳或1211灭火 B、沙土 C、水

358、对不符合防雷标准、规范防雷工程专业设计方案，以下（B）应当按照审核结论进行修改并重新报批。

A、建设单位 B、防雷工程专业设计单位 C、工程施工单位

359、发现人员触电时，应（B），使之脱离电源。

A、立即用手拉开触电人员 B、用绝缘物体拨开电源或触电者 C、用铁棍拨开电源线

360、凡设在年平均雷电日大于（C）的地区的计算机信息系统，原则上均应装设计算机信息系统防雷保安器，以防止雷电电磁脉冲过电压和过电流侵入计算机信息系统设备。

A、40 B、45 C、5 D、15

361、废电池随处丢弃会造成（B）的污染。

A、白色污染 B、重金属污染 C、酸雨

362、干粉灭火器多长时间检查一次？（A）

A、半年 B、一年 C、三个月 D、两年

363、根据国家相关规定，电压（D）以下不必考虑防止电击的安全？

A、48伏 B、36伏 C、65伏 D、25伏

364、根据作业环境的不同，安全帽的颜色也不同，如在爆炸性作业场所工作宜戴（A）安全帽。

A、红色 B、黄色 C、白色

365、关于空气的正向压力，下面哪项描述是正确的？（B）

A、当门打开时，空气向内流动 B、当门打开，空气向外流动

C、当发生火灾，系统自动切断电源 D、当发生火灾，烟雾向另外一间房间流动

366、国家颁布的《安全色》标准中，表示警告、主要的颜色为（C）。

A、红色 B、蓝色 C、黄色

367、火灾中对人员威胁最大的是（B）。

A、火 B、烟气 C、可燃物

368、机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（B）m。

A、0.1 B、0.6 C、1.2 D、0.3

369、计算机电源系统的所有节点均应镀铅锡处理（B）连接。

A、热压 B、冷压 C、焊锡 D、直接

370、计算机系统接地应采用（A）。

A、专用底线 B、和大楼的钢筋专用网相连

C、大楼的各种金属管道相连 D、没必要

371、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

372、计算机系统应选用（A）电缆。

A、铜芯 B、铅芯

C、铁芯 D、没有要求

373、进行腐蚀品的装卸作业应戴（B）手套。

A、帆布 B、橡胶 C、棉布

374、人体在电磁场作用下，由于（C）将使人体受到不同程度的伤害。

A、电流 B、电压 C、棉布

375、身上着火后，下列哪种灭火方法是错误的（C）。

A、就地打滚 B、用厚重衣物覆盖压灭火苗 C、迎风快跑

376、生产经营单位必须为从业人员提供符合国家标准或（C）标准的劳动防护用品。

A、当地 B、本单位 C、行业

377、使用新设备，必须了解、掌握其安全技术特征，采取有效的安全防护措施，并对从业人员进行专门的安全生产。（B）

A、当地 B、本单位 C、行业

378.实验地点相对湿度大于75%时，则此实验环境属于易触电的环境：（A）

A、危险 B、特别危险 C、一般

379、通过人身的安全交流电流规定在(A)以下。

A、10mA B、30mA C、50mA

380、下列不属于对物理层信息窃取的是(D)

A、对存储介质的盗取 B、对监视器的窃听

C、对网络线路的窃听 D、对设备屏蔽电磁干扰

381、新、改、扩建项目的安全设施投资应当纳入(C)。

A、企业成本 B、安措经费 C、建设项目概算

382、液体表面的蒸汽与空气形成可燃气体，遇到点火源时，发生一闪即灭的现象称为(C)

A、爆炸 B、蒸发 C、闪燃

383、防雷保安器：防止(B)破坏计算机信息系统的保安装置，可分为两大类：电源

线防雷保安器（简称电源防雷保安器）和信号传输线防雷保安器（简称通道防雷保安器）。

A、直击雷 B、感应雷 C、雷暴 D、雷电电磁脉冲

384、EMC标准是为了保证(D)正常工作而制走的。

A、网络 B、媒体 C、信息 D、系统和设备

385、以下不符合防静电要求的是(B)。

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

386、以下哪些属于系统的物理故障？(A)

A、硬件故障与软件故障 B、计算机病毒

C、人为的失误 D、网络故障和设备环境故障

387、用灭火器灭火时，灭火器的喷射口应该对准火焰的(C)。

A、上部 B、中部 C、根部

388、运输、携带、邮寄计算机信息媒体进出靖的，应当如实向(A)申报。

A、海关 B、工商

C、税务 D、边防

389、在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ (B)

A、产生静电 B、计算机部件腐蚀

C、有污染物 D、B+A

390、在空气不流通的狭小地方使用二氧化碳灭火器可能造成的危险是(B)。

A中毒 B缺氧 C爆炸

391、在雷雨天不要走近高压电杆、铁塔、避雷针、远离至少(C)米以外。

A、IO米 B、15米 C、20米

392、在易燃易爆场所穿(C)最危险。

A、布鞋 B、胶鞋 C、带钉鞋

393、在遇到高压电线断落地面时，导线断落点(B)m内，禁止人员进入。

A、IO B、20 C、30

394、数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？(C)

A、30%-40% B、40%-50% C、45%-60% D、50%-70%

395、计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所

以防雷保安器必须有合理的(B)。

A、屏蔽配置 B、接地配置

C、分流配置 D、均压配置

396、计算站场地宜采用(A)蓄电池。

A、封闭式 B、半封闭式

C、开启式 D、普通任意的

397、多层的楼房中，最适合做数据中心的位置是(D)。

A、楼 B、地下室

C、顶楼 D、除以上外的任何楼层

398、计算机机房是安装计算机信息系统主体的关键场所，是(A)工作的重点，所以

对计算机机房要加强安全管理。

A、实体安全保护 B、人员管理

C、媒体安全保护 D、设备安全保护

399、区域安全，首先应考虑（B），用来识别来访问的用户的身份，并对其合法性进行验证，主要通过特殊标示符、口令、指纹等来实现。

A、来访者所持物 B、物理访问控制 C、来访者所具有的特征 D、来访者所知信息

400、在计算机房出入口处或值班室，应设置（D）和应急断电装置。

A、 电视 B、电扇 C、报警器 D、应急电话

401、下列（A）灭火器是扑救精密仪器火灾的最佳选择。

A、二氧化碳灭火剂 B、干粉灭火剂 C、泡沫灭火剂

402、电气安全主要包括人身安全、（B）安全。

A、照明 B、设备 C、电器 D、空调

403、（C）基于IDEA算法。

A、S/MIME B、SET C、PGP D、SSL

404、(C）类型的加密，使得不同的文档和信息进行运算以后得到一个唯一的128位编码。

A、对称加密 B、非对称加密 C、哈希加密 D、强壮加密

405、(C)是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

406、(D)是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。

A、认证机构 B、密码 C、票据 D、数字证书

407、（D）协议主要用于加密机制。

A、HTTP B、FTP C、TELNET D、SSL

408、（A）原则保证只有发送方与接收方能访问消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

409、（D）原则允许某些用户进行特定访问。

A、保密性 B、鉴别 C、完整性 D、访问控制

410、（B）增加明文冗余度。

A、混淆 B、扩散 C、混淆与扩散 D、都不是

411、3DES加密算法的密钥长度是：（A）。

A、168 B、128 C、56 D、256

412、AES密钥长度不能是（D）。

A、128位 B、192位 C、256位 D、512位

413、AES算法是哪种算法？（A）。

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

414、AES属于哪种加密方式？（B）。

A、流加密 B、分组加密 C、异或加密 D、认证加密

415、CA指的是（A）。

A、证书授权 B、加密认证 C、虚拟专用网 D、安全套接层

416、DES经过（A）轮运算后，左右两部分合在一起经过一个末置换，输出一个64位的密文。（A）

A、16 B、8 C、32 D、4

417、DES算法是哪种算法？（A）

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

418、DES属于哪种加密方式？（B）

A、流加密 B、块加密 C、异或加密 D、认证加密

419、DNSSec中并未采用（C）。

A、数字签名技术 B、公钥加密技术 C、地址绑定技术 D、报文摘要技术

420、ECB指的是（D）。

A、密文链接模式 B、密文反馈模式 C、输出反馈模式 D、电码本模式

421、EC-DSA复杂性的程度是（D）。

A、简单 B、最简单 C、困难 D、最困难

422、EFS可以用在什么文件系统下（C）。

A、FAT16 B、FAT32 C、NTFS D、以上都可以

423、IDEA的密钥长度是多少bit？（D）。

A、56 B、64 C、96 D、128

424、Kerberos是80年代中期，麻省理工学院为Athena项目开发的一个认证服务系统，其目标是把认证、记账和（B）的功能扩展到网络环境。

A、访问控制 B、审计 C、授权 D、监控

425、Kerberos是为TCP/IP网络设计的基于（B）的可信第三方鉴别协议，负责在网络上进行仲裁及会话密钥的分配。

A、非对称密钥体系 B、对称密钥体系 C、公钥体系 D、私钥体系

426、Kerberos是一种网络认证协议。它采用的加密算法是（C）。

A、RSA B、PGP C、DES D、MD5

427、Kerberos算法是一个（B）。

A、面向访问的保护系统 B、面向票据的保护系统

C、面向列表的保护系统 D、面向门与锁的保护系统

428、Kerberos提供的最重要的安全服务是？（A）。

A、鉴别 B、机密性 C、完整性 D、可用性

429、MD5产生的散列值是多少位？（C）。

A、56 B、64 C、128 D、160

430、MD5是按每组512位为一组来处理输入的信息，经过一系列变换后，生成一个（B）为散列值。

A、64 B、128 C、256 D、512

431、MD5是以512位分组来处理输入的信息，每一分组又被划分为（A）32位子分组。

A、16个 B、32个 C、64个 D、128个

432、MD5算法将输入信息M按顺序每组（D）长度分组，即：M1，M2，...，Mn-1，Mn。

A、64位 B、128位 C、256位 D、512位

433、PKI（公共密钥基础结构）中应用的加密方式为（B）。

A、对称加密 B、非对称加密 C、HASH加密 D、单向加密

434、PKI的全称是（D）。

A、Private Key Intrusion B、Public Key Intrusion

C、Private Key Infrastructure D、Public Key Infrastructure

435、PKI无法实现（D）。

A、身份认证 B、数据的完整性 C、数据的机密性 D、权限分配

436、RC4是由RIVEST在1987年开发的一种流式的密文，就是实时地把信息加密成一个整体，它在美国一般密钥长度是128位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）。

A、64位 B、56位 C、40位 D、32位

437、RSA公钥加密系统中，他想给她发送一份邮件，并让她知道是他发出，应选用的加密秘钥是（C）。

A、他的公钥 B、她的公钥 C、他的私钥 D、她的私钥

438、RSA使用不方便的最大问题是（A）。

A、产生密钥需要强大的计算能力 B、算法中需要大数

C、算法中需要素数 D、被攻击过很多次

439、RSA算法建立的理论基础是（C）。

A、DES B、替代想组合 C、大数分解和素数检测 D、哈希函数

440、SHA-1产生的散列值是多少位？（D）。

A、56 B、64 C、128 D、160

441、按密钥的使用个数，密码系统可以分为（C）。

A、置换密码系统和易位密码系统 B、分组密码系统和序列密码系统

C、对称密码系统和非对称密码系统 D、密码系统和密码分析系统

442、充分发挥了DES和RSA两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是：（C）。

A、数字签名 B、数字指纹 C、数字信封 D、数字时间戳

443、从技术角度上看数据安全的技术特征主要包含哪几个方面？（B）。

A、数据完整性、数据的方便性、数据的可用性 B、数据的完整性、数据的保密性、数据的可用性 C、数据的稳定性、数据的保密性、数据的可用性 D、数据的方便性、数据的稳定性、数据的完整性

444、单项散列函数的安全性来自于他的（A）。

A、单向性 B、算法复杂性 C、算法的保密性 D、离散性

445、电路网关防火墙工作在OSI协议的哪一层？（A）。

A、传输层 B、链路层 C、应用层 D、物理层

446、电子邮件的机密性与真实性是通过下列哪一项实现的？（A）

A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密

B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密

C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密

D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

447、端对端加密只需要保证消息都在哪里进行加密？（A）

A、源点和目的地节点 B、经过的每一个节点

C、源点和中间经过的每一个节点 D、所有节点

448、对明文字母重新排列，并不隐藏他们的加密方法属于（C）。

A、置换密码 B、分组密码 C、易位密码 D、序列密码

449、对网络中两个相邻节点之间传输的数据进行加密保护的是（A）。

A、节点加密 B、链路加密 C、端到端加密 D、DES加密

450、发送消息和用发送方私钥加密哈希加密信息将确保消息的：（A）。

A、真实性和完整性 B、真实性和隐私 C、隐私和不可否认性 D。隐私和不可否性

451、高级加密标准AES算法中，加密回合数不可能是（D）。

A、10 B、12 C、14 D、16

452、公钥机制利用一对互相匹配的（B）进行加密，解密。

A、私钥 B、密钥 C、数字签名 D、数字证书

453、公钥加密体制中，没有公开的是（A）。

A、明文 B、密文 C、公钥 D、算法

454、公钥证书提供了一种系统的、可扩展的、统一的（A）。

A、公钥分发方案 B、实现不可否认方案

C、对称密钥分发方案 D、保证数据完整性方案

455、关于CA和数字证书的关系，以下说法不正确的是（B）。

A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由CA签发

B、数字证书一般依靠CA中心的对称密钥机制来实现

C、在电子交易中，数字证书可以用于表明参与方的身份

D、数字证书能以一种不能被假冒的方式证明证书持有人身份

456、关于数字签名说法正确的是（A）。

A、数字签名的加密方法以目前的计算机的运算能力来破解是不现实的

B、采用数字签名，不能够保证信息自签发后到收到为止没有做过任何修改（能保证信息收到后没做个任何修改）

C、采用数字签名，能够保证信息是有签名者自己签名发送的，但由于不是真实的签名，签名者容易否认（签名不容易否认）

D、用户可以采用公钥对信息加以处理，形成数字签名（需使用私钥对信息加以处理）

457、基于私有密钥体制的信息认证方法采用的算法是（D）。

A、素数检测 B、非对称算法 C、RSA算法 D、对称加密算法

458、加密技术不能实现（D）。

A、数据信息的完整性 B、基于密码技术的身份认证 C、机密文件加密 D基于IP头信息的包过滤

459、加密技术不能提供以下哪种安全服务？（D）。

A、鉴别 B、机密性 C、完整性 D可用性

460、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）。

A、对称密钥加密 B、非对称密钥加密 C、 D

461、假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（A）。

A、对称加密技术 B、分组加密技术 C、公钥加密技术 D、单项函数密码技术

462、就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。（C）

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

463、利用非对称密钥体制实现加密通信时，若A要向B发送加密信息，则该加密信息应该使用（B）。

A、A的公钥加密 B、B的公钥加密 C、A的私钥加密 D、B的私钥加密

464、利用物理设备将各类型的无法预测的输入集中起来生成随机数的设备是（A）。

A、随机数生成器 B、伪随机数生成器 C、中央处理 D、非易失存储

465、链路加密要求必须先对链路两端的加密设备进行（C）。

A、异步 B、重传 C、同步 D、备份

466、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？（C）

A、对称的公钥算法 B、非对称私钥算法 C、对称密钥算法 D、非对称密钥算法

467、密码分析的目的是什么？（A）

A、确定加密算法的强度 B、增加加密算法的代替功能

C、减少加密算法的换为功能 D、确定所使用的换位

468、请从下列各项中选出不是HASH函数算法的一项。（D）

A、MD5 B、SHA C、HMAC D、MMAC

469、如今，DES加密算法面临的问题是（A）。

A、密钥太短，已经能被现代计算机暴力破解 B、加密算法有漏洞，在数学上已被破解 C、留有后门，可能泄露部分信息 D、算法过于陈旧，已经有更好的替代方案

470、若单项散列函数的输入串有很小的变化，则输出串（A）。

A、可能有很大的变化 B、一定有很大的变化 C、可能有很小的变化 D、一定有很小的变化

471、散列算法可以做哪些事？（C）。

A、碰撞约束 B、入侵检测 C、组合散列 D、随机数生成器

472、身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（B）。

A、可信性 B、访问控制 C、完整性 D、保密性

473、数字签名常用的算法有（B）。

A、DES算法 B、RSA算法 C、Hash函数 D、AES算法

474、数字签名和随机数挑战不能防范以下哪种攻击或恶意行为？（D）。

A、伪装欺骗 B、重放攻击 C、抵赖 D、DOS攻击

475、数字签名可以解决（D）。

A、数据被泄露 B、数据被篡改 C、未经授权擅自访问 D、冒名发送数据或发送后抵赖

476、数字签名通常使用（B）方式。

A、公钥密码体系中的私钥 B、公钥密码系统中的私钥对数字摘要进行加密

C、密钥密码体系 D、公钥密码体系中公钥对数字摘要进行加密

477、数字信封是用来解决（C）。

A、公钥分发问题 B、私钥分发问题 C、对称密钥分发问题 D、数据完整性问题

478、数字证书不包括（B）。

A、签名算法 B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号 D、颁发数字证书单位的数字签名

479、数字证书的应用阶段不包括（D）。

A、证书检索 B、证书验证 C、密钥恢复 D、证书撤销

480、下列说法中错误的是（D）。

A、非对称算法也叫公开密钥算法 B、非对称算法的加密密钥和解密密钥是分离的 C、非对称算法不需要对密钥通信进行保密 D、非对称算法典型的有RSA算法、AES算法等

481、下列算法中，哪种不是对称加密算法？（C）

A、AES B、DES C、RSA D、RC5

482、下列算法中属于Hash算法的是（C）。

A、DES B、IDEA C、SHA D、RSA

483、以下对于链路加密哪项是正确的？（B）

A、消息只在源点加密，目的节点解密 B、消息在源点加密，在每一个经过的节点解密并加密 C、消息在所有经过的节点中都是加密的，但只在目的节点解密 D、消息以明文形式在节点之间传输

484、以下各种加密算法中属于单钥制加密算法的是（A）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密算法

485、以下各种加密算法中属于双钥制加密算法的是（D）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密486、以下各种算法中属于古典加密算法的是（B）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密487、以下关于CA认证中心说法正确的是（C）。

A、CA认证时使用对称密钥机制的认证方法 B、CA认证中心支负责签名，不负责证书的产生 C、CA认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份 D、CA认证中心不用保持中立，可以随便找一个用户来作为CA认证中心

488、以下关于VPN说法正确的是（B）。

A、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B、VPN指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接

C、VPN不能做到信息认证和身份认证 D、VPN只能提供身份认证、不能提供加密数据的功能

489、以下关于数字签名说法正确的是（D）。

A、数字签名是在所传输的数据后附上一段和传输数据毫无关系的数字信息

B、数字签名能够解决数据的加密传输，即安全传输问题

C、数字签名一般采用对称加密机制 D、数字签名能够解决篡改、伪造等安全性问题

490、以下密码使用方法中正确的是（D）。

A、将密码记录在日记本上以避免忘记 B、任何情况下均不得使用临时性密码

C、密码中的字母不得重复 D、不要使用全部由字母组成的密码

491、以下哪个不包含在证书中？（C）

A、密钥采取的算法 B、公钥及其参数 C、私钥及其参数 D、签发证书的CA名称

492、以下哪个选项不会破坏数据库的完整性？（A）

A、对数据库中的数据执行删除操作 B、用户操作过程中出错

C、操作系统的应用程序错误 D、DBMS或操作系统程序出错

493、以下哪项不属于数据库系统实体安全？（B）

A、环境安全 B、线路安全 C、设备安全 D、媒体安全

494、以下哪一种算法产生最长的密钥？（D）

A、Diffe-Hellman B、DES C、IDEA D、RSA

495、以下认证方式中，最为安全的是（D）。

A、用户名+密码 B、卡+密码 C、用户名+密码+验证码 D、卡+指纹

496、远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（B）

A、知道什么 B、拥有什么 C、是谁 D、双因素认证

497、在3DES算法中，密钥最高可达到多少位？（C）

A、96 B、128 C、168 D、200

498、在IPSec中，（C）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的IPSec协议、密码算法、密钥等信息。

A、ESP B、SPI C、SA D、SP

499、在IPSec中，IKE提供（B）方法供两台计算机建立。

A、解释域 B、安全关联 C、安全关系 D、选择关系

500、在RIP的MD5认证报文中，经过加密的密钥是放在哪里的？（B）

A、保温的第一个表项里 B、报文的最后一个表项里

C、报文的第二个表项里 D、报文头里

501、在非对称加密算法中，涉及到的密钥个数是？（B）

A、一个 B、两个 C、三个 D、三个以上

502、在高级加密标准AES算法中，区块大小为（A）。

A、128位 B、192位 C、256位 D、512位

503、在给定的密钥体制中，密钥与密码算法可以看成是（A）。

A、前者是可变的，后者是固定的 B、前者是固定的，后者是可变的

C、两者都是可变的 D、两者都是固定的

504、在公钥体制中，不公开的是（B）。

A、公钥 B、私钥 C、公钥和私钥 D、私钥和加密算法

505、在密码学中，需要被交换的原消息被称为什么？（D）

A、密文 B、算法 C、密码 D、明文

506、一般证书采用哪个标准？（D）

A、ISO/IEC 15408 B、ISO/IEC 17799 C、BS 7799 D、X. 509V3

507、一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（D）

A、信息的数据和时间戳 B、识别发信的计算机

C、对信息内容进行加密 D、对发送者的身份进行识别

508、在数据库中，下列哪些数据不能加密？（A）

A、索引字段 B、存放日期字段

C、存放密码的 D、存放名称字段

509、在一个网络节点中，链路加密仅在以下哪项中提供安全性？（D）

A、数据链路层 B、物理层

C、通信层 D、通信链路

510、在以下隧道协议中，属于三层隧道协议的是（D）。

A、L2F B、PPTP C、L2TP D、IPSec

511、以下哪一项是基于一个大的整数很难分解成两个素数因数？（B）

A、ECC B、RSA C、DES D、D-H

512、以下哪种数据加密技术可以在基础架构层面进行？（A）

A、IPSec B、Secure Sockets Layer

C、Transport Layer Securit D、RSA

513、目前最安全的身份认证机制是（A）。

A、一次口令机制 B、双因素法

C、基于智能卡的用户身价认证 D、身价认证的单因素法

514、当数据库由于各种原因而使其完整性遭到破坏时，必须采取以下哪项措施来恢复数据库？（C）

A、重新安装数据库 B、换一种数据库

C、使用数据库备份 D、将数据库中的数据利用工具导出，并保存

515、PGP加密算法是混合使用（B）算法和IDEA算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES B、RSA C、IDEA D、AES

516、以下哪些软件是用于加密的软件？（A）

A、PGP B、SHA C、EFS D、DES

517、如果消息接受方要确定发送方身价，则要使用（B）原则。

A、保密性 B、鉴别 C、完整性 D、访问控制

518、对于现代密码破解，（D）是最常的方法。

A、攻破算法 B、监听截获 C、信息猜测 D、暴力破解

519、非对称密码技术的缺点有哪些？（B）

A、密钥持有量减少 B、加/解密速度慢 C、耗用资源较少 D、以上都是

520、CA不能提供下列哪种证书？（D）

A、个人数字证书 B、SSL服务器证书

C、安全电子邮件证书 D、SET服务器证书

521、以下关于混合加密方式说法正确的是（B）。

A、采用公开密钥体制进行通信过程中的加解密处理

B、采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C、采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D、采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密

处理速度快的双重优点

522.、果要保证（C）原则，则不能在中途修改消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

523、口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（D）

A、长期没有修改的口令 B、过短的口令

C、两个人共用的口令 D、设备供应商提供的默认的口令

524.非对称密钥的密码技术具有很多优点，其中不包括：（B）。

A、可提供数字签名、零知识证明等额外服务

B、加密/解密速度快，不需占用较多资源

C、通信双方事先不需要通过保密信道交换密钥

D、密钥持有量大大减少

525．DES是一种block（块）密文的加密算法，是把数据加密成多大的块？（B）

A、32位 B、64位 C、128位 D、256位

526．CA数字证书中不包含的信息有（C）。

A、CA的数字签名 B、证书申请者的个人信息

C、证书申请者的私钥 D、证书申请者的公钥信息

527．以下关于对称密钥加密说法正确的是（C）。

A、加密方和解密可以使用不同的算法 B、加密密钥和解密密钥可以是不同的

C、加密密钥和解密密钥必须是相同的 D、密钥的管理非常简单

528、在为计算机设置使用密码时，下面（D）密码是最安全的。

A、12345678 B、66666666

C、20061001 D、72aB@#41

529、（C）的攻击者发生在Web应用层？

A、25% B、50%

C、75% D、90%

530、“U盘破坏者”病毒（Worm.vhy）采用（B）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。

A、网上邻居 B、我的电脑

C、我的文档 D、收藏夹

531、“冲击波”病毒运行时会将自身复制到Windows目录下，并命名为（C）

A、Gsrss.exe B、msbast.exe

C、msblast.exe D、lsass.exe

532、Code Red 爆发于2001年7月，利用微软的IIS漏洞在Web服务器之间传播。针对这一漏洞，微软早在2001年三月就发布了相关的补丁。如果今天服务器仍然感染Code Red，那么属于哪个阶段的问题？（A）

A、系统管理员维护阶段的失误 B、微软公司软件的设计阶段的失误

C、最终用户使用阶段的失误 D、微软公司软件的实现阶段的失误

533、病毒的传播机制主要有哪些？（D）

A、移动存储 B、电子邮件 C、网络共享 D、以上均是

534、病毒的反静态反汇编技术都有（D）。

A、数据压缩 B、数据加密 C、感染代码 D、以上均是

535、病毒在感染计算机系统时，一般（B）感染系统的。

A、病毒程序都会在屏幕上提示，待操作者确认（允许）后

B、实在操作者不觉察的情况下

C、病毒程序会要求操作者制定存储的磁盘和文件夹后

D、在操作者为病毒制定存储的文件名以后

536、杀毒软件时提示“重新启动计算机后删除文件”其主要原因是（A）

A、文件插入了系统关键进程，杀毒时无法处理

B、文件是病毒文件，无法处理

C、由于病毒的加壳形式不同，杀毒时无法正确处理

D、文件正在运行且无法安全的结束，需要其他处理方法

537、蠕虫的目标选择算法有（D）。

A、随机性扫描 B、基于目标列表的扫描

C、顺序扫描 D、以上均是

538、网络钓鱼是指（A）

A、通过大量发送声来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息。

B、网上进行钓鱼活动

C、通过网络组织钓鱼活动，从而获得利益 D、以上都不是

539、不属于常见把入侵主机的信息发送给攻击者的方法是（D）。

A、E-MAIL B、UDP C、ICMP D、连接入侵主机

540、不属于黑客被动攻击的是（A）

A、缓冲区溢出 B、运行恶意软件 C、浏览恶意代码网页 D、打开病毒附件

541、不属于黑客前期收集信息的工具是（D）

A、Nmap B、Xscan C、Nslookup D、LC

542、常见Web攻击方法，不包括？（D）

A、利用服务器配置漏洞 B、恶意代码上传下载

C、构造恶意输入（SQL注入攻击、命令注入攻击、跨站脚本攻击）

D、业务测试

543、常用的抓包软件有（A）。

A、ethereal B、MS office C、fluxay D、netscan

544.网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（A）

A、密码加密后，不会被窃听 B、Cookie字段可以被窃听

C、报文和帧可以窃听 D、高级窃听者还可以进行ARPSpoof，中间人攻击

545、除了在代码设计开发阶段预防SQL注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（C）

A、禁止将任何高权限账号（例如sa,dba等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户

B、拒绝用户访问敏感的系统存储过程

C、禁止用户访问的数据库表 D、限制用户所能够访问的数据库表

546、防止用户被冒名所欺骗的方法是（A）。

A、对信息源发放进行身份验证 B、进行数据加密

C、对访问网络的流量进行过滤和保护 D、采用防火墙

547、给电脑设置多道口令，其中进入电脑的第一道口令是（B）。

A、系统口令 B、CMOS口令

C、文件夹口令 D、文档密码

548、攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息重新发往B称为（D）。

A、中间人攻击 B、口令猜测器和字典攻击

C、强力攻击 D、回放攻击

549、故意制作、传播计算机病毒，造成计算机信息系统不能正常运行，但如果后果不严重就无罪，可以原谅，这种说法（C）。

A、不对，对这种蓄意破坏行为不能原谅 B、即使不是故意的，后果也不很严重

C、对。我国实行成文法，根据《中华人民共和国刑法》第286条的规定，只有造成严重后果者才有罪

D、无法断定

550、关于80年代Mirros蠕虫危害的描述，哪句话是错误的？（B）

A、占用了大量的计算机处理器的时间，导致拒绝股务

B、窃取用户的机密信息，破坏计算机数据文件

C、该蠕虫利用Unix系统上的漏洞传播

D、大量的流量堵塞了网络，导致网络瘫痪

551、关于黑客注入攻击说法错误的是： (D)

A、它的主要原因是程序对用户的输入缺乏过滤

B、一般情况下防火墙对它无法防范

C、对它进行防范时要关注操作系统的版本和安全补丁

D、注入成功后可以获取部分权限

552、基于主机评估报告对主机进行加固时，第一步是（B）。

A、账号、口令策略修改 B、补丁安装

C、文件系统加固 D、日志审核增强

553、计算机病毒会对下列计算机服务造成威胁，除了（C）。

A、完整性 B、有效性

C、保密性 D、可用性

554、计算机病毒是一段可运行的程序，它一般（C）保存在磁盘中。

A、作为一个文件 B、作为一段数据

C、不作为单独文件 D、作为一段资料

555、什么方式能够从远程绕过防火墙去入侵一个网络？(D)

A、IP services\_ B、Active ports

C、Identified network topology D、Modem banks

556、输入法漏洞通过（D）端口实现的。

A、21 B、23 C、445 D、3389

557、特洛伊木马攻击的威胁类型属于（B）。

A、授权侵犯威胁 B、植入威胁

C、渗入威胁 D、旁路控制威胁

558、通常黑客扫描目标机的445端口是为了(B)。

A、利用NETBIOS SMB服务发起DOS攻击

B、发现并获得目标机上的文件及打印机共享

C、利用SMB服务确认Windows系统版本

D、利用NETBIOS服务确认Windows系统版本

559、网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？(A)

A、残余风险评估阶段 B、检查阶段

C、入侵检测系统监控阶段 D、网络异常流量临控阶段

560、网络病毒预防范阶段的主要措施是什么？(A)

A、强制补丁、网络异常流量的发现 B、强制补丁、入侵检测系统监控

C、网络异常流量的发现、入侵检测系统的监控阶段 D、缺少D选项

561、下列除了(B)以外，都是防范计算机病毒侵害的有效方法。

A、使用防病毒软件 B、机房保持卫生，经常进行消毒

C、避免外来的磁盘接触系统 D、网络使用防病毒网关设备

562、下列除了(A)以外，都是计算机病毒传

A、通过操作员接触传播 B、通过U盘接触传播

C、通过网络传播 D、通过电子播的途径邮件传播

563、下列措施中，(C)不是减少病毒的传染

和造成的损失的好办法。

A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B、外来的文件要经过病毒检测才能使用，不要使用盗版软件

C、不与外界进行任何交流，所有软件都自行开发

D、定期用抗病毒软件对系统进行查毒、杀毒

564、下列哪项是跨站脚本Cross Site Scripting攻击具体事例？（B）

A、搜索用户 B、发帖子，发消息 C、上传附件 D、下载文件

565、下列哪项为信息泄露与错误处理不当Information Leakage and Improper

Error Handlina攻击具体实例？(D)

A、不明邮件中隐藏的html链接 B、发帖子，发消息

C、上传附件 D、错误信息揭示路径

566、下面哪一项是黑客用来实施DDoS攻击的工具？(D)

A、LC5 B、Rootkit C、Icesword D、Trinoo

567、以下哪个工具可以抹去所有NT/2K配置，并将其还原到初始状态？(A)

A、Rollback. exe B、Recover. exe C、Zap. exe D、Reset. exe

568、以下哪个工具通常是系统自带任务管理器的替代？(D)

A、Regmon B、Filemon C、Autoruns D、Process explorer

569、以下哪个针对访问控制的安全措施是最容易使用和管理的？(C)

A、密码 B、加密标志 C、硬件加密 D、加密数据文件

570、以下哪项不是分布式拒绝服务攻击常用的工具？(D)

A、Trinoo B、Trinoo C、TFN D、synkill

571、以下哪项不属于针对数据库的攻击？(D)

A、特权提升 B、强力破解弱口令或默认的用户名及口令

C、SQL注入 D、利用xss漏洞攻击

572、以下哪项工具不适合用来做网络监听？(B)

A、sniffer B、Webscan C、 Windump D、 D-Iris

573、以下哪项是SYN变种攻击经常用到的工具？(B)

A、sessionIE B、synkill C、TFN D、Webscan

574、以下哪一项不是流氓软件的特征？(D)

A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装

B、通常添加驱动保护使用户难以卸载

C、通常会启动无用的程序浪费计算机的资源

D、通常会显示下流的言论

575、一个数据仓库中发生了安全性破坏。以下哪一项有助于安全调查的进行？(B)

A、访问路径 B、时戳 C、数据定义 D、数据分类

576、以下哪一项不属于恶意代码？(C)

A、病毒 B、蠕虫 C、宏 D、特洛伊木马

577、以下哪一项不属于计算机病毒的防治策略？(D)

A、防毒能力 B、查毒能力 C、杀毒能力 D、禁毒能力

578、以下哪一项是常见Web站点脆弱性扫描工具？(A)

A、Appscan B、Nmap C、Sniffer D、LC

579、以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？(A)

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将臀陆信息写入记事本

580、以下哪种符号在SQL注入攻击中经常用到？(D)

A、$\_ B、1 C、@ D、;

581、以下哪种工具能从网络上检测出网络监听软件(A)

A、sniffdet, , B、purify, , C、Dsniff D、WireShark

582、以下哪种攻击可能导致某些系统在重组IP分片的过程中宕机或者重新启动？(B)

A、分布式拒绝服务攻击 B、Ping of Death

C、NFS攻击 D、DNS缓存毒化攻击

583、下面哪部分不属于入侵的过程？(B)

A、数据采集 B、数据存储 C、数据检测 D、数据分析

584、以下对木马阐述不正确的是(A)。

A、木马可以自我复制和传播

B、有些木马可以查看目标主机的屏幕

C、有些木马可以对目标主机上的文件进行任意揉作

D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。

585、由于攻击者可以借助某种手段，避开DBMS以及应用程序而直接进入系统访问

数据，我们通常采取以下哪种方式来防范？(A)

A、数据库加密

B、修改数据库用户的密码，将之改得更为复杂

C、使用修改查询法，使用户在查询数据库时需要满足更多的条件

D、使用集合法

586、在大多数情况下，病毒侵入计算机系统以后，(D)。

A、病毒程序将立即破坏整个计算机软件系统

B、计算机系统将立即不能执行我们的各项任务

C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

587、在确定威胁的可能性时，可以不考虑以下哪项？(D)

A、威胁源 B、潜在弱点

C、现有控制措施 D、攻击所产生的负面影响

588、在以下人为的恶意攻击行为中，属于主动攻击的是(A)。

A、身份假冒 B、数据GG C、数据流分析 D、非法访问

589、下面哪一种攻击方式最常用于破解口 令？(B)

A、哄骗( spoofing) B、字典攻击(dictionary attack)

C、拒绝服务(DoS) D、WinNuk

590、针对DNS服务器发起的查询DoS攻击，属于下列哪种攻击类型？(C)

A、syn flood B、ack flood C、 udpflood D、Connection flood

591、下列哪项不是安全编码中输入验证的控制项？(D)

A、数字型的输入必须是合法的数字

B、字符型的输入中对’进行特殊处理

C、验证所有的输入点，包括Get，Post，Cookie以及其他HTTP头

D、正确使用静态查询语句，如PreDaredStatement

592、以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？(C)

A、早期的SMTP协议没有发件人认证的功能

B、网络上存在大量开放式的邮件中转服务器，导致垃圾邮件的来源难于追查

C、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因

D、Internet分布式管理的性质，导致很难控制和管理

593、以下哪种方法是防止便携式计算机机密信息泄露的最有效方法？（A）

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将登录信息写入记事本

594、以下哪种攻击属于DDoS类攻击？（A）

A、SYN变种攻击 B、smurf攻击 C、arp攻击 D、Fraggle攻击

595、URL访问控制不当不包括（D）

A、Web应用对页面权限控制不严 B、缺乏统一规范的权限控制框架

C、部分页面可以直接从URL中访问 D、使用分散登录认证

596、Web应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（A）

A、静态密码 B、短信挑战 C、指纹认证 D、图片认证

597、Web应用漏洞按类别进行排名，由多到少正确的顺序为？（A）

A、跨站脚本、注入、恶意代码、引用不当

B、注入、跨站脚本、恶意代码、引用不当

C、恶意代码、跨站脚本、注入、引用不当

D、引用不当、跨站脚本、注入、恶意代码

598、从技术角度，以下不是漏洞来源的是（D）

A、软件或协议设计时候的瑕疵 B、软件或协议实现中的弱点

C、软件本身的瑕疵 D、显示卡内存容量过低

599、（C）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A、身份假冒 B、数据篡改 C、信息窃取 D、越权访问

600、有关密码学分支的定义，下列说法中错误的是（D）

A、密码学是研究信息系统安全保密的科学，由两个相互对立、相互斗争、而且又相辅相成、相互渗透的分支科学所组成的、分别称为密码编码学和密码分析学

B、密码编码学是对密码体制、密码体制的输入输出关系进行分析、以便推出机密变量、包括明文在内的敏感数据

C、密码分析学主要研究加密信息的破译或信息的伪造

D、密码编码学主要研究对信息进行编码，实现信息的隐藏

601、与RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（C）

A、数字签名 B、鉴别机制 C、加密机制 D、数据完整性

602、以下哪项是数据库加密方法中的库外加密的缺点？（A）

A、即使访问一条数据也要对整个数据库解密 B、密钥管理比较复杂

C、加密之后不能完整的查询数据 D、密钥过于简单，容易被破解

603、以下哪项数据中涉及安全保密的最主要问题？（A）

A、访问控制问题 B、数据完整性 C、数据正确性 D、数据安全性

604、以下哪一个最好的描述了数字证书？（A）

A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，它使得黑客不能得知用户的身份

C、网站要求用户使用用户名和密码登陆的安全机制

D、伴随在线交易证明购买的收据

605、TCP SYN Flood网络攻击时利用了TCP建立连接过程需要（C）次握手的特点而完成对目标进行攻击的。

A、1 B、2 C、3 D、6

二、多项选择题（606-789）

606、COBIT度量过程的三个纬度分别是（ABC）。

A、能力 B、绩效 C、控制度 D、能力成熟度

607、IT系统内网与互联网连接检查手段有哪些？（BCD）

A、工具扫描 B、人员访谈 C、人工检查 D、文档检查

608、公司应该采取以下措施，对第三方访问进行控制。（ABCD）

A、公司应于第三发公司法人签署保密协议，并要求其第三方个人签署保密承诺，此项工作应在第三方获得网络与信息资产的访问权限之前完成

B、实行访问授权管理，未经授权，第三方不得进行任何形式的访问

C、公司应加强第三方访问的过程控制，监督其活动及操作，对其进行适当的安全宣传与培训

D、第三方人员应佩戴易于识别的标志，并在访问公司重要场所时有专人陪同

609、计算机信息系统安全的三个相辅相成，互补互通的有机组成部分是（ABD）

A、安全策略 B、安全法规 C、安全技术 D、安全管理

610、劳动合同中应包含网络与信息安全条款，这些条款规定（ACD）。

A、员工的安全责任和违约罚则

B、安全责任不可延伸至公司场所以外和正常工作时间以外

C、安全责任可延伸至公司场所以外和正常工作时间以外

D、如必要，一些安全责任应在雇佣结束后延续一段特定的时间

611、审核是网络安全工作的核心，下列应用属于主动审核的是：（CD）

A、Windows事件日志记录 B、数据库的事务日志记录

C、防火墙对访问站点的过滤 D、系统对非法链接的拒绝

612、通用准则CC实现的目标有（ABC）

A、成为统一的国际通用安全产品、系统的安全标准

B、在不同国家达成协议，相互承认产品安全等级评估

C、概述IT产品的国际通用性 D、都不是

613、系统用户账号登记表应包括（ABCD）。

A、使用者姓名、部门、职务、联系电话 B、账号权限

C、批准人、开通人 D、开通时间、到期日

614、下列情况哪些是对公司经营管理的影响为“一般”级别的互联网网络安全事件？（ABD）

A、发生未到达“预警”的一般性安全事件

B、出现新的漏洞，尚未发现利用方法或利用迹象

C、有来自境外的网络性能明显下降的报警，并且其技术原因普遍适用于我国互联网 D、出现新的蠕虫/病毒或其它恶意代码，尚未证明可能造成严重危害

615、信息安全的主要原则有（BCD）

A、认证性 B、保密性 C、可用性 D、完整性

**616、针对支撑系统，除业务关联性、对业务网络的影响，资产价值主要体现在（ACD）几个方面。 缺少D选项**

**A、业务收益的影响 B、设备购买成本 C、面向客户的重要程度 D、**

617、IT系统病毒泛滥的主要原因有哪些？（ABCD）

A、主机和终端防病毒软件缺乏统一管理

B、主机和终端防病毒软件没有设置为自动更新或更新周期较长

C、防病毒服务器没有及时更新放病毒库

D、缺乏防病毒应急处理流程和方案

618、IT系统病毒防护评估检查对象包括哪些内容？（ABCD）

A、防病毒服务器 B、重要应用Windows主机

C、Windows终端 D、主机管理员

619、互联网连接防火墙设备的安全策略配置要求包括哪几点（ABCD）。

A、远程登录是否禁止telnet方式 B、最后一条策略是否是拒绝一切流量

C、是否存在允许any to any的策略

D、是否设置了管理IP，设备只能从管理IP登录维护

620、《安全基线标准》在安全管理层面主要围绕哪几部分考评安全基线？（ABC）

A、组织架构管理 B、人员安全管理 C、运维安全管理 D、制度安全管理

621、IT系统维护人员权限原则包括（ACD）。

A、工作相关 B、最大授权 C、最小授权 D、权限制约

622、安全系统加固手册中关于造成系统异常中断的各方面因素，主要包括哪三方面（ABD）

A、人为原因 B、环境原因 C、生产原因 D、设备原因

623、IT系统维护人员权限原则包括（ACD）

A、工作相关 B、最大授权 C、最小授权 D、权限制约

624、计算当前Linux系统中所有用户的数量，可以使用（ABC）命令

A、wc -l /etc/passwd B、wc -l</etc/passwd

C、cat/etc/passwd|wc -l D、cat/etc/passwd>wc -l

625、Solarid系统中，攻击者在系统中增加账户会改变哪些文件？（AB）

A、shadow B、passwd C、inetd,conf D、hosts

626、Syn Flood攻击的现象有以下哪些？（ABC）

A、大量连接处于SYN\_RCVD状态 B、正常网络访问受阻

C、系统资源使用率高

627、UNIX安全审计的主要技术手段有哪些？（ABCDEF）

A、文件完整性审计 B、用户、弱口令审计 C、安全补丁审计

D、端口审计 E、进程审计 F、系统日志审计

628、Unix系统提供备份工具有（ABCD）

A、cp：可以完成把某一目录内容拷贝到另一目录

B、tar：可以创建、把文件添加到或从一个tar档案中解开文件

C、cpio：把文件拷贝进或拷贝出一个cpio档案或tar档案

D、dump：用来恢复整个文件系统或提取单个文件

629、操作系统应利用安全工具提供以下哪些访问控制功能？（ABC）

A、验证用户身份，必要的话，还应进行终端或物理地点识别

B、记录所有系统访问日志

C、必要时，应能限制用户连接时间 D、都不对

630、从哪些地方可以看到遗留痕迹？（ABCD）

A、回收站 B、最近使用过的文件 C、注册表 D、文件最后更改的时间戳631、

632、关于Windows活动目录说法正确的是（ABD）。

A、活动目录是采用分层结构来存储网络对象信息的一种网络管理体系

B、活动目录可以提供存储目录数据和网络用户级管理员使用这些数据的方法

C、利用活动目录来实现域内计算机的分布式管理

D、活动目录与域紧密结合构成与目录林和域目录树，使大型网络中庞大、复杂的网络管理、控制、访问变得简单，使网络管理效率更高

633、建立堡垒主机的一般原则是（AC）。

A、最简化原则 B、复杂化原则 C、预防原则 D、网络隔离原则

634、逻辑空间主要包括哪些部分？（ABDE）

A、TABLESPACES B、SEGMENTS C、DATAFILE

D、EXTENTS E、BLOCK

635、哪些属于Windows日志？（ABCD）

A、AppEvent.Evt B、SecEvent.Evt C、SysEvent.Evt D、W3C扩展日志

636、如何设置listener口令？（ACDE）

A、以Oracle用户运行lsnrctl命令 B、set log\_file

C、change\_password D、set password E、save\_config

637、审计启动其日志有哪两种存放方式？（BD）

A、NONE B、OS C、TRUE D、SYS.AUD$

638、生产服务器通常都是UNIX平台，资产价值最高，不直接连接外部网络，主要的安全需求是（ABD）

A、访问控制 B、账号口令 C、数据过滤 D、权限管理和补丁管理

639、使用md5sum工具对文件签名，以下说法正确的是？（ADE）

A、md5sum对任何签名结果是定长的16字节

B、md5sum对文件签名具有不可抵赖性

C、md5sum是对文件进行加密运算得出签名，不同文件结果几乎不相同

D、md5sum是对文件进行哈希运算得出签名，不同文件结果几乎不相同

E、md5sum对文件签名时，与文件的日期和时间无关

640、为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有（ABCD）

A、口令/账号加密 B、定期更换口令

C、限制对口令文件的访问 D、设置复杂的、具有一定位数的口令

641、文件系统是构成Linux基础，Linux中常用文件系统有（ABD）？

A、ext3 B、ext2 C、hfs D、reiserfs

642、下列关于UNIX下日志说法正确的是（AC）

A、wtmp记录每一次用户登录和注销的历史信息

B、acct记录每个用户使用过的命令

C、sulog记录su命令的使用情况

D、acct记录当前登录的每个用户

643、下列哪些操作可以看到自启动项目？（ABD）

A、注册表 B、开始菜单 C、任务管理器 D、msconfig

644、下列哪些命令行可用于查看当前进程？（ABC）

A、Ps -ef B、Strings -f/proc/[0-9]\*/cmdline

C、Ls -al /proc/[0-9]\*/exe D、Cat/etc/inetd.conf

645、下面操作系统中，哪些是UNIX操作系统？（CD）

A、Red-hat Linux B、Novell Netware C、Free BSD D、SCO Unix

646、严格的口令策略应当包含哪些要素（ABC）

A、满足一定的长度，比如8位以上 B、同时包含数字，字母和特殊字符

C、系统强制要求定期更改口令 D、用户可以设置空口令

647、在Solaris 8 下，使用ps -ef命令列出进程中有一行如下“root 1331 0 00:01:00? 0:00 /usr/sbin/inetd -s -t”，以下说法正确的是（ABE）

A、参数-t是trace，记录包括IP和PORT等信息

B、参数-t对于UDP服务无效 C、进程启动的时间不能确定

D、进程已经运行了1分钟 E、进程的父进程号是1

648、在Solaris 8 下，以下说法正确的是：（AB）

A、/etc/rc2.d里S开头的文件在系统缺省安装的缺省级别会自动运行

B、/etc/rc3.d里S开头的文件在系统缺省安装的缺省级别会自动运行

C、/etc/init.d里的文件在系统启动任何级别时会自动运行

D、init 0是进入单用户级别 E、init 6命令会运行所有级别的rc目录下以S开头的文件

649、在Solaris 8 下，以下说法正确的是：（BC）

A、PATH环境变量最后带有“.”，会使当前目录的命令比其他目录的命令有限执行

B、可以修改/etc/inittab里ttymon的参数，使得登录的SHELL在无输入时自动退出

C、在使用/bin/ksh时，可以设置TMOUT值，使得登录的SHELL在无输入时自动退出

D、在/etc/login中，可以设置TIMEOUT值，使得登录的SHELL在无输入时自动退出

E、tar xvf命令的意思是以tar格式解开输入，并且保持文件属性等参数不变

650、在配置Apache访问控制时，Allow和Deny指令可以允许或拒绝来自特定主机名或主机名地址的访问。那么下列哪些配置是不正确的？（AD）

A、Order allow,deny Allow from 192.101.205

B、B、Order deny,allow Deny from all Allow from example

C、C、Order deny,allow Deny from 192.101.205

D、D、Order allow,deny Deny from 192.101.205 Allow from all

651、造成操作系统安全漏洞的原因是（ABC）。

A、不安全的编程语言 B、不安全的编程习惯

C、考虑不周的架构设计 D、人为的恶意破坏

652、针对Linux主机，一般的加固手段包括（ABC）。

A、打补丁 B、关闭不必要的服务 C、限制访问主机 D、切断网络

653、做系统快照，查看端口信息的方式有（AD）。

A、netstat -an B、net share C、net use D、用taskinfo来查看连接情况

654、网厅安全解决方案主要从哪几个方面对网厅安全进行建议和指导？（ABCD）

A、安全管理 B、安全防护 C、安全运维 D、灾备/恢复

655、IT系统软件设计中应当考虑并执行安全审计功能，详细记录访问信息的活动，包括（ABCD）。

A、记录的活动以是否有数据的修改、应用程序的异常关闭、异常删除触发

B、应用系统应当配置单独的审计数据库，审计记录应单独存放，并设置严格的边界访问控制，只有安全管理人员才能够看到审计记录

C、信息系统的审计功能包括：事件日期、时间、发起者信息、类型、描述和结果

D、应用系统的审计进程为后台处理，与应用系统运行同步进行，并且对于审计进程应当涉及相应的守护进程，一旦出现异常停止系统可重新启动审计进程，从而保障审计的“完整性”

656、IPSec的配置步骤包括：（ABCD）

A、防火墙基本配置 B、定义保护数据流和域间规则

C、配置IPSec安全提议 D、配置IKEPeer

657、Juniper路由器在配置SSH访问时应注意如下（ABCD）细节。

A、建立允许访问的SSH-ADDRESSES过滤器

B、确保只允许来自内部接口的授权用户访问

C、针对SSH进行限速以保护路由引擎

D、过滤器应用在loopback接口

658、对于使用RPF反向地址验证，以下说法错误的是：（BCD）。

A、对称路由可以使用 B、非对称路由可以使用

C、有些情况不可以使用，但与对称或非对称路由无关

D、在任何情况下都可以使用

659、防病毒服务升级检查包括如下几项内容？（ABC）

A、检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决

B、在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本

C、对重要的服务器，定期抽查防病毒客户端的病毒库升级情况

660、防范DOS攻击的方法主要有（ABCD）。

A、安装Dos检测系统 B、对黑洞路由表里的地址进行过滤

C、及时打好补丁 D、正确配置TCP/IP参数

661、防火墙trust域中的客户机通过nat访问untrust中的服务器的ftp服务，已经允许客户机访问服务器的tcp21端口，但只能登陆到服务器，却无法下载文件，以下解决办法中可能的是：（ABC）

A、修改trust untrust域间双向的默认访问策略为允许

B、FTP工作方式为port模式时，修改untrust trust域间in方向的默认访问策略为允许 C、在trust untrust域间配置中启用detect ftp

D、FTP工作方式为passive模式时，修改untrust trust域间in方向的默认访问策略为允许

662、防火墙不能防止以下哪些攻击？（ABD）

A、内部网络用户的攻击 B、传送已感染病毒的软件和文件

C、外部网络用户的IP地址欺骗 D、数据驱动型的攻击

663、防火墙常见的集中工作模式有（ABC）。

A、路由 B、NAT C、透明 D、旁路

664、防火墙的缺陷主要有（ABCD）。

A、限制有用的网络服务 B、无法防护内部网络用户的攻击

C、不能防备新的网络安全问题 D、不能完全防止传送已感染病毒的软件或文件

665、防火墙的日志管理应遵循如下原则：（BC）

A、本地保存日志 B、本地保存日志并把日志保存到日志服务器上

C、保持时钟的同步 D、在日志服务器保存日志

666、防火墙的特征是（ABCD）。

A、保护脆弱和有缺陷的网络服务 B、加强对网络系统的访问控制

C、加强隐私，隐藏内部网络结构 D、对网络存取和访问进行监控审计

667、防火墙的主要功能有哪些？（ABCD）

A、过滤进、出网络的数据 B、管理进、出网络的访问行为

C、封堵某些禁止的业务，对网络攻击进行检测和报警

D、记录通过防火墙的信息内容和活动

668、防火墙的作用主要有（ABCD）。

A、实现一个公司的安全策略 B、创建一个阻塞点

C、记录Internet活动 D、限制网络暴露

669、防火墙技术，涉及到（ABCD）。

A、计算机网络技术 B、密码技术 C、软件技术 D、安全操作系统

670、防火墙可以部署在下列位置：（ABCD）。

A、安全域边界 B、服务器区域边界

C、可信网络区域和不可信网络区域之间 D、根据网络特点设计方案

671、防火墙配置时应确保（ABCD）服务不开放。

A、Rlogin B、NNTP C、Finger D、NFS

672、启用Cisco设备的访问控制列表，可以起到如下作用（ABC）。

A、过滤恶意和垃圾路由信息 B、控制网络的垃圾信息流

C、控制未授权的远程访问 D、防止DDoS攻击

673、如果Cisco设备的VTY需要远程访问，则需要配置（ABCD）。

A、至少8位含数字、大小写、特写字符的密码 B、远程连接的并发数目

C、访问控制列表 D、超市退出

674、如果需要配置Cisco路由器禁止从网络启动和自动从网络下载初始配置文件，配置命令包括（AB）。

A、no boot network B、no service config C、no boot config D、no service network

675、入侵检测的内容主要包括：（BC）。

A、独占资源、恶意使用 B、试图闯入或成功闯入、冒充其他用户

C、安全审计 D、违反安全策略、合法用户的泄露

676、入侵检测系统包括以下哪些类型？（AC）

A、主机入侵检测系统 B、链路状态入侵检测系统

C、网络入侵检测系统 D、数据包过滤入侵检测系统

677、随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器（sniffer）来监听整个子网的办法不再可行。可选择解决的办法有（ABCD）。

A、使用交换机的核心芯片上的一个调试的端口

B、把入侵检测系统放在交换机内部或防火墙等数据流的关键入口

C、采用分解器（tap）

D、使用以透明网桥模式接入的入侵检测系统

678、通常要求把路由器的日志存储在专用日志服务器上，假设把Cisco路由器日志存储在192.168.0.100的syslog服务器上，需要在路由器侧配置的操作时：（ABCD）。

A、使用Router(config)# logging on启用日志：使用Router(config)# logging trap information将记录日志级别设定为“information”

B、使用Routee(config)# logging192.168.0.100将记录日志类型设定为“local6”

C、使用(config)# logging facility local6将日志发送到192.168.0.100

D、使用(config)# logging sourceinterface loopback0设定日志发送源loopback0

679、通过SSL VPN接入企业内部的应用，其优势体现在哪些方面：（ABCD）。

A、应用代理 B、穿越NAT和防火墙设备

C、完善的资源访问控制 D、抵御外部攻击

680、网络地址端口转换（NAPT）与普通地址转换有什么区别？（AD）

A、经过NAPT转换后，对于外网用户，所有报文都来自于同一个IP地址

B、NAT只支持应用层的协议地址转换

C、NAPT只支持网络层的协议地址转换

D、NAT支持网络层的协议地址转换

681、网络攻击的类型包括以下哪几种？（ABCD）

A、窃取口令 B、系统漏洞和后门 C、协议缺陷 D、拒绝服务

682、网络面临的典型威胁包括（ABCD）。

A、未经授权的访问 B、信息在传送过程中被截获、篡改

C、黑客攻击 D、滥用和误用

683、网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，该类病毒程序大规模爆发后，会对相关网络造成拒绝服务攻击，为了防止受到网络蠕虫的侵害，应当注意对（ACD）及时进行升级更新。

A、计算机操作系统 B、计算机硬件 C、文字处理软件 D、应用软件

684、下列关于NAT地址转换的说法中哪些事正确的：（ABCD）。

A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

B、地址转换可以按照用户的需要，在局域网内向外提供FTP、WWW、Telnet等服务

C、有些应用层协议在数据中携带IP地址信息，对它们作NAT时还要修改上层数据中的IP地址信息

D、对于某些非TCP、UDP的协议（如ICMP、PPTP），作上层NAT时，会对它们的特征参数（如ICMP的id参数）进行转换。

685、下列哪两项正确描述了由WPA定义的无线安全标准？（BC）

A、使用公开密钥的认证方法 B、当客户端连接的时候都要进行动态密钥交换

C、包含PSK认证 D、定制了一个经常更换的静态的加密密钥来增强安全性

686、下列配置中，可以增强无线AP（access point）安全性的有（ABCD）。

A、禁止SSID广播 B、禁用DHCP服务

C、采用WPA2-PSK加密认证 D、启用MAC地址接入过滤

687、下面可以攻击状态检测的防火墙方法有：（ABD）

A、协议隧道攻击 B、利用FTP-pasv绕过防火墙认证的攻击

C、ip欺骗攻击 D、反弹木马攻击

688、下面什么路由协议不可以为HSRP的扩充：（ABC）

A、SNMP B、CDP C、HTTP D、VRRP

689、下面什么协议有MD5认证：（ABC）

A、BGP B、OSPF C、EIGER D、RIPversion 1

690、下面是网络安全技术的有：（ABC）

A、防火墙 B、防病毒 C、PKI D、UPS

691、选购一个防火墙时应该考虑的因素有：（ABCD）

A、网络受威胁的程度 B、可能受到的潜在损失

C、站点是否有经验丰富的管理员 D、未来扩展的需要

692、一台路由器的安全快照需要保存如下哪些信息？（AB）

A、当前的配置--running-config B、当前的开放端口列表

C、当前的路由表 D、当前的CPU状态

693、以下对于包过滤防火墙的描述正确的有（ACD）。

A、难以防范黑客攻击 B、处理速度非常慢

C、不支持应用层协议 D、不能处理新的安全威胁

694、以下对于代理防火墙的描述正确的有（ABCD）。

A、能够理解应用层上的协议 B、时延较高，吞吐量低

C、能做复杂一些的访问控制，并做精细的认证和审核 D、可伸缩性较差

695、以下关于L2TP VPN配置注意事项的说法中正确的有：（ABC）

A、L2TP的LNS端必须配置虚拟接口模板（Virtual-Template）的IP地址，该虚拟接口模板需要加入域

B、防火墙缺省需要进行隧道的认证。如果不配置认证，需要undo tunnel authentication命令

C、为了使L2TP拨号上来的用户分配的地址不能喝内网用户的地址在同一个网段

D、LNS端不允许配置多个L2TP-Group

1. 以下哪几项关于安全审计和安全审计系统的描述是正确的？（CD）

A、对入侵和攻击行为只能起到威慑作用

B、安全审计不能有助于提高系统的抗抵赖性

C、安全审计是对系统记录和活动的独立审查和检验

D、安全审计系统可提供侦破辅助和取证功能

697、以下哪些属于网络欺骗方式？（ABCD）

A、IP欺骗 B、ARP欺骗 C、DNS欺骗 D、Web欺骗

698、以下哪些是防火墙规范管理需要的？（ABCD）

A、需要配置两个防火墙管理员 B、物理访问防火墙必须严密地控制

C、系统软件、配置数据文件在更改后必须进行备份

D、通过厂商指导发布的硬件和软件的bug和防火墙软件升级版

699、以下硬件安装维护重要安全提示正确的有：（ABCD）

A、不要在雷雨天气进行故障处理 B、保持故障处理区域的干净、干燥

C、上防静电手套或防静电腕带再执行安装和更换操作

D、在使用和操作设备时，需要按照正确的操作流程来操作

700、以下属于DTE(Data Terminal Equipment)数据终端设备的有（AB）

A、路由器 B、PC C、交换机 D、HUB

701、在防火墙的“访问控制”应用中，内网、外网、DMZ三者的访问关系为：（ABD）

A、内网可以访问外网 B、内网可以访问DMZ区

C、DMZ区可以访问内网 D、外网可以访问DMZ区

702、关于GRE校验和验证技术，当本端配置了校验和而对端没有配置校验和时，以下叙述正确的有（BC）。

A、本端对接收报文检查校验和 B、对端对接收报文检查校验和

C、本端对发送报文计算校验和 D、对端对发送报文计算校验和

703、配置PPP链路层协议时，链路层协议状态始终不能转为Up状态的处理建议：（ABCD）

A、PPP链路两端的接口上配置的参数和验证方式都必须一致，LCP检查才能成功

B、如果LCP协商失败，请检查LCP配置协商参数

C、请检查验证方式配置是否正确。因为LCP协商中，包含验证方式的协商。因为LCP协商中，包含验证方式的协商。验证方式协商失败也会导致LCP协商失败

D、接口试图下先执行shutdown命令将接口关闭，再执行undo shutdown命令重启接口

704、对DNSSEC的描述正确的有（AC）。

A、为DNS数据提供来源验证，即保证数据来自正确的名称服务器

B、DNSSEC可防御DNS Query Flood攻击

C、为域名数据提供完整性验证，即保证数据在传输的过程中没有被篡改

D、实施DNSSEC后，只需升级软件系统，对网络、服务器等硬件设备不需考虑

705、MySQL安装程序会给出三种选择，用户可以根据自身的需要选择一种适合的安装方式，以下哪些是正确的？（ABD）

A、Typical（典型安装） B、Compact(最小安装)

C、Full(全部安装) D、Custom(选择安装)

706、MySQL中用DROP语句可删除数据库和数据表，以下哪句是正确的语法？（ABCD）

A、DROP TABLE table\_name1 B、DROP TABLE table\_name1,table\_name2

C、DROP TABLE IF EXISTS table\_name1 D、DROP DATABASE DB name1

707、Oracle 7.2之前的数据库连接用户名和密码在网络传输时是不进行加密的，为了要和旧版本兼容Oracle数据库9.02存在DBLINK\_ENCRYPT\_LOGIN参数用来调节数据库连接时用户名和密码的加密特性，以下说法正确的是：（ACD）。

A、DBLINK\_ENCRYPT\_LOGIN为TRUE时，数据库连接加密用户名和密码

B、DBLINK\_ENCRYPT\_LOGIN时，数据库连接不加密用户名和密码

C、DBLINK\_ENCRYPT\_LOGIN为FALSE时，如果加密的数据库连接失败，会尝试不加密的连接

D、DBLINK\_ENCRYPT\_LOGIN为TRUE时，加密的数据库连接失败，也不会尝试不加密的连接

708、Oracle实例主要由哪两部分组成：（AC）

A、内存 B、Share pool buffer C、后台进程 D、pmon和smon

709、Oracle中如何设置audit trail审计，正确的说法是：（ABD）

A、在init.ora文件中设置“audit\_trail = true”或者“audit\_trail = db”

B、以SYSDBA身份使用AUDIT ALL ON SYS.AUD$ BY ACCESS，语句对audit trail审计

C、Oracle不支持对audit trail的审计

D、在设置audit trail审计前，要保证已经打开Oracle的审计机制

710、SQL Server的登录认证种类有以下哪些？（ACD）

A、Windows认证模式 B、双因子认证模式

C、混合认证模式 D、SQL Server认证

711、SQL Server的取消权限的操作有以下哪些？（ABC）

A、在“详细信息”窗格中右击要授予/拒绝/取消其权限的用户定义的角色

B、单击“属性”命令在“名称”下单击“权限”单击列出全部对象

C、选择在每个对象上授予拒绝或废除的权限，选中标志表示授予权限，X表示拒绝权限，空框表示废除权限，只列出适用于该对象的权限

D、回到“数据库用户属性”对话框中，再点击“确定”按钮，所有的设置就完成了

712、SQL Server中ALTER DATABASE可以提供以下哪些功能选项？（ABCD）

A、更改数据库名称 B、文件组名称 C、数据文件 D、日志文件的逻辑名称

713、SQL Server中关于实例的描述，请选择正确的答案。（ABD）

A、如果安装选择“默认”的实例名称。这时本SQL Server的名称将和Windows 2000服务器的名称相同

B、SQL Server可以在同一台服务器上安装多个实例

C、SQL Server只能在一台服务器上安装一个实例

D、实例各有一套不为其他实例共享的系统及用户数据库，所以各实例的运行是独立的。

714、SQL Server中使用企业管理器从数据库中删除数据或日志文件的步骤如下，正确的步骤是？（ABCD）

A、展开服务器组，然后展开服务器

B、展开“数据库”文件夹，右击要从中删除数据或日志文件的数据库，然后单击“属性”命令

C、若要删除数据文件，单击“常规”选项卡。若要删除日志文件，单击“事务日志”选项卡

D、在“文件名”列户，单击要删除的文件名旁边的箭头，再点DELETE键，文件名旁出现十字光标，表明将删除此文件

715、参数REMOTE\_LOGIN\_PASSWORDFILE在Oracle数据库实例的初始化参数文件中，此参数控制着密码文件的使用及其状态，以下说法正确的是：（ABCD）

A、NONE：只是Oracle系统不使用密码文件，不允许远程管理数据库

B、EXCLUSIVE：指示只有一个数据库实例可以使用密码文件

C、SHARED：指示可有多个数据库实例可以使用密码文件

D、以上说法都正确

716、关于SQL Server 2000中的SQL账号、角色，下面说法正确的是：（ABC）

A、PUBLIC,guest为缺省的账号 B、guest不能从master数据库清除

C、可以通过删除guest账号的角色，从而消弱guest可能带来的安全隐患

D、SQL Server角色的权限是不可以修改的

717、连接MySQL后选择需要的数据库DB\_NAME？以下哪些方法是对的（AC）

A、连接后用USE DB\_NAME选择数据库

B、连接后用SET DB\_NAME选择数据库

C、用mysql -h host -u user -p DB\_NAME连接数据库

D、用mysql -h host -u user -p -T DB\_NAME连接数据库

718、如果数据库不需要远程访问，可以禁止远程tcp/ip连接，以增强安全性。可选择的有效方法：（AC）

A、用防火墙封堵数据库侦听端口避免远程连接 B、禁止tcp/ip协议的使用

C、在mysqld服务器中参数中添加 --skip-networking启动参数来使mysql

D、在/etc/my.cnf下添加remoteConnnect=disable

719、以下哪些MySQL中GRANT语句的权限指定符？（ABCDEF）

A、ALTER B、CREATE C、DELETE

D、UPLOAD E、DROP F、INSERT

720、用THC组织的Oracle的工具，通过sniffer方式抓取数据库的认证信息可有效破解Oracle密码，以下哪些数据是必须获取的？（ABC）

A、AUTH\_SESSKEY B、AUTH\_PASSWORD C、用户名 D、实例名

721、在Oracle 9数据库可以通过配置$Oracle\_HOME\network\admin\sqlnet.ora文件实现数据库层次的基于TCP协议和地址的访问控制。下面说法正确的是：（ABCD）

A、首先需要配置TCP,VALIDNODE\_CHECKING=yes启用节点检查功能

B、其次配置TCP.INVITED\_NODES=192.168.0.12，192.168.0.33将会允许地址是192.168.0网段的12和33的主机访问

C、然后配置TCP.EXCLUDED\_NONES=192.168.0.123将会禁止地址是192.168.0网段的123的主机访问

D、要以上配置生效必须重启lsnrctl监听器

722、在SQL Server 2000中，如果想查询当前数据库服务器软件的版本，可以使用下面哪些方式（ABCD）

A、在查询分析器中通过如下语句查询SELECT ServerPROPERTY(‘productversion’),ServerPROPERTY(‘productlevel’),ServerPROPERTY(‘edition’)

B、在命令行下，用SQL Server自带的管理工具osql连接进入数据库，输入select@@version

C、企业管理器查看服务器属性 D、在SQL Server服务管理器里面查看“关于”

723、在SQL Server 2000中一些无用的存储过程，这些存储过程极容易被攻击者利用，攻击数据库系统。下面的存储过程哪些可以用来执行执行系统命令或修改注册表？（ABC）

A、xp\_cmdshell B、xp\_regwrite C、xp\_regdeletekey D、select \* from master

724、在SQL Server中创建数据库，如下哪些描述是正确的？（ABCD）

A、创建数据库的权限默认授权sysadmin和dbcreator固定服务器角色的成员，但是它仍可以授予其他用户

B、创建数据库的用户将成为该数据库的所有者

C、在一个服务器上，最多可以创建32,767个数据库

D、数据库名称必须遵循标示符规则

725、在对SQL Server 2000的相关文件、目录进行安全配置时，下面可以采用的措施是：（ABCD）

A、删除缺省安装时的例子样本库

B、将存放数据的库文件，配置权限为administrators组、system和启动SQL Server服务的用户账号及DBA组具有完全控制权限

C、对SQL Server安装目录，去除everyone的所有控制权限

D、将数据库数据相关的文件，保存在非系统盘的NTFS独立分区

726、sybase数据库文件系统需要哪些裸设备？（ABCD）

A、master B、proce C、data D、log

727、Oracle支持哪些加密方式？（ABCD）

A、DES B、RC4\_256 C、RC4\_40 D、DES40

728、SQL Server用事件探测器可以帮助排除故障和解决问题，创建跟踪的步骤如下哪些是正确的？（ABCD）

A、从“模板名称”下拉菜单为你创建跟踪选择一个模板

B、“事件探查器”主界面打开后，从“文件”菜单选择“新跟踪”

C、在“跟踪名称”文本框中输入你想要为这个跟踪创建的跟踪名称

D、修改这些默认的选项设置。通过点击“显示全部事件”和“显示全部列”复选框来查看其他的选项。

729、最重要的电磁场干扰源是：（BCD）

A、电源周波干扰 B、雷电电磁脉冲LEMP

C、电网操作过电压SEMP D、静电放电ESD

730、雷电侵入计算机信息系统的途径主要有：（ABD）

A、信息传输通道线侵入 B、电源馈线侵入 C、建筑物 D、地电位反击

731、电信生产其机房作业，是由专门的值机员、机务员来完成，作业内容是：固定电话、无线电话、电报、载波、短波、微波、卫星和电力等电信通信设备，使设备出去良好状态，保证其正常运行。（ABCD）

A、安装 B、值守 C、维护 D、检修

732、对计算机系统有影响的腐蚀性气体大体有如下几种：（ABCD）

A、二氧化硫 B、氢化硫 C、臭氧 D、一氧化碳

733、防火工作的基本措施有：（ABCD）

A、加强对人员的教育管理 B、加强对可燃物的管理

C、加强对物的管理 D、加强对火源、电源的管理

734、会导致电磁泄漏的有（ABCDE）

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

E、信号处理电

735、火灾自动报警、自动灭火系统部署应注意（ABCD）。

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、具有自动和手动两种触发装置

736、计算机场地安全测试包括（ABCD）。

A、温度，湿度，尘埃 B、照度，噪声，电磁场干扰环境场强

C、接地电阻，电压、频率 D、波形失真率，腐蚀性气体的分析方法

737、计算机信息系统设备处于不同雷电活动地区，其雷电电磁场强度有很大差异，根据这一差异，将被防护空间分为下列哪些防护区？（ABCD）

A、直击雷非防护区（LPZOA） B、直击雷防护区（LPZOB）

C、第一防护区（LPZI） D、后续防护区（LPZ2,3...等）

738、静电的危害有（ABCD）。

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

739、灭火的基本方法有（ABCD）。

A、冷却法 B、隔离法 C、窒息法 D、抑制

740、实体安全技术包括（ABD）。

A、环境安全 B、设备安全 C、人员安全 D、媒体安全

741、使用配有计算机的仪器设备时，不应该做的有：（ABCD）

A、更改登机密码和系统设置

B、自行安装软件

C、玩各种电脑游戏

D、将获得的图像、数据等资料存储在未予指定的硬盘分区上

742、硬件设备的使用管理包括（ABCD）。

A、严格按硬件设备的操作使用规程进行操作

B、建立设备使用情况日志，并登记使用过程

C、建立硬件设备故障情况登记表

D、坚持对设备进行例行维护和保养

743、预防静电的措施有（ABCD）。

A、接地 B、不使用或安装产生静电的设备

C、不在产生静电场所穿脱工作服 D、作业人员穿防静电鞋

744、在实验室中引起火灾的通常原因包括：（ABCD）

A、明火 B、电器保养不良

C、仪器设备在不使用时未关闭电源 D、使用易燃物品时粗心大意

745、直击雷：直接击在（ABCD）并产生电效应、热效应和机械力的雷电放电。

A、建筑物 B、构建物 C、地面突进物 D、大地或设备

746、员工区域安全守则包括：（ABCD）

A、非工作时间，员工进入或离开办公区域，应在值班人员处登记

B、外来人员进入办公区域或机房，相关员工必须全程陪同

C、将物品带入/带出公司，要遵守公司相关的规定及流程

D、参加会议时遵守会前、会中、会后的保密流程

747、机房出入控制措施包括：（ABCD）

A、机房接待前台须核查弄清业务系统安全区域的来访者的身份，并记录其进入和离开安全区域的日期与时间

B、机房须告知进入安全区的来访者，该区域的安全要求和紧急情况下的行动步骤

C、可采用强制性控制措施，对来访者的访问行为进行授权和验证

D、要求所有进出机房人员佩带易于辨识的标识

748、为了减小雷电损失，可以采取的措施有（ACD）

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

749、安全要求可以分解为（ABCDE）。

A、可控性 B、保密性 C、可用性 D、完整性 E、不可否认性

750、HASH加密使用复杂的数字算法来实现有效的加密，其算法包括（ABC）

A、MD2 B、MD4 C、MD5 D、Cost256

751、利用密码技术，可以实现网络安全所要求的。（ABCD）

A、数据保密性 B、数据完整性 C、数据可用性 D、身份验证

752、一个密码体系一般分为以下哪几个部分？（ABCD）

A、明文 B、加密密钥和解密密钥

C、密文 D、加密算法和解密算法

753、公钥密码体质的应用主要在于。（AC）

A、数字签名 B、加密 C、密钥管理 D、哈希函数

754、目前基于对称密钥体制的算法主要有。（BC）

A、RSA B、DES C、AES D、DSA

755、使用esp协议时，可以使用的加密运算是。（ABC）

A、DES B、3DES C、AES D、RSA

756、数字签名的作用是。（ACD）

A、确定一个人的身份 B、保密性

C、肯定是该人自己的签字 D、使该人与文件内容发生关系

757、以下属于对称加密算法的是：（ABD）

A、DES B、3DES C、SHA-1 D、RC4 E、MD5

758、在加密过程中，必须用到的三个主要元素是（ABC）

A、所传输的信息（明文） B、加密 钥匙（Encryption Key）

C、加密函数 D、传输信道

759、账号口令管理办法适用于所有和DSMP系统、智能网系统、彩铃平台相关的（ACD）

A、系统管理员 B、操作系统

C、操作维护人员 D、所有上述系统中存在的账号和口令

760、为保证密码安全，我们应采取的正确措施有（ABC）

A、不使用生日做密码 B、不使用少于5为的密码

C、不适应纯数字密码 D、将密码设的非常复杂并保证20位以上

761、公司在使用数据签名技术时，除充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名外，还应注意（ABCD）

A、采取保护公钥完整性的安全措施，例如使用公约证书

B、确定签名算法的类型、属性以及所用密钥长度

C、用于数字签名的密钥应不同于用来加密内容的密钥

D、符合有关数字签名的法律法规，必要时，应在合同或协议中规定使用数字签名的相 关事宜

762、相对于对称加密算法，非对称密钥加密算法（ACD）

A、加密数据的速率较低

B、更适合于现有网络中对所传输数据（明文）的加解密处理

C、安全性更好 D、加密和解密的密钥不同

763、一个典型的PKI应用系统包括（ABCD）实体

A、认证机构CA B、册机构RA C、证书及CRL目录库 D、用户端软件

764、加密的强度主要取决于（ABD）

A、算法的强度 B、密钥的保密性 C、明文的长度 D、密钥的强度

765、一下对于对称密钥加密说法正确的是（BCD）

A、对称加密算法的密钥易于管理 B、加解密双方使用同样的密钥

C、DES算法属于对称加密算法 D、相对于非对称加密算法，加解密处理速度比较快

766、在通信过程中，只采用数字签名可以解决（ABC）等问题

A、数据完整性 B、数据的抵抗赖性 C、数据的篡改 D、数据的保密性

767、对称密钥算法体系包括：（ABCDE）

A、明文(plaintext)：原始消息或数据，作为算法的输入

B、加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换

C、秘密密钥(secret key)：秘密密钥也是算法输入，算法进行的具体替换和转换取决于 这个密钥

D、密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对 于一个给定的消息，两个不同的密钥会产生两个不同的密文

、.解密算法(decryption algorithm)：本质上是加密算法的执行。它使用密文和统一密钥 产生原始明文

768、一下对于混合加密方式说法正确的是。（BCD）

A、 使用公开密钥密码体制对要传输的信息（明文）进行加解密处理

B、使用对称加密算法对要传输的信息（明文）进行加解密处理

C、使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信

D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的

769、电信的网页防篡改技术有（ABC）

A、外挂轮询技术 B、核心内嵌技术

C、时间触发技术 D、安装防病毒软件

770、病毒发展的趋势是？（ABC）

A、 范围更广 B、度更快 C、方式更多

771、病毒自启动方式一般有（ABC）

A、 修改注册表 B、将自身添加为服务

C、将自身添加到启动文件夹 D、修改系统配置文件

772、常见Web攻击方法有一下哪种？（ABCD）

A、SQL Injection B、Cookie欺骗 C、跨站脚本攻击

D、信息泄露漏洞 E、文件腹泻脚本存在的安全隐患

F、 GOOGLE HACKING

773、宏病毒感染一下哪些类型的文件？（ABCDEF）

A.、DOC B、EXE C、XLS D、DOT

774、木马传播包括一下哪些途径：（ACD）

A.、通过电子邮件的附件传播 B、通过下载文件传播

C、通过网页传播 D、通过聊天工具传播

775、目前最好的防病毒软件能做到的是（ABCD）

A.、检查计算机是否感染病毒，消除已感染的任何病毒

B、杜绝病毒对计算的侵害

C、查出计算机已感染的已知病毒，消除其中的一部分

D、检查计算机是否染有已知病毒，并作相应处理

776、通用的DoS攻击手段有哪些？（CD）

A、 SYN Attack B、ICMP Flood C、UDP Flood

D、Ping of Death E、Tear Drop F、Ip Spoofing

777、以下关于蠕虫的描述正确的有：（ABCDEF）

A、 蠕虫具有自动利用网络传播的特点，在传播的同时，造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪

B、 隐藏式蠕虫的基本特征，通过在主机上隐藏，使得用户不容易发现它的存在

C、蠕虫需要传播受感染的宿主文件来进行复制

D、蠕虫的传染能力主要是针对计算机内的文件系统。

778、以下哪几种扫描检测技术属于被动式的检测技术？（AB）

A、 基于应用的检测技术 B、基于主动的检测技术

C、基于目标的漏洞检测技术 D、基于网络的检测技术

779、以下是检查磁盘与文件是否被病毒感染的有效方法：（BC）

A、 检查磁盘目录中是否有病毒文件 B、用抗病毒软件检查磁盘的各个文件

C、用放大镜检查磁盘编码是否有霉变现象 D、检查文件的长度是否无故变化

780、造成计算机不安全的因素有（BD）等多种。

A、 技术原因 B、自然原因 C、认为原因 D、管理原因

781、嗅探技术有哪些特点？（ABCD）

A、间接性 B、.直接性 C、隐蔽性 D、开放性

782、一个恶意的攻击者必须具备哪几点？（ABC）

A、 方法 B、机会 C、动机 D、运气

783、对于DOS网络攻击，可以采用以下哪些措施来缓解主机系统被攻击进程。（ACD）

A.、缩短SYN Timeout时间和设置SYN Cookie B、增加网络带宽

C、在系统之前增加负载均衡设备 D、在防火墙上设置ACL或黑客路由

784、利用Bind/DNS漏洞攻击的分类主要有（ACD）

A、 拒绝服务 B、匿名登录 C、.缓冲区溢出

D、DNS缓存中毒 E、病毒或后门攻击

785、常见Web攻击方法有一下哪种？（ABCD）

A、 SQL Injection B、 Cookie欺骗 C、 跨站脚本攻击 D、信息泄露漏洞

786、黑客所使用的入侵技术主要包括（ABCDE）

A.、协议漏洞渗透 B、密码分析还原 C、应用漏洞分析与渗透

D、拒绝服务攻击 E、病毒或后门攻击

787、主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有（ABC）

A、针对入侵者采取措施 B、修正系统

C、收集更详细的信息 D、入侵追踪

788、下面哪些漏洞属于网络服务类安全漏洞：（BC）

A.、Windows 2000中文版输入法漏洞 B、IS Web服务存在的IDQ远程溢出漏洞

C、RPC DCOM服务漏洞 D、Web服务asp脚本漏洞

789、系统感染病毒后的现象有哪些？（ABCD）

A、系统错误或系统崩溃 B、系统反应慢，网络拥塞

C、陌生的进程或服务 D、陌生的自启动

**三、判断题：（790-1000）**

790、TCSEC将信息安全风机防护等级一共分为7个安全等级：D、C1、C2、B1、B2、B3、 A。(A)

A、正确 B、错误

791、通用标准v2版（CC）的安全等级是以EAL来表示的。（A）

A、正确 B、错误

792、一个企业的信息安全组织能否顺利开展工作（定期安全评估、日志安全巡检、定期安全审核、应急演练等），主要取决于公司领导对信息安全工作的认识程度和支持力度。（A）

A、正确 B、错误

793、在信息安全领域，CIA通常是指：保密性、完整性和可用性。（A）

A、正确 B、错误

794、信息安全是永远是相对的，并且需要不断持续关注和改进，永远没有一劳永逸的安全

防护措施。（A）

A、正确 B、错误

795、在信息安全领域，CIA通常是指：保密性、完整性和非抵赖性。（B）

A、正确 B、错误

796、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

797、信息安全的威胁主体包括内部人员、准内部人员、外部人员、系统自身等方面。（B）

A、正确 B、错误误

798、互联网网络安全事件根据危害和紧急程度分为一般、预警、报警、紧急、重大五种。 （B）

A、正确 B、错误

799、安全审计是从管理和技术两个方面检查公司的安全策略和控制措施的执行情况，发现安全隐患的过程。（A）

A、正确 B、错误

800、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

801、计算机系统安全是指应用系统具备访问控制机制，数据不被泄露、丢失、篡改等。（B）

A、正确 B、错误

802、主机加固完成后，一般可以有效保证主机的安全性增强。（A）

A、正确 B、错误

803、黑客在进行信息收集时，通常利用Windows的IPC漏洞可以获得系统用户的列表的信 息。（A）

A、正确 B、错误

804、Solaris系统中一般需要确认ROOT账号只能本地登录，这样有助于安全增强。（A）

A、正确 B、错误

805、HP-UX系统加固中在设置ROOT环境变量不能有相对路径设置。（A）

A、正确 B、错误

806、屏幕保护的木马是需要分大小写。（B）

A、正确 B、错误

807、安全审计就是日志的记录。（B）

A、正确 B、错误误

808、HP-UX系统加固中在设置通用用户环境变量不能有相对路径设置。（A）

A、正确 B、错误

809、AIX系统加固时，对系统配置一般需要自编脚本完成。（A）

A、正确 B、错误

810、Windows NT中用户登录域的口令是以明文方式传输的。（B）

A、正确 B、错误

811、操作系统普通用户账号审批记录应编号、留档。（A）

A、正确 B、错误

812、计算机病毒是计算机系统中自动产生的。（B）

A、正确 B、错误

813、主机系统加固时根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。（A）

A、正确 B、错误

814、4A系统的建设能够减轻账户管理员的维护工作。（A）

A、正确 B、错误

815、4A系统的接入管理可以管理到用户无力访问的接入。（B）

A、正确 B、错误

816、Cisco路由器可以使用enable password命令为特权模式的进入设置强壮的密码。（B）

A、正确 B、错误

817、Cisco设备的AUX端口默认是启用的。（A）

A、正确 B、错误

818、DHCP可以向终端提供IP地址、网关、DNS服务器地址等参数。（A）

A、正确 B、错误误

819、Inbound方向的NAT使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际IP地址。（B）

A、正确 B、错误

820、IPS设备即使不出现故障，它仍然是一个潜在的网络瓶颈，需要强大的网络结构来配合。（A）

A、正确 B、错误

821、IPS的过滤器规则不能自由定义。（B）

A、正确 B、错误

822、IPS的某些功能和防火墙类似。（A）

A、正确 B、错误

823、IPS和IDS都是主动防御系统。（B）

A、正确 B、错误

824、NAT是一种网络地址翻译的技术，它能是的多台没有合法地址的计算机共享一个合法的IP地址访问Internet。（A）

A、正确 B、错误

825、Netscreen的ROOT管理员具有的最高权限，为了避免ROOT管理员密码被窃取后造成威胁，应该限制ROOT只能通过CONSOLE接口访问设备，而不能远程登录。(A)

A、正确 B、错误

826、Netscreen防火墙的外网口应禁止PING测试，内网口可以不限制。（B）

A、正确 B、错误

827、OSI是开放的信息安全的缩写。（B）

A、正确 B、错误

828、OSI七层模型中，传输层数据成为段（Segment），主要是用来建立主机端到端连接，包括TCP和UDP连接。（A）

A、正确 B、错误

829、OSI中会话层不提供机密性服务。（A）

A、正确 B、错误

830、SSH使用TCP 79端口的服务。（B）

A、正确 B、错误

831、TCP/IP模型从下至上分为四层：物理层，数据链路层，网络层和应用层。（B）

A、正确 B、错误

832、TCP/IP模型与OSI参考模型的不同点在于TCP/IP把表示层和会话层都归于应用层，所以TCP/IP模型从下至上分为五层：物理层，数据链路层，网络层，传输层和应用层。 （A）

A、正确 B、错误

833、TCP/IP协议体系结构中，IP层对应OSI/RM模型的网络层。（A）

A、正确 B、错误

834、默认情况下需要关闭Cisco设备的Small TCP/UDP服务。（A）

A、正确 B、错误

835、缺省情况下，防火墙工作模式为路由模式，切换工作模式后可直接进行进一步配置。（B）

A、正确 B、错误

836、入侵检测具有对操作系统的校验管理，判断是否有破坏安全的用户活动。（A）

A、正确 B、错误

837、入侵检测可以处理数据包级的攻击。（B）

A、正确 B、错误

838、入侵检测系统不能弥补由于系统提供信息的质量或完整性的问题。（A）

A、正确 B、错误

839、入侵检测系统能够检测到用户的对主机、数据库的网络操作行为。（B）

A、正确 B、错误

840、入侵检测系统是一种对计算机系统或网络事件进行检测并分析这个入侵事件特征的过程。（A）

A、正确 B、错误

841、统计分析的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。（B）

A、正确 B、错误

842、统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。（A）

A、正确 B、错误

843、透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决IP地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的IP的地址。（A）

A、正确 B、错误

844、完整性分析的缺点是一般以批处理方式实现，不用于实时响应。（A）

A、正确 B、错误

845、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（B）

A、正确 B、错误

846、网络边界的Cisco路由器应关闭CDP服务。（A）

A、正确 B、错误

847、网络边界Cisco设备的CDP协议可以开放。（B）

A、正确 B、错误

848、网络层的防护手段（防火墙，SSL，IDS，加固）可以组织或检测到应用层攻击。（B）

A、正确 B、错误

849、针对不同的攻击行为，IPS只需要一个过滤器就足够了。（B）

A、正确 B、错误

850、主机型IDS其数据采集部分当然位于其所检测的网络上。（B）

A、正确 B、错误

851、状态检测防火墙检测每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。（B）

A、正确 B、错误

852、IPS虽然能主动防御，但是不能坚挺网络流量。（B）

A、正确 B、错误

853、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。（B）

A、正确 B、错误

854、审计系统进行关联分析时不需要关注日志时间。（B）

A、正确 B、错误

855、垃圾邮件一般包括商业广告、政治邮件、病毒邮件、而已欺诈邮件（网络钓鱼）等几个方面。（A）

A、正确 B、错误

856、防止网络窃听最好的方法就是给网上的信息加密，是的侦听程序无法识别这些信息模式。（A）

A、正确 B、错误

857、侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。（A）

A、正确 B、错误

858、模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。（A）

A、正确 B、错误

859、入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。（A）

A、正确 B、错误

860、VPN的主要特点是通过加密是信息安全的通过Internet传递。（A）

A、正确 B、错误

861、传输层协议使用端口号（Port）来标示和区分上层应用程序，如：Telnet协议用的是23号端口、DNS协议使用69号端口。（B）

A、正确 B、错误

862、如果Web应用对URL访问控制不当，可能造成用户直接在浏览器中输入URL，访问不该访问的页面。（A）

A、正确 B、错误

863、如果Web应用没有对攻击者的输入进行适当的编码和过滤，就用于构造数据库查询或操作系统命令时，可能导致注入漏洞。（A）

A、正确 B、错误

864、HTTP协议定义了Web浏览器向Web服务器发生Web页面请求的格式及Web页面在Internet上传输的方式。（A）

A、正确 B、错误

865、HTTP协议是文本协议，可利用回车换行做边界干扰。（A）

A、正确 B、错误

866、Init<sid>.ora文件是Oracle启动文件，任何参数的配置错误都会造成Oracle不能启动，任何参数的不合理配置都可能造成系统故障。（A）

A、正确 B、错误

867、Mysqldump是采用SQL级别的备份机制，它将数据表导成SQL脚本文件，在不同的MySQL版本之间升级时相对比较合适，这也是最常见的备份方法。（A）

A、正确 B、错误

868、Orabrute是进行远程破解Oracle密码的工具，要猜解的密码可以在password.txt中设置。（A）

A、正确 B、错误

869、Oracle的SYS账户在数据库中具有最高权限，能够做任何事情，包括启动/关闭Oracle数据库。即使SYS被锁定，也已然能够访问数据库。（A）

A、正确 B、错误

870、Oracle的若算法加密机制：两个相同的用户名和密码在两个不同的Oracle数据库机器中，将具有相同的哈希值。（A）

A、正确 B、错误

871、Oracle密码允许包含像“SELECT”，“DELETE”，“CREATE”这类的Oracle/SQL关键字。（B）

A、正确 B、错误

872、Oracle的HTTP的基本验证可选择SYS破解，因为它始终存在和有效。（A）

A、正确 B、错误

873、Oracle默认情况下，口令的传输方式是加密。（B）

A、正确 B、错误

874、Oracle数据库的归档日志不是在线日志的备份。（B）

A、正确 B、错误

875、OSI网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。（A）

A、正确 B、错误

876、OSI网络安全体系结构的五类安全服务是鉴别、访问控制、保密性、完整性、抗否认。（A）

A、正确 B、错误

877、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因。（A）

A、正确 B、错误

878、SQL Server如果设置了不恰当的数据库文件权限，可能导致敏感文件被非法删除或读取，威胁系统安全。（A）

A、正确 B、错误

879、SQL Server数据库应禁止使用除tcp/ip以外的协议，保护数据库通信安全。（A）

A、正确 B、错误

880、SQL Server应该社会自日志审核无法追踪回溯安全事件。（A）

A、正确 B、错误

881、Web服务器一般省缺不允许攻击者访问Web根目录以外的内容，内容资源不可以任意访问。(A)

882、Web攻击面不仅仅是浏览器中可见的内容。（A）

A、正确 B、错误

883、Web应用对网络通讯中包含的敏感信息进行加密，就不会被窃听。（B）

A、正确 B、错误

884、暴力猜解不能对Web应用进行攻击。（B）

A、正确 B、错误

885、在Oracle自身的配置上做限定方法是：修改$Oracle\_HOME\network\admin目录下面的SQLNET..ORA文件，类似设置如下：

Tcp\_validnode\_checking=YES

Tcp\_invited\_nodes=

(192.168.0.1,ip2,ip3•••...)。

( A )

A、正确 B、错误

886、不设置必要的日志审核，就无法追踪回溯安全事件，Oracle中若果要审计记录成功的登陆语句”SQL>audit session whenever successful;”. ( A )

A、正确 B、错误

887、对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是DNS服务器。（B）

A、正确 B、错误

888、防止XSS各种方法都有优劣之处，防范XSS的真正挑战不在于全免，而在于细致。（B）

A、正确 B、错误

889、访问控制、强制登陆、自动安全更新都属于Window2000的安全组件（B）

A、正确 B、错误

890、复杂的系统存在大量的相互引用访问，如果开发者不能有效的进行权限控制，就可能被恶意引用。（A）

A、正确 B、错误

891、攻击者可以通过SQL注入手段获取其他用户的密码。（A）

A、正确 B、错误

892、几乎所有的关系数据库系统和相应的SQL语言都面临SQL注入的潜在威胁。（A)

A、正确 B、错误

893、简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架（B）

A、正确 B、错误

894、默认可通过Web程序来远程管理Oracle10g数据库，端口是8080.（A）

A、正确 B、错误

895、如果sa是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。（A）

A、正确 B、错误

896、如果在SQL Server等领域成功并不意味这该用户已经可以访问SQL Server上的数据库。（A）

A、正确 B、错误

897、如果知道Oracle密码长度，用Rainbow表生成器来破解其密码哈希值是绝对成功的。（A）

A、正确 B、错误

898、所有操作系统、数据库、网络设备，包括一部分业务系统，均需要支持基于账号的访问控制功能。（B）

A、正确 B、错误

899、网络拓扑分析为检查是否有配置错误项泄露内部IP地址，从而推断网站系统拓扑。（A）

A、正确 B、错误

900、为Oracle数据库安全考虑，在对人共同对数据库进行维护时应依赖数据库预定义的传统角色。（B）

A、正确 B、错误

901、为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。(A)

A、正确 B、错误

902、系统类型鉴别为检查主机系统与开放服务是否存在安全漏点。（B）

A、正确 B、错误

903、系统漏洞扫描为检查目标的操作系统与应用系统信息。（B）

A、正确 B、错误

904、选择远程破解Oracle的最好账户是SYS，因为此账户永远有效。（A）

A、正确 B、错误

905、一封电子邮件可以拆分成对个IP包，每个IP包可以沿不同的路径到达目的地。（A）

A、正确 B、错误

906、一个共享文件夹。将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有读取的权限。（A）

A、正确 B、错误

907、用Sqlplus登陆到Oracle数据库，使用slesct username, password form dba\_users命令可查看数据库中的用户名和密码明文。（B）

A、正确 B、错误

908、有的Web应用登陆界面允许攻击者暴力猜解口令，在自动工具与字典表的帮助下，可以迅速找到弱密码用户。（A）

A、正确 B、错误

909、在Oracle所有版本在安装的时候都没有提示修改SYS的默认密码。（B）

A、正确 B、错误

910、在ORacle数据库安装补丁时，不需要关闭所有与数据库有关的服务。（B）

A、正确 B、错误

911、在SQL Server安装SP3补丁时不需要系统中已经安装了SP1或SP2。（B）

A、正确 B、错误

912、在SQL Server中具有sysadmin权限的用户可以通过xp\_cmdshell存储扩展以system的权限执行任意系统命令。（A）

A、正确 B、错误

913、Oracle默认配置下，每个账户如果有30次的失败登陆，此账户将被锁定。（B）

A、正确 B、错误

914、定制开发Web系统的安全度不如标准的产品。（A）

A、正确 B、错误

915、对MySQL注入攻击时，经常用到注释符号#来屏蔽剩下的内置SQL语句。（A）

A、正确 B、错误

916、一个登录名只能进入服务器，但是不能让用户访问服务器中的数据库资源。每个登录名的定义存放在msater数据库的syslogins表中。（A）

A、正确 B、错误

917、Web错误信息可能泄露服务器型号版本、数据库型号、路径、代码。（A）

A、正确 B、错误

918、Oracle的密码哈希值存储在SYS.USER$表中。可以通过像DBA USERS这类的视图来访问。（A）

A、正确 B、错误

919、产品的定制开发是应用安全中最薄弱的一环。（A）

A、正确 B、错误

920、Oracle限制了密码由英文字母，数字，#，下划线（\_），美元字符（$）构成，密码的最大长度为30字符；并不能以”$”,”#”,”\_”或任何数字开头。（A）

A、正确 B、错误

921、网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。（B）

A、正确 B、错误

922、计算机场地可以选择在公共区域人流量比较大的地方。（B）

A、正确 B、错误

923、EMC测试盒约束用户关心的信息信号的电磁发射、TEMPEST只测试盒约束系统和设备的所有电磁发射。（B）

A、正确 B、错误

924、加密传输是一种非常有效并经常使用的方法，也能解决输入和输出端的电磁信息泄露问题。（B）

A、正确 B、错误

925、出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。（B）

A、正确 B、错误

926、红区：红新号的传输通道或单元电路称为红区，反之为黑区。（A）

A、正确 B、错误

927、机房应设置相应的活在报警和灭火系统。（A）

A、正确 B、错误

928、计算机机房的建设应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。（A）

A、正确 B、错误

929、计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。（B）

A、正确 B、错误

930、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。（A）

A、正确 B、错误

931、提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。（A）

A、正确 B、错误

932、在计算机机房附近施工，不负有维护计算机信息系统安全的责任和义务。（B）

A、正确 B、错误

933、只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。（B）

A、正确 B、错误

934、主管计算机信息系统安全的公安机关和城建及规划部门，应与设施单位进行协调，在不危害用户利益的大前提下，制定措施。合理施工，做好计算机信息系统安全保护工作。（B）

A、正确 B、错误

935、防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。（A）

A、正确 B、错误

936、对于公司机密信息必须根据公司的相关规定予以适当的标识。（A）

A、正确 B、错误

937、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。（A）

A、正确 B、错误

938、如果在电话、电视会议中涉及讨论工伤机密信息，会议主持人或组织人在会议全过程中一定要确认每一个与会者是经授权参与的。（A）

A、正确 B、错误

939、为防止信息非法泄露，需要销毁存储介质时，应该批准后自行销毁。（B）

A、正确 B、错误

940、将公司的机密信息通过互联网络传送时，必须予以加密。（A）

A、正确 B、错误

941、机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。（A）

A、正确 B、错误

942、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式进行保密。（A）

A、正确 B、错误

943、“一次一密”属于序列密码的一种。（A）

A、正确 B、错误

944、3DES算法的加密过程就是用一个秘钥对待加密的数据执行三次DES算法的加密操作。（B）

A、正确 B、错误

945、AES加密算法的秘钥长度为128、192或256位。（A）

A、正确 B、错误

946、AES是一种非对称算法。（B）

A、正确 B、错误

947、DES3和RSA是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。（A）

A、正确 B、错误

948、Diffie-Hellman算法的安全性取决于离散对数计算的困难性，可以实现秘钥交换。（A）

A、正确 B、错误

949、DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。（A）

A、正确 B、错误

950、MD5是一种加密算法。（B）

A、正确 B、错误

951、PGP协议缺省的压缩算法是ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。（A）

A、正确 B、错误

952、PKI是一个用对称密码算法和技术来实现并提供安全服务的具有通用性的安全基础设施。（B）

A、正确 B、错误

953、RC4是典型的的序列密码算法。（A）

A、正确 B、错误

954、RSA算法作为主要的非对称算法，使用公钥加密的秘闻一定要采用公钥来街。（B）

A、正确 B、错误

955、安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。（A）

A、正确 B、错误

956、常见的公钥密码算法有RSA算法、Diffie-Hellman算法和EIGamal算法。（A）

A、正确 B、错误

957、当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（A）

A、正确 B、错误

958、发送方使用AH协议处理数据包，需要对整个IP的数据包计算MAC，包括IP头的所有字段和数据。（B）

A、正确 B、错误

959、分组密码的优点是错误扩展小、速度快、安全程度高。（B）

A、正确 B、错误

960、公共迷药密码体制在秘钥管理上比对称秘钥密码体制更安全。（A）

A、正确 B、错误

961、古典加密主要采用的主要方法是置换，代换。（A）

A、正确 B、错误

962、古典加密主要是对加密算法的保密，现代加密算法是公开的，主要是针对秘钥进行保密。（A）

A、正确 B、错误

963、基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。（A）

A、正确 B、错误

964、口令应在120天至少更换一次。（B）

A、正确 B、错误

965、链路加密方式适用于在广域网系统中应用。（B）

A、正确 B、错误

966、密码保管不善属于操作失误的安全隐患。（B）

A、正确 B、错误

967、日常所见的校园饭卡是利用身份认证的单因素法。（A）

A、正确 B、错误

968、身份认证要求对数据和信息来源进行验证，以确保发信人的身份。（B）

A、正确 B、错误

969、身份认证与权限控制是网络社会的管理基础。（A）

A、正确 B、错误

970、数据在传输过程中用哈希算法保证其完整性后，非法用户无法无法对数据进行任何修改。（B）

A、正确 B、错误

971、数字签名比较的是摘要结果长度是否都是128位。（B）

A、正确 B、错误

972、通信数据与文件加密是同一个概念。（B）

A、正确 B、错误

973、为AES开发的Rijndae1算法的秘钥长度是128位，分组长度也为128位。（B）

A、正确 B、错误

974、为了保证安全性，密码算法应该进行保密。（B）

A、正确 B、错误

975、文件压缩变换是一个单向加密过程。（B）

A、正确 B、错误

976、我的公钥证书不能在网络上公开，否则其他人可能冒充我的身份或伪造我的数字签名。（B）

A、正确 B、错误

977、现代加密算法可以分为对称加密算法和非对称加密。（A）

A、正确 B、错误

978、虚拟专用网VPN的关键技术主要是隧道技术、加解密技术、秘钥管理技术以及使用者与设备身份认证技术。（A）

A、正确 B、错误

979、以当前的技术来说，RSA体制是无条件安全的。（B）

A、正确 B、错误

980、在4A系统的远期建设中，应用系统自身不需要保留系统从账户信息。（B）

A、正确 B、错误

981、在MD5算法中，要先将以初始化的A、B、C、D这四个变量分别复制到a、b、c、d中。（A）

A、正确 B、错误

982、在MD5算法中要用到4个变量，分别表示A、B、C、D，均为32位长。（A）

A、正确 B、错误

983、在PKI中，注册机构RA是必要的组件。（B）

A、正确 B、错误

984、在SSL握手协议过程中，需要服务器发送自己的证书。（A）

A、正确 B、错误

985、在非对称加密过程中，加密和解密使用的是不同的秘钥。（A）

A、正确 B、错误

986、在公钥加密系统中，用公钥加密的密文可以由私钥解密，但用公钥加密的密文，不能用公钥解密。 （B）

A、正确 B、错误

987、在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一种“破解”。 （A）

A、正确 B、错误

988、账户管理的Agent不适用于在网络设备中部署。 （A）

A、正确 B、错误

989、整个PKI系统有证书服务器AS、票据许可服务器TGS、客户机和应用服务器四部分组成。 （B）

A、正确 B、错误

990、最基本的认证方式选择证书是数字证书。（B）

A、正确 B、错误

991、最小特权、纵深防御是网络安全原则之一。（A）

A、正确 B、错误

992、数字证书是由权威机构CA发行的一种权威的电子文档，是网络环境中的一种身份证。（A）

A、正确 B、错误

993、数字证书是由权威机构PKI发行的一种权威性的电子文档，是网络环境中的一种身份证。 （B）

A、正确 B、错误

994、信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段。（A）

A、正确 B、错误

995、病毒能隐藏在电脑的CMOS存储器里。（B）

A、正确 B、错误

996、对感染病毒的软盘进行浏览会导致硬盘被感染。（B）

A、正确 B、错误

997、已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（B）

A、正确 B、错误

998、重新格式化硬盘可以清楚所有病毒。（B）

A、正确 B、错误

999、专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，并根据评估结果提供评估报告。 （A）

A、正确 B、错误

1000、冒充信件回复、假装纯文字ICON、冒充微软雅虎发信、下载电子贺卡同意书、是使用的叫做字典攻击法的方法。（B）

A、正确 B、错误

连云港专业技术继续教育—网络信息安全总题库及答案

**信息安全技术试题及答案**

**信息安全网络基础：**

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. 由于传输的内容不同，电力线可以与网络线同槽铺设。**×**

8. 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. **√**

9. 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。**√**

10. 机房内的环境对粉尘含量没有要求。**×**

11. 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。**√**

12. 纸介质资料废弃应用碎纸机粉碎或焚毁。**√**

**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，磁带是应用得最广的介质。**√**

4. 增量备份是备份从上次完全备份后更新的全部数据文件。**×**

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。**×**

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

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 B

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

3. 容灾的目的和实质是 C

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

4. 容灾项目实施过程的分析阶段，需要进行 D

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

5. 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。 B

A.磁盘 B. 磁带 c. 光盘 D. 自软盘

6. 下列叙述不属于完全备份机制特点描述的是一一一。 D

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

7. 下面不属于容灾内容的是 A

A. 灾难预测 B.灾难演习 C. 风险分析 D.业务影响分析

8、IBM TSM Fastback 是一款什么软件（ D）

A、防病毒产品； B、入侵防护产品； C、上网行为管理产品； D、数据存储备份产品

9、IBM TSM Fastback产品使用的什么技术（a )

A、磁盘快照； B、文件拷贝； C、ISCSI技术； D、磁盘共享

12、IBM TSM Fastback产品DR（远程容灾）功能备份的是什么（ BABC）

A、应用系统； B、本地备份的数据； C、文件系统； D、数据库

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。ABCDE

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。ABD

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。ACD

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

4、数据安全备份有几种策略（ ABC ）

A、全备份； B、增量备份； C、差异备份； D、手工备份

5、建立Disaster Recovery（容灾系统）的前提是什么（ ABC ）多选

A、自然灾害（地震、火灾，水灾...)； B、人为灾害（错误操作、黑客攻击、病毒发作...)

C、技术风险（设备失效、软件错误、电力失效...）

6、IBM TSM Fastback 可以支持数据库系统包括（ ABC ）多选

A、MS SQL； B、Oracle； C、DB2； D、MY SQL

7、IBM TSM Fastback 可以支持的存储介质包括（ BD ）

A、磁带介质； B、磁盘介质； C、磁带库； D、磁盘柜

**基础安全技术**

系统安全

一、判断题

1. 常见的操作系统包括 DOS 、UNIX 、Linux、Windows 、 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 Microsoft Windows 、 UNIX 、 Linux 等 ); 另一些的内核与壳关系紧 密 ( 如 UNIX 、 Linux 等内核及壳只是操作层次上不同而已。**×**

3. 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。**×**

4.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**√**

5. 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。**×**

6. 数据库安全只依靠技术即可保障。**×**

7. 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。**×**

8. 数据库管理员拥有数据库的一切权限。**√**

9. 完全备份就是对全部数据库数据进行备份。**√**

二、单选题

1.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 B. 域帐号 C. 来宾帐号D. 局部帐号

2.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。 (C)

A. 本地帐号 B. 域帐号 C. 来宾帐号 D. 局部帐号

3. 计算机网络组织结构中有两种基本结构，分别是域和(b)

A. 用户组 B. 工作组 C. 本地组 D. 全局组

4. 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(d)

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

5 、.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(b)

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

三、多选题

1. 操作系统的基本功能有(abcd)

A. 处理器管理 B. 存储管理 C. 文件管理 D. 设备管理

2.Windows 系统中的用户组包括(abc)

A. 全局组 B. 本地组

C. 特殊组 D. 标准组

3.Windows 系统登录流程中使用的系统安全模块有(abc)

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

4. 数据库故障可能有(abcde)

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

**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. 软件防火墙就是指个人防火墙。**×**

3. 防火墙必须要提供 VPN 、 NAT 等功能。**×**

4. 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。**√**

5. 只要使用了防火墙，企业的网络安全就有了绝对的保障。**×**

6. 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。**√**

7. 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 。**√**

8. 所有的漏洞都是可以通过打补丁来弥补的。**×**

9. 通过网络扫描，可以判断目标主机的操作系统类型。**√**

10. 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。**×**

11. 计算机病毒可能在用户打开 "txt" 文件时被启动。**√**

12. 在安全模式下木马程序不能启动。**×**

13. 大部分恶意网站所携带的病毒就是脚本病毒。**√**

14. 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。**√**

二、单选题

1. 防火墙提供的接入模式不包括一一一。(d)

A. 网关模式 B.透明模式 C. 混合模式 D.旁路接入模式

2. 下面关于 DMZ 区的说法错误的是(c)

A. 通常 DMZ 包含允许来自互联网的通信可进入的设备，如 Web 服务器、 FTP 服务器、 SMTP 服务器和 DNS 服务器等

B. 内部网络可以无限制地访问外部网络以及 DMZ

C.DMZ 可以访问内部网络

D. 有两个 DMZ 的防火墙环境的典型策略是主防火墙采用 NAT 方式工作，而内部防 火墙采用透明模式工作以减少内部网络结构的复杂程度

3. 下面病毒出现的时间最晚的类型是(b)

A. 携带特洛伊术马的病毒 B. 以网络钓鱼为目的的病毒

C. 通过网络传播的蠕虫病毒 D.OEice 文档携带的宏病毒

4. 不能防止计算机感染病毒的措施是(a)

A. 定时备份重要文件

B. 经常更新操作系统

C. 除非确切知道附件内容，否则不要打开电子邮件附件

D. 重要部门的计算机尽量专机专用与外界隔绝

5. 企业在选择防病毒产品时不应该考虑的指标为(d)

A. 产品能够从一个中央位置进行远程安装、升级 '

B. 产品的误报、漏报率较低

C. 产品提供详细的病毒活动记录

D. 产品能够防止企业机密信息通过邮件被传出

6. 病毒传播的途径有(acde)

A. 移动硬盘 B. 内存条

C. 电子邮件 D. 聊天程序

E 网络浏览

7. 可能和计算机病毒有关的现象有(acd)

A. 可执行文件大小改变了

B. 在向写保护的 U 盘复制文件时屏幕上出现 U 盘写保护的提示

C. 系统频繁死机

D. 内存中有来历不明的进程

E. 计算机主板损坏

**应用安全**

一、判断题

1. 运行防病毒软件可以帮助防止遭受网页仿冒欺诈。**√**

2. 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。**√**

3. 网络钓鱼的目标往往是细心选择的一些电子邮件地址。**√**

4. 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。**×**

5. 在来自可信站点的电子邮件中输入个人或财务信息是安全的。**×**

6. 可以采用内容过滤技术来过滤垃圾邮件。**√**

7. 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。**√**

8. 随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模块成为信息安全领域的一个发展趋势**√**

9 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才肤内容。**√**

10. 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。**√**

11. 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。**×**

二、单选题

1. 以下不会帮助减少收到的垃圾邮件数量的是一一一。(c)

A. 使用垃圾邮件筛选器帮助阻止垃圾邮件 .

B. 共享电子邮件地址或即时消息地址时应小心谨慎

C. 安装入侵检测软件

D. 收到垃圾邮件后向有关部门举报

三、多选题

1. 下列邮件为垃圾邮件的有(ade)

A. 收件人无法拒收的电子邮件

B. 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件 C. 含有病毒、色情、反动等不良信息或有害信息的邮件

D. 隐藏发件人身份、地址、标题等信息的电子邮件

E. 含有虚假的信息源、发件人、路由等信息的电子邮件

2. 垃圾邮件带来的危害有(abd)

A. 垃圾邮件占用很多互联网资源

B. 垃圾邮件浪费广大用户的时间和精力

C. 垃圾邮件提高了某些公司做广告的效益

D. 垃圾邮件成为病毒传播的主要途径

E. 垃圾邮件迫使企业使用最新的操作系统

3. 网页防篡改技术包括(bd)

A. 网站采用负载平衡技术 B. 防范网站、网页被篡改

C. 访问网页时需要输入用户名和口令 D. 网页被篡改后能够自动恢复

E 采用 HITPS 协议进行网页传输主

4. 网络钓鱼常用的手段有(abcde)

A. 利用垃圾邮件 B. 利用假冒网上银行、网上证券网站

C. 利用虚假的电子商务 D. 利用计算机病毒

E. 利用社会工程学

5. 内容过滤的目的包括(abcde)

A. 阻止不良信息对人们的侵害

B. 规范用户的上网行为，提高工作效率

C. 防止敏感数据的泄漏

D. 遏制垃圾邮件的蔓延

E. 减少病毒对网络的侵害

7. 内容过滤技术的应用领域包括(acde)

A. 防病毒 B.网页防篡改 C. 防火墙 D.入侵检测 E. 反垃圾邮件

|  |  |
| --- | --- |
| 1282 | 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.A |
|  | A 正确 B 错误 |
| 1283 | 计算机场地可以选择在公共区域人流量比较大的地方。b |
|  | A 正确 B 错误 |
| 1284 | 计算机场地可以选择在化工厂生产车间附近。b |
|  | A 正确 B 错误 |
| 1285 | 计算机场地在正常情况下温度保持在18～28摄氏度。b |
|  | A 正确 B 错误 |
| 1286 | 机房供电线路和动力、照明用电可以用同一线路。b |
|  | A 正确 B 错误 |
| 1287 | 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。b |
|  | A 正确 B 错误 |
| 1288 | 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a。 |
|  | A 正确 B 错误 |
| 1289 | 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。a |
|  | A 正确 B 错误 |
| 1290 | 屏蔽室的拼接、焊接工艺对电磁防护没有影响。b |
|  | A 正确 B 错误 |
| 1291 | 由于传输的内容不同，电力线可以与网络线同槽铺设。b |
|  | A 正确 B 错误 |
| 1292 | 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。地线做电气连通。a |
|  | A 正确 B 错误 |
| 1293 | 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。a |
|  | A 正确 B 错误 |
| 1294 | 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。a |
|  | A 正确 B 错误 |
| 1295 | 机房内的环境对粉尘含量没有要求。b |
|  | A 正确 B 错误 |
| 1296 | 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。a |
|  | A 正确 B 错误 |
| 1297 | 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。a |
|  | A 正确 B 错误 |
| 1298 | 纸介质资料废弃应用碎纸机粉碎或焚毁。a |
|  | A 正确 B 错误 |
| 1299 | 以下不符合防静电要求的是\_b\_\_\_。 |
|  | 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 |
| 1300 | 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\_\_。 |
|  | 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 |
| 1301 | 对电磁兼容性(Electromagnetic Compatibility，简称EMC)标准的描述正确的是\_\_\_c\_。 |
|  | 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 |
| 1302 | 物理安全的管理应做到\_\_\_c\_。 |
|  | 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 |
| 1303 | 场地安全要考虑的因素有\_\_c\_\_。 |
|  | 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 |
| 1304 | 火灾自动报警、自动灭火系统部署应注意\_\_ascd\_\_。 |
|  | 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 具有自动和手动两种触发装置 |
| 1305 | 为了减小雷电损失，可以采取的措施有\_\_acd\_\_。 |
|  | 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 |
| 1306 | 会导致电磁泄露的有\_\_abcde\_\_。 |
|  | 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 |
| 1307 | 磁介质的报废处理，应采用\_\_cd\_\_。 |
|  | A 直接丢弃B 砸碎丢弃 C 反复多次擦写 D 专用强磁工具清除 |
| 1308 | 静电的危害有\_\_abcd\_\_。 |
|  | 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 |
| 1309 | 防止设备电磁辐射可以采用的措施有\_\_b\_\_。 |
|  | A 屏蔽 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 |
| 1310 | 灾难恢复和容灾具有不同的含义。a |
|  | A 正确 B 错误 |
| 1311 | 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。a |
|  | A 正确 B 错误 |
| 1312 | 对目前大量的数据备份来说，磁带是应用得最广的介质。b |
|  | A 正确 B 错误 |
| 1313 | 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。b |
|  | A 正确 B 错误 |
| 1314 | 容灾等级通用的国际标准SHARE 78将容灾分成了六级。b |
|  | A 正确 B 错误 |
| 1315 | 容灾就是数据备份。b |
|  | A 正确 B 错误 |
| 1316 | 数据越重要，容灾等级越高。a |
|  | A 正确 B 错误 |
| 1317 | 容灾项目的实施过程是周而复始的。a |
|  | A 正确 B 错误 |
| 1318 | 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。b |
|  | A 正确 B 错误 |
| 1319 | 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。a |
|  | A 正确 B 错误 |
| 1320 | 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。 |
|  | A 正确 B 错误 |
| 1321 | 代表了当灾难发生后，数据的恢复程度的指标是\_\_A\_\_。 |
|  | A RPO B RTOC NROD SDO |
| 1322 | 代表了当灾难发生后，数据的恢复时间的指标是\_\_B\_\_。 |
|  | A RPO B RTO C NROD SDO |
| 1323 | 我国《重要信息系统灾难恢复指南》将灾难恢复分成了\_B\_\_\_级。 |
|  | A 五 B 六 C 七D 八 |
| 1324 | 容灾的目的和实质是\_\_C\_\_。 |
|  | 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 |
| 1325 | 容灾项目实施过程的分析阶段，需要进行\_D\_\_\_。 |
|  | 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 |
| 1326 | 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\_\_\_。 |
|  | A 磁盘 B 磁带 C 光盘D 软盘 |
| 1327 | 下列叙述不属于完全备份机制特点描述的是\_\_D\_\_。 |
|  | A 每次备份的数据量较大B 每次备份所需的时间也就较长C 不能进行得太频繁 D 需要存储空间小 |
| 1328 | 下面不属于容灾内容的是\_\_\_A\_。 |
|  | A 灾难预测 B 灾难演习C 风险分析D 业务影响分析 |
| 1329 | 信息系统的容灾方案通常要考虑的要点有\_ABCDE\_\_\_。 |
|  | A 灾难的类型 B 恢复时间 C 恢复程度 D 实用技术 E 成本 |
| 1330 | 系统数据备份包括的对象有\_\_\_ABD\_。 |
|  | A 配置文件 B 日志文件 C 用户文档 D 系统设备文件 |
| 1331 | 容灾等级越高，则\_\_\_ACD\_。 |
|  | A 业务恢复时间越短 B 所需人员越多 C 所需要成本越高 D 保护的数据越重要 |
| 1332 | 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。 |
|  | A 正确 B 错误 A |
| 1333 | 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。A |
|  | A 正确 B 错误 |
| 1334 | 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。A |
|  | A 正确 B 错误 |
| 1335 | 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。A |
|  | A 正确 B 错误 |
| 1336 | 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。A |
|  | A 正确 B 错误 |
| 1337 | PKI系统的基本组件包括\_\_ACDBEF\_\_。 |
|  | 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 |
| 1338 | 数字证书可以存储的信息包括\_ABCD\_\_\_。 |
|  | 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 |
| 1339 | PKI提供的核心服务包括\_ABCD\_\_\_。 |
|  | A 认证 B 完整性 C 密钥管理 D 简单机密性 E 非否认 |
| 1340 | 常见的操作系统包括DOS、0S／2、UNIX、XENIX、Linux、Windows、Netware、Oracle等。 |
|  | A 正确 B 错误 |
| 1341 | 操作系统在概念上一般分为两部分：内核(Kernel)以及壳(Shell)，有些操作系统的内核与壳完全分开(如Microsoft Windows、UNIX、Linux等)；另一些的内核与壳关系紧密(如UNIX、Linux等)，内核及壳只是操作层次上不同而已。B |
|  | A 正确 B 错误 |
| 1342 | 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。B |
|  | A 正确 B 错误 |
| 1343 | Windows系统的用户帐号有两种基本类型：全局帐号(GlobalAccounts)和本地帐号(LocalAccounts)。 |
|  | A 正确 B 错误 A |
| 1344 | 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。B |
|  | A 正确 B 错误 |
| 1345 | 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。A |
|  | A 正确 B 错误 |
| 1346 | 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。B |
|  | A 正确 B 错误 |
| 1347 | 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。B |
|  | A 正确 B 错误 |
| 1348 | 在默认情况下，内置DomainAdmins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。A |
|  | A 正确 B 错误 |
| 1349 | 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。B |
|  | A 正确 B 错误 |
| 1350 | 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BackupOperators组有此权限，而Lois又是该组成员，则Lois也有此权限。A |
|  | A 正确 B 错误 |
| 1351 | Windows文件系统中，只有Administrator组和ServerOperation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。B |
|  | A 正确 B 错误 |
| 1352 | 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。 |
|  | A 正确 B 错误 B |
| 1353 | 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。A |
|  | A 正确 B 错误 |
| 1354 | 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。B |
|  | A 正确 B 错误 |
| 1355 | 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。B |
|  | A 正确 B 错误 |
| 1356 | 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。A |
|  | A 正确 B 错误 |
| 1357 | 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。A |
|  | A 正确 B 错误 |
| 1358 | 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只定义了一个操作系统内核。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。 |
|  | A 正确 B 错误 |
| 1359 | 每个UNIX／Linux系统中都只有一个特权用户，就是root帐号。B |
|  | A 正确 B 错误 |
| 1360 | 与Windows系统不一样的是UNIX／Linux操作系统中不存在预置帐号。B |
|  | A 正确 B 错误 |
| 1361 | UNIX／Linux系统中一个用户可以同时属于多个用户组。A |
|  | A 正确 B 错误 |
| 1362 | 标准的UNIX／Linux系统以属主(Owner)、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。A |
|  | A 正确 B 错误 |
| 1363 | 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。 |
|  | A 正确 B 错误 B |
| 1364 | UNIX／Linux系统和Windows系统类似，每一个系统用户都有一个主目录。A |
|  | A 正确 B 错误 |
| 1365 | 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。B |
|  | A 正确 B 错误 |
| 1366 | UNIX／Linux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。 B |
|  | A 正确 B 错误 |
| 1367 | Httpd.conf是Web服务器的主配置文件，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。 A |
|  | A 正确 B 错误 |
| 1368 | 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。B |
|  | A 正确 B 错误 |
| 1369 | UNIX／Linux系统中的／etc／shadow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／etc／passwd文件中)。B |
|  | A 正确 B 错误 |
| 1370 | 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。B |
|  | A 正确 B 错误 |
| 1371 | 数据库安全只依靠技术即可保障。B |
|  | A 正确 B 错误 |
| 1372 | 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。B |
|  | A 正确 B 错误 |
| 1373 | 数据库的强身份认证与强制访问控制是同一概念。B |
|  | A 正确 B 错误 |
| 1374 | 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。A |
|  | A 正确 B 错误 |
| 1375 | 数据库视图可以通过INSERT或UPDATE语句生成。B |
|  | A 正确 B 错误 |
| 1376 | 数据库加密适宜采用公开密钥密码系统。A |
|  | A 正确 B 错误 |
| 1377 | 数据库加密的时候，可以将关系运算的比较字段加密。B |
|  | A 正确 B 错误 |
| 1378 | 数据库管理员拥有数据库的一切权限。A |
|  | A 正确 B 错误 |
| 1379 | 不需要对数据库应用程序的开发者制定安全策略。B |
|  | A 正确 B 错误 |
| 1380 | 使用登录ID登录SQL Server后，即获得了访问数据库的权限。B |
|  | A 正确 B 错误 |
| 1381 | MS SQL Server与Sybase SQL Server的身份认证机制基本相同。A |
|  | A 正确 B 错误 |
| 1382 | SQL Server不提供字段粒度的访问控制。B |
|  | A 正确 B 错误 |
| 1383 | MySQL不提供字段粒度的访问控制。A |
|  | A 正确 B 错误 |
| 1384 | SQL Server中，权限可以直接授予用户ID。A |
|  | A 正确 B 错误 |
| 1385 | SQL注入攻击不会威胁到操作系统的安全。B |
|  | A 正确 B 错误 |
| 1386 | 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。A |
|  | A 正确 B 错误 |
| 1387 | 完全备份就是对全部数据库数据进行备份。A |
|  | A 正确 B 错误 |
| 1388 | 美国国防部发布的可信计算机系统评估标准(TCSEC)定义了\_\_\_C\_个等级。 |
|  | A 五B 六 C 七 D 八 |
| 1389 | 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 B 域帐号C 来宾帐号D 局部帐号 |
| 1390 | Windows系统安装完后，默认隋况下系统将产生两个帐号，分别是管理员帐号和\_\_C\_\_。 |
|  | A 本地帐号B 域帐号 C 来宾帐号 D 局部帐号 |
| 1391 | 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 |
| 1392 | —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\_\_\_\_和\_\_\_\_。 |
|  | A 12 8B 14 10C 12 10 D 14 8 |
| 1393 | 符合复杂性要求的WindowsXP帐号密码的最短长度为\_\_\_\_。 |
|  | A 4 B 6 C 8D 10 |
| 1394 | 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\_\_\_\_。 |
|  | A kedaB kedaliu C kedawuj D dawu |
| 1395 | 某公司的工作时间是上午8点半至12点，下午1点555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\_\_\_\_。 |
|  | A 上午8点B 中午12点C 下午3点 D 凌晨l点 |
| 1396 | 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\_\_\_\_。 |
|  | 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 |
| 1397 | 在正常情况下，Windows 2000中建议关闭的服务是\_\_\_\_。 |
|  | A TCP／IP NetBIOS Helper Service B Logical Disk ManagerC Remote Procedure CallD Security Accounts Manager |
| 1398 | FTP(文件传输协议，File Transfer Protocol，简称FFP)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\_\_\_\_。 |
|  | A 25 21 80 554 B 21 25 80 443 C 21 110 80 554D 21 25 443 554 |
| 1399 | 下面不是UNIX／Linux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 |
| 1400 | 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 |
| 1401 | 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NFSDaemon 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NFSDaemon，其中安全性能较强的是基于内核的NFSDaemonC UNIX系统中现只有一种NFS服务器，就是基于内核的NFSDaemon，原有的用户空间Daemon已经被淘汰，因为NFSDaemon安全性能较好D UNIX系统中现只有一种NFS服务器，就是基于内核的Daemon，原有的用户空间NFSDaemon已经被淘汰，因为Daemon安全性能较好 |
| 1402 | 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 tarB cpio C umask D backup |
| 1403 | 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—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 |
| 1404 | UNIX工具(实用程序，utilities)在新建文件的时候，通常使用\_\_\_\_作为缺省许可位，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 888D 888 999 |
| 1405 | 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／groupC 设置足够强度的帐号密码D 使用shadow密码 |
| 1406 | UNIX／Linux系统中，下列命令可以将普通帐号变为root帐号的是\_\_\_\_。 |
|  | A chmod命令B ／bin／passwd命令C chgrp命令 D ／bin／su命令 |
| 1407 | 有编辑／etc／passwd文件能力的攻击者可以通过把UID变为\_\_\_\_就可以成为特权用户。 |
|  | A -1 B 0 C 1D 2 |
| 1408 | 下面不是保护数据库安全涉及到的任务是\_\_\_\_。 |
|  | 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 |
| 1409 | 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 |
| 1410 | 关于用户角色，下面说法正确的是\_\_\_\_。 |
|  | A SQL Server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 |
| 1411 | 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D 自主原则 |
| 1412 | 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 |
| 1413 | 有关数据库加密，下面说法不正确的是\_\_\_\_。 |
|  | 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 |
| 1414 | 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 |
| 1415 | 下面不是SQL Server支持的身份认证方式的是\_\_\_\_。 |
|  | A Windows NT集成认证B SQL Server认证C SQL Server混合认证 D 生物认证 |
| 1416 | 下面\_\_\_\_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RDBMSD 开放源码数据库 |
| 1417 | 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 |
| 1418 | 下面不是Oracle数据库支持的备份形式的是\_\_\_\_。 |
|  | A 冷备份 B 温备份 C 热备份D 逻辑备份 |
| 1419 | 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 |
| 1420 | 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 |
| 1421 | 根据SahzerJ.H、SchroederM.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 |
| 1422 | 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 |
| 1423 | 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(SecurityAccountManager，简称SAM)模块 B Windows系统的注册(WinLogon)模块 C 本地安全认证(10calSecurityAuthority，简称LSA)模块 D 安全引用监控器模块 |
| 1424 | 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\_\_\_\_。 |
|  | A DomainAdmins组 B DomainUsers组 C DomainReplicators组 D Domain Guests组 |
| 1425 | 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(ApplicationsLog) D 用户日志(UserLog) |
| 1426 | 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 |
| 1427 | UNIX／Linux系统中的密码控制信息保存在／etc／passwd或／ect／shadow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 密码最近的改变时间 D 密码有效的最大天数 |
| 1428 | 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\_\_\_\_。 |
|  | A 利用HTYP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 |
| 1429 | 数据库访问控制的粒度可能有\_\_\_\_。 |
|  | A 数据库级 B 表级 C 记录级(行级) D 属性级(字段级) E 字符级 |
| 1430 | 下面标准可用于评估数据库的安全级别的有\_\_\_\_。 |
|  | A TCSEC B ITSEC C CC DBMS.PP D GB 17859——1999 E TDI |
| 1431 | 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 模式对象设计 E 外部对象审计 |
| 1432 | SQL Server中的预定义服务器角色有\_\_\_\_。 |
|  | A sysadmin B serveradmin C setupadmin D securityadmin E processadmin |
| 1433 | 可以有效限制SQL注入攻击的措施有\_\_\_\_。 |
|  | A 限制DBMS中sysadmin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 |
| 1434 | 事务的特性有\_\_\_\_。 |
|  | A 原子性(Atomicity) B 一致性(Consistency) C 隔离性(1solation) D 可生存性(Survivability) E 持续性(Durability) |
| 1435 | 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 |
| 1436 | 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。 |
|  | A 正确 B 错误 |
| 1437 | 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(DynamicPacketFilter)。 |
|  | A 正确 B 错误 |
| 1438 | 软件防火墙就是指个人防火墙。 |
|  | A 正确 B 错误 |
| 1439 | 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。 |
|  | A 正确 B 错误 |
| 1440 | 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。 |
|  | A 正确 B 错误 |
| 1441 | 防火墙安全策略一旦设定，就不能在再做任何改变。 |
|  | A 正确 B 错误 |
| 1442 | 对于防火墙的管理可直接通过Telnet进行。 |
|  | A 正确 B 错误 |
| 1443 | 防火墙规则集的内容决定了防火墙的真正功能。 |
|  | A 正确 B 错误 |
| 1444 | 防火墙必须要提供VPN、NAT等功能。 |
|  | A 正确 B 错误 |
| 1445 | 防火墙对用户只能通过用户名和口令进行认证。 |
|  | A 正确 B 错误 |
| 1446 | 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。 |
|  | A 正确 B 错误 |
| 1447 | 只要使用了防火墙，企业的网络安全就有了绝对的保障。 |
|  | A 正确 B 错误 |
| 1448 | 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。 |
|  | A 正确 B 错误 |
| 1449 | iptables可配置具有状态包过滤机制的防火墙。 |
|  | A 正确 B 错误 |
| 1450 | 可以将外部可访问的服务器放置在内部保护网络中。 |
|  | A 正确 B 错误 |
| 1451 | 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。 |
|  | A 正确 B 错误 |
| 1452 | 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。 |
|  | A 正确 B 错误 |
| 1453 | 主动响应和被动响应是相互对立的，不能同时采用。 |
|  | A 正确 B 错误 |
| 1454 | 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。 |
|  | A 正确 B 错误 |
| 1455 | 针对入侵者采取措施是主动响应中最好的响应措施。 |
|  | A 正确 B 错误 |
| 1456 | 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。 |
|  | A 正确 B 错误 |
| 1457 | 性能“瓶颈”是当前入侵防御系统面临的一个挑战。 |
|  | A 正确 B 错误 |
| 1458 | 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。 |
|  | A 正确 B 错误 |
| 1459 | 与入侵检测系统不同，入侵防御系统采用在线(inline)方式运行。 |
|  | A 正确 B 错误 |
| 1460 | 蜜罐技术是一种被动响应措施。 |
|  | A 正确 B 错误 |
| 1461 | 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。 |
|  | A 正确 B 错误 |
| 1462 | 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。 |
|  | A 正确 B 错误 |
| 1463 | 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。 |
|  | A 正确 B 错误 |
| 1464 | 在早期用集线器(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子网。 |
|  | A 正确 B 错误 |
| 1465 | 可以通过技术手段，一次性弥补所有的安全漏洞。 |
|  | A 正确 B 错误 |
| 1466 | 漏洞只可能存在于操作系统中，数据库等其他软件系统不会存在漏洞。 |
|  | A 正确 B 错误 |
| 1467 | 防火墙中不可能存在漏洞。 |
|  | A 正确 B 错误 |
| 1468 | 基于主机的漏洞扫描不需要有主机的管理员权限。 |
|  | A 正确 B 错误 |
| 1469 | 半连接扫描也需要完成TCP协议的三次握手过程。 |
|  | A 正确 B 错误 |
| 1470 | 使用漏洞库匹配的方法进行扫描，可以发现所有的漏洞。 |
|  | A 正确 B 错误 |
| 1471 | 所有的漏洞都是可以通过打补丁来弥补的。 |
|  | A 正确 B 错误 |
| 1472 | 通过网络扫描，可以判断目标主机的操作系统类型。 |
|  | A 正确 B 错误 |
| 1473 | x-scan能够进行端口扫描。 |
|  | A 正确 B 错误 |
| 1474 | 隔离网闸采用的是物理隔离技术。 |
|  | A 正确 B 错误 |
| 1475 | “安全通道隔离”是一种逻辑隔离。 |
|  | A 正确 B 错误 |
| 1476 | 隔离网闸两端的网络之间不存在物理连接。 |
|  | A 正确 B 错误 |
| 1477 | QQ是与朋友联机聊天的好工具，不必担心病毒。 |
|  | A 正确 B 错误 |
| 1478 | 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。 |
|  | A 正确 B 错误 |
| 1479 | 计算机病毒可能在用户打开“txt”文件时被启动。 |
|  | A 正确 B 错误 |
| 1480 | 在安全模式下木马程序不能启动。 |
|  | A 正确 B 错误 |
| 1481 | 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。 |
|  | A 正确 B 错误 |
| 1482 | 家里的计算机没有联网，所以不会感染病毒。 |
|  | A 正确 B 错误 |
| 1483 | 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。 |
|  | A 正确 B 错误 |
| 1484 | 校验和技术只能检测已知的计算机病毒。 |
|  | A 正确 B 错误 |
| 1485 | 采用Rootkit 技术的病毒可以运行在内核模式中。 |
|  | A 正确 B 错误 |
| 1486 | 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。 |
|  | A 正确 B 错误 |
| 1487 | 大部分恶意网站所携带的病毒就是脚本病毒。 |
|  | A 正确 B 错误 |
| 1488 | 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。 |
|  | A 正确 B 错误 |
| 1489 | 防火墙是\_\_\_\_在网络环境中的应用。 |
|  | A 字符串匹配 B 访问控制技术 C 入侵检测技术D 防病毒技术 |
| 1490 | iptables中默认的表名是\_\_\_\_。 |
|  | A filter B firewallC natD mangle |
| 1491 | 包过滤防火墙工作在OSI网络参考模型的\_\_\_\_。 |
|  | A 物理层B 数据链路层 C 网络层 D 应用层 |
| 1492 | 通过添加规则，允许通往192.168.0.2的SSH连接通过防火墙的iptables指令是\_\_\_\_。 |
|  | A iptables -F INPUT -d 192.168.0.2 -p tcp--dport 22 -j ACCEPTB iptables -A INPUT -d 192.168.0.2 -p tcp--dport 23 -j ACCEPT C iptables -A FORWARD -d 192.168.0.2 -p tcp--dport22 -j ACCEPT D iptables -A FORWARD -d 192.168.0.2 -p tcp--dport 23 -j ACCEPT |
| 1493 | 防火墙提供的接入模式不包括\_\_\_\_。 |
|  | A 网关模式B 透明模式C 混合模式 D 旁路接入模式 |
| 1494 | 关于包过滤防火墙说法错误的是\_\_\_\_。 |
|  | A 包过滤防火墙通常根据数据包源地址、目的地址、端口号和协议类型等标志设置访问控制列表实施对数据包的过滤B 包过滤防火墙不检查OSI网络参考模型中网络层以上的数据，因此可以很快地执行 C 包过滤防火墙可以有效防止利用应用程序漏洞进行的攻击 D 由于要求逻辑的一致性、封堵端口的有效性和规则集的正确性，给过滤规则的制定和配置带来了复杂性，一般操作人员难以胜任管理，容易出现错误 |
| 1495 | 关于应用代理网关防火墙说法正确的是\_\_\_\_。 |
|  | A 基于软件的应用代理网关工作在OSI网络参考模型的网络层上，它采用应用协议代理服务的工作方式实施安全策略 B 一种服务需要一种代理模块，扩展服务较难 C 和包过滤防火墙相比，应用代理网关防火墙的处理速度更快D 不支持对用户身份进行高级认证机制。一般只能依据包头信息，因此很容易受到“地址欺骗型”攻击 |
| 1496 | 关于NAT说法错误的是\_\_\_\_。 |
|  | A NAT允许一个机构专用Intranet中的主机透明地连接到公共域中的主机，无需内部主机拥有注册的(已经越采越缺乏的)全局互联网地址B 静态NAT是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址C 动态NAT主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态NAT就会分配给用户一个IP地址，当用户断开时，这个IP地址就会被释放而留待以后使用 D 动态NAT又叫做网络地址端口转换NAPT |
| 1497 | 下面关于防火墙策略说法正确的是\_\_\_\_。 |
|  | A 在创建防火墙策略以前，不需要对企业那些必不可少的应用软件执行风险分析B 防火墙安全策略一旦设定，就不能在再作任何改变 C 防火墙处理人站通信的缺省策略应该是阻止所有的包和连接，除了被指出的允许通过的通信类型和连接 D 防火墙规则集与防火墙平台体系结构无关 |
| 1498 | 下面关于DMZ区的说法错误的是\_\_\_\_。 |
|  | A 通常DMZ包含允许来自互联网的通信可进入的设备，如Web服务器、FTP服务器、SMTP服务器和DNS服务器等B 内部网络可以无限制地访问外部网络以及DMZ C DMZ可以访问内部网络 D 有两个DMZ的防火墙环境的典型策略是主防火墙采用NAT方式工作，而内部防火墙采用透明模式工作以减少内部网络结构的复杂程度 |
| 1499 | 在PDRR模型中，\_\_\_\_是静态防护转化为动态的关键，是动态响应的依据。 |
|  | A 防护 B 检测 C 响应D 恢复 |
| 1500 | 从系统结构上来看，入侵检测系统可以不包括\_\_\_\_。 |
|  | A 数据源B 分析引擎 C 审计 D 响应 |
| 1501 | 通用入侵检测框架(CIDF)模型中，\_\_\_\_的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。 |
|  | A 事件产生器 B 事件分析器C 事件数据库D 响应单元 |
| 1502 | 基于网络的入侵检测系统的信息源是\_\_\_\_。 |
|  | A 系统的审计日志B 系统的行为数据C 应用程序的事务日志文件 D 网络中的数据包 |
| 1503 | 误用入侵检测技术的核心问题是\_\_\_\_的建立以及后期的维护和更新。 |
|  | A 异常模型B 规则集处理引擎 C 网络攻击特征库 D 审计日志 |
| 1504 | \_\_\_\_是在蜜罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个蜜罐，来构成一个黑客诱捕网络体系架构。 |
|  | A 蜜网 B 鸟饵C 鸟巢D 玻璃鱼缸 |
| 1505 | 下面关于响应的说法正确的是\_\_\_\_。 |
|  | A 主动响应和被动响应是相互对立的，不能同时采用B 被动响应是入侵检测系统中的唯一响应方式C 入侵检测系统提供的警报方式只能是显示在屏幕上的警告信息或窗口 D 主动响应的方式可以是自动发送邮件给入侵发起方的系统管理员请求协助以识别问题和处理问题 |
| 1506 | 下面说法错误的是\_\_\_\_。 |
|  | A 由于基于主机的入侵检测系统可以监视一个主机上发生的全部事件，它们能够检测基于网络的入侵检测系统不能检测的攻击B 基于主机的入侵检测可以运行在交换网络中 C 基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描 D 基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击，因为应用程序日志并不像操作系统审计追踪日志那样被很好地保护 |
| 1507 | 使用漏洞库匹配的扫描方法，能发现\_\_\_\_。 |
|  | A 未知的漏洞 B 已知的漏洞 C 自行设计的软件中的漏洞D 所有漏洞 |
| 1508 | 下面\_\_\_\_不可能存在于基于网络的漏洞扫描器中。 |
|  | A 漏洞数据库模块B 扫描引擎模块C 当前活动的扫描知识库模块 D 阻断规则设置模块 |
| 1509 | 网络隔离技术，根据公认的说法，迄今已经发展了\_\_\_\_个阶段。 |
|  | A 六 B 五 C 四D 三 |
| 1510 | 下面关于隔离网闸的说法，正确的是\_\_\_\_。 |
|  | A 能够发现已知的数据库漏洞B 可以通过协议代理的方法，穿透网闸的安全控制 C 任何时刻，网闸两端的网络之间不存在物理连接 D 在OSI的二层以上发挥作用 |
| 1511 | 关于网闸的工作原理，下面说法错误的是\_\_\_\_. |
|  | A 切断网络之间的通用协议连接B 将数据包进行分解或重组为静态数据；对静态数据进行安全审查，包括网络协议检查和代码扫描等 C 网闸工作在OSI模型的二层以上 D 任何时刻，网闸两端的网络之间不存在物理连接 |
| 1512 | 当您收到您认识的人发来的电子邮件并发现其中有意外附件，您应该\_\_\_\_。 |
|  | A 打开附件，然后将它保存到硬盘B 打开附件，但是如果它有病毒，立即关闭它 C 用防病毒软件扫描以后再打开附件 D 直接删除该邮件 |
| 1513 | 下面病毒出现的时间最晚的类型是\_\_\_\_. |
|  | A 携带特洛伊木马的病毒 B 以网络钓鱼为目的的病毒 C 通过网络传播的蠕虫病毒D Office文档携带的宏病毒 |
| 1514 | 某病毒利用RPCDCOM缓冲区溢出漏洞进行传播，病毒运行后，在％System％文件夹下生成自身的拷贝nvchip4.exe，添加注册表项，使得自身能够在系统启动时自动运行。通过以上描述可以判断这种病毒的类型为\_\_\_\_。 |
|  | A 文件型病毒B 宏病毒 C 网络蠕虫病毒 D 特洛伊木马病毒 |
| 1515 | 采用“进程注入”可以\_\_\_\_。 |
|  | A 隐藏进程B 隐藏网络端口 C 以其他程序的名义连接网络 D 以上都正确 |
| 1516 | 下列关于启发式病毒扫描技术的描述中错误的是\_\_\_\_。 |
|  | A 启发式病毒扫描技术是基于人工智能领域的启发式搜索技术B 启发式病毒扫描技术不依赖于特征代码来识别计算机病毒 C 启发式病毒扫描技术不会产生误报，但可能会产生漏报 D 启发式病毒扫描技术能够发现一些应用了已有机制或行为方式的病毒 |
| 1517 | 不能防止计算机感染病毒的措施是\_\_\_\_\_。 |
|  | A 定时备份重要文件 B 经常更新操作系统C 除非确切知道附件内容，否则不要打开电子邮件附件D 重要部门的计算机尽量专机专用与外界隔绝 |
| 1518 | 企业在选择防病毒产品时不应该考虑的指标为\_\_\_\_。 |
|  | A 产品能够从一个中央位置进行远程安装、升级B 产品的误报、漏报率较低C 产品提供详细的病毒活动记录 D 产品能够防止企业机密信息通过邮件被传出 |
| 1519 | 防火墙通常阻止的数据包包括\_\_\_\_。 |
|  | A 来自未授权的源地址且目的地址为防火墙地址的所有入站数据包(除Email传递等特殊用处的端口外) B 源地址是内部网络地址的所有入站数据包 C 所有ICMP类型的入站数据包 D 来自未授权的源地址，包含SNMP的所有入站数据包 E 包含源路由的所有入站和出站数据包 |
| 1520 | 目前市场上主流防火墙提供的功能包括\_\_\_\_。 |
|  | A 数据包状态检测过滤 B 应用代理 C NAT D VPN E 日志分析和流量统计分析 |
| 1521 | 防火墙的局限性包括\_\_\_\_。 |
|  | A 防火墙不能防御绕过了它的攻击 B 防火墙不能消除来自内部的威胁 C 防火墙不能对用户进行强身份认证 D 防火墙不能阻止病毒感染过的程序和文件进出网络 |
| 1522 | 防火墙的性能的评价方面包括\_\_\_\_。 |
|  | A 并发会话数 B 吞吐量 C 延时 D 平均无故障时间 |
| 1523 | 下面关于防火墙的维护和策略制定说法正确的是\_\_\_\_。 |
|  | A 所有防火墙管理功能应该发生在使用了强认证和加密的安全链路上 B Web界面可以通过SSL加密用户名和密码。非Web的图形界面如果既没有内部加密，也没有SSL，可以使用隧道解决方案，如SSH C 对防火墙策略进行验证的最简单的方法是，获得防火墙配置的拷贝，然后把这些拷贝和根据已定义的策略产生的期望配置进行比较 D 对防火墙策略进行验证的另一种方式通过使用软件对防火墙配置进行实际测试 E 渗透分析可以取代传统的审计程序 |
| 1524 | 蜜罐技术的主要优点有\_\_\_\_。 |
|  | A 蜜罐技术属于被动响应，使用者没有成为刑事诉讼或民事诉讼对象的危险 B 收集数据的真实性，蜜罐不提供任何实际的业务服务，所以搜集到的信息很大可能性都是由于黑客攻击造成的，漏报率和误报率都比较低 C 可以收集新的攻击工具和攻击方法，不像目前的大部分防火墙和入侵检测系统只能根据特征匹配方法来检测已知的攻击 D 不需要强大的资金投入，可以用一些低成本的设备 E 可以及时地阻断网络入侵行为 |
| 1525 | 通用入侵检测框架(CIDF)模型的组件包括\_\_\_\_。 |
|  | A 事件产生器 B 活动轮廓 C 事件分析器 D 事件数据库 E 响应单元 |
| 1526 | 主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有\_\_\_\_。 |
|  | A 针对入侵者采取措施 B 修正系统 C 收集更详细的信息 D 入侵追踪 |
| 1527 | 随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器(sniffer)来监听整个子网的办法不再可行。可选择解决的办法有\_\_\_\_。 |
|  | A 不需要修改，交换网络和以前共享媒质模式的网络没有任何区别 B 使用交换机的核心芯片上的一个调试的端口 C 把入侵检测系统放在交换机内部或防火墙等数据流的关键入口、出口处 D 采用分接器(tap) E 使用以透明网桥模式接入的入侵检测系统 |
| 1528 | 入侵防御技术面临的挑战主要包括\_\_\_\_。 |
|  | A 不能对入侵活动和攻击性网络通信进行拦截 B 单点故障 C 性能“瓶颈” D 误报和漏报 |
| 1529 | 网络安全扫描能够\_\_\_\_。 |
|  | A 发现目标主机或网络 B 判断操作系统类型 C 确认开放的端口 D 识别网络的拓扑结构 E 测试系统是否存在安全漏洞 |
| 1530 | 主机型漏洞扫描器可能具备的功能有\_\_\_\_。 |
|  | A 重要资料锁定：利用安全的校验和机制来监控重要的主机资料或程序的完整性 B 弱口令检查：采用结合系统信息、字典和词汇组合等的规则来检查弱口令 C 系统日志和文本文件分析：针对系统日志档案，如UNIX的syslogs及NT的事件日志(EventLog)，以及其他文本文件的内容做分析 D 动态报警：当遇到违反扫描策略或发现已知安全漏洞时，提供及时的告警。告警可以采取多种方式，可以是声音、弹出窗口、电子邮件甚至手机短信等 E 分析报告：产生分析报告，并告诉管理员如何弥补漏洞 |
| 1531 | 下面对于x-scan扫描器的说法，正确的有\_\_\_\_。 |
|  | A 可以进行端口扫描 B 含有攻击模块，可以针对识别到的漏洞自动发起攻击 C 对于一些已知的CGI和RPC漏洞，x-scan给出了相应的漏洞描述以及已有的通过此漏洞进行攻击的工具 D 需要网络中每个主机的管理员权限 E 可以多线程扫描 |
| 1532 | 下面软件产品中，\_\_\_\_是漏洞扫描器。 |
|  | A x-scan B nmap C Internet Scanner D Norton AntiVirusE Snort |
| 1533 | 隔离网闸的三个组成部分是\_\_\_\_。 |
|  | A 漏洞扫描单元B 入侵检测单元 C 内网处理单元 D 外网处理单元 E 专用隔离硬件交换单元 |
| 1534 | 网闸可能应用在\_\_\_\_。 |
|  | A 涉密网与非涉密网之间 B 办公网与业务网之间 C 电子政务的内网与专网之间 D 业务网与互联网之间 E 局域网与互联网之间 |
| 1535 | 下面不是网络端口扫描技术的是\_\_\_\_。 |
|  | A 全连接扫描B 半连接扫描 C 插件扫描 D 特征匹配扫描 E 源码扫描 |
| 1536 | 按照2000年3月公布的《计算机病毒防治管理办法》对计算机病毒的定义，下列属于计算机病毒的有\_\_\_\_。 |
|  | A 某Word文档携带的宏代码，当打开此文档时宏代码会搜索并感染计算机上所有的Word文档 B 某用户收到来自朋友的一封电子邮件，当打开邮件附件时，邮件附件将自身发送给该用户地址簿中前五个邮件地址 C 某员工在公司内部使用的系统中加入一个逻辑炸弹，如果该员工在一年内被解雇则逻辑炸弹就会破坏系统D 黑客入侵了某服务器，并在其上安装了一个后门程序 E 某QQ用户打开了朋友发送来的一个链接后，发现每次有好友上线QQ都会自动发送一个携带该链接的消息 |
| 1537 | 病毒传播的途径有\_\_\_\_。 |
|  | A 移动硬盘 B 内存条 C 电子邮件 D 聊天程序 E 网络浏览 |
| 1538 | 可能和计算机病毒有关的现象有\_\_\_\_。 |
|  | A 可执行文件大小改变了 B 在向写保护的U盘复制文件时屏幕上出现U盘写保护的提示 C 系统频繁死机 D 内存中有来历不明的进程 E 计算机主板损坏 |
| 1539 | 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。 |
|  | A 正确 B 错误 |
| 1540 | 反向查询方法可以让接收邮件的互联网服务商确认邮件发送者是否就是如其所言的真实地址。 |
|  | A 正确 B 错误 |
| 1541 | SenderlD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。 |
|  | A 正确 B 错误 |
| 1542 | DKIM(Domain Keys Identified 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。 |
|  | A 正确 B 错误 |
| 1543 | 运行防病毒软件可以帮助防止遭受网页仿冒欺诈。 |
|  | A 正确 B 错误 |
| 1544 | 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。 |
|  | A 正确 B 错误 |
| 1545 | 网络钓鱼的目标往往是细心选择的一些电子邮件地址。 |
|  | A 正确 B 错误 |
| 1546 | 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。 |
|  | A 正确 B 错误 |
| 1547 | 在来自可信站点的电子邮件中输入个人或财务信息是安全的。 |
|  | A 正确 B 错误 |
| 1548 | 包含收件人个人信息的邮件是可信的。 |
|  | A 正确 B 错误 |
| 1549 | 可以采用内容过滤技术来过滤垃圾邮件。 |
|  | A 正确 B 错误 |
| 1550 | 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。 |
|  | A 正确 B 错误 |
| 1551 | 随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模块成为信息安全领域的一个发展趋势。 |
|  | A 正确 B 错误 |
| 1552 | 启发式技术通过查找通用的非法内容特征，来尝诩蝴IJ新形式和已知形式的非法内容。 |
|  | A 正确 B 错误 |
| 1553 | 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。 |
|  | A 正确 B 错误 |
| 1554 | 实时黑名单是简单黑名单的进—步发展，可以从根本上解决垃圾邮件问题。 |
|  | A 正确 B 错误 |
| 1555 | 贝叶斯过滤技术具有自适应、自学习的能力，目前已经得到了广泛的应用。 |
|  | A 正确 B 错误 |
| 1556 | 对网页请求参数进行验证，可以防止SQL注入攻击。 |
|  | A 正确 B 错误 |
| 1557 | 以下不会帮助减少收到的垃圾邮件数量的是\_\_\_\_。 |
|  | A 使用垃圾邮件筛选器帮助阻止垃圾邮件B 共享电子邮件地址或即时消息地址时应小心谨慎 C 安装入侵检测软件 D 收到垃圾邮件后向有关部门举报 |
| 1558 | 下列不属于垃圾邮件过滤技术的是\_\_\_\_。 |
|  | A 软件模拟技术 B 贝叶斯过滤技术C 关键字过滤技术D 黑名单技术 |
| 1559 | 下列技术不支持密码验证的是\_\_\_\_。 |
|  | A S／MIMEB PGPC AMTP D SMTP |
| 1560 | 下列行为允许的有\_\_\_\_。 |
|  | A 未经授权利用他人的计算机系统发送互联网电子邮件B 将采用在线自动收集、字母或者数字任意组合等手段获得的他人的互联网电子邮件地址用于出售、共享、交换或者向通过上述方式获得的电子邮件地址发送互联网电子邮件C 未经互联网电子邮件接收者明确伺意，向其发送包含商业广告内容的互联网电子邮件 D 爱选包含商业广告内容的互联网电子邮件时，在互联网电子邮件标题信息前部注明“广告”或者“AD'’字样 |
| 1561 | 下列技术不能使网页被篡改后能够自动恢复的是\_\_\_\_。 |
|  | A 限制管理员的权限 B 轮询检测C 事件触发技术D 核心内嵌技术 |
| 1562 | 以下不可以表示电子邮件可能是欺骗性的是\_\_\_\_。 |
|  | A 它要求您点击电子邮件中的链接并输入您的帐户信息B 传达出一种紧迫感 C 通过姓氏和名字称呼您 D 它要求您验证某些个人信息 |
| 1563 | 如果您认为您已经落入网络钓鱼的圈套，则应采取\_\_\_\_措施。 |
|  | A 向电子邮件地址或网站被伪造的公司报告该情形B 更改帐户的密码C 立即检查财务报表 D 以上全部都是 |
| 1564 | 内容过滤技术的含义不包括\_\_\_\_。 |
|  | A 过滤互联网请求从而阻止用户浏览不适当的内容或站点B 过滤流入的内容从而阻止潜在的攻击进入用户的网络系统C 过滤流出的内容从而阻止敏感数据的泄漏 D 过滤用户的输入从而阻止用户传播非法内容 |
| 1565 | 下列内容过滤技术中在我国没有得到广泛应用的是\_\_\_\_。 |
|  | A 内容分级审查 B 关键字过滤技术C 启发式内容过滤技术D 机器学习技术 |
| 1566 | 会让一个用户的“删除”操作去警告其他许多用户的垃圾邮件过滤技术是\_\_\_\_。 |
|  | A 黑名单B 白名单C 实时黑名单 D 分布式适应性黑名单 |
| 1567 | 不需要经常维护的垃圾邮件过滤技术是\_\_\_\_。 |
|  | A 指纹识别技术 B 简单DNS测试 C 黑名单技术D 关键字过滤 |
| 1568 | 下列关于网络钓鱼的描述不正确的是\_\_\_\_。 |
|  | A 网络钓鱼(Phishing)一词，是“Fishing”和“Phone”的综合体 B 网络钓鱼都是通过欺骗性的电子邮件来进行诈骗活动 C 为了消除越来越多的以网络钓鱼和电子曲6件欺骗的形式进行的身份盗窃和欺诈行为，相关行业成立了一个协会——反网络钓鱼工作小组D 网络钓鱼在很多方面和一般垃圾邮件有所不同，理解这些不同点对设计反网络钓鱼技术至关重要 |
| 1569 | 下面技术中不能防止网络钓鱼攻击的是\_\_\_\_。 |
|  | A 在主页的底部设有一个明显链接，以提醒用户注意有关电子邮件诈骗的问题B 利用数字证书(如 USB KEY)进行登录 C 根据互联网内容分级联盟(ICRA)提供的内容分级标准对网站内容进行分级 D 安装杀毒软件和防火墙、及时升级、打补丁、加强员工安全意识 |
| 1570 | 下列邮件为垃圾邮件的有\_\_\_\_。 |
|  | A 收件人无法拒收的电子邮件 B 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件 C 含有病毒、色情、反动等不良信息或有害信息的邮件 D 隐藏发件人身份、地址、标题等信息的电子邮件 E 含有虚假的信息源、发件人、路由等信息的电子邮件 |
| 1571 | 垃圾邮件带来的危害有\_\_\_\_。 |
|  | A 垃圾邮件占用很多互联网资源 B 垃圾邮件浪费广大用户的时间和精力 C 垃圾邮件提高了某些公司做广告的效益 D 垃圾邮件成为病毒传播的主要途径 E 垃圾邮件迫使企业使用最新的操作系统 |
| 1572 | 网页防篡改技术包括\_\_\_\_。 |
|  | A 网站采用负载平衡技术 B 防范网站、网页被篡改 C 访问网页时需要输入用户名和口令 D 网页被篡改后能够自动恢复 E 采用HTTPS协议进行网页传输 |
| 1573 | 网络钓鱼常用的手段有\_\_\_\_。 |
|  | A 利用垃圾邮件 B 利用假冒网上银行、网上证券网站 C 利用虚假的电子商务 D 利用计算机病毒 E 利用社会工程学 |
| 1574 | 内容过滤的目的包括\_\_\_\_。 |
|  | A 阻止不良信息对人们的侵害 B 规范用户的上网行为，提高工作效率 C 防止敏感数据的泄漏 D 遏制垃圾邮件的蔓延 E 减少病毒对网络的侵害 |
| 1575 | 下面技术为基于源的内容过滤技术的是\_\_\_\_。 |
|  | A 内容分级审查 B DNS过滤 C IP包过滤 D URL过滤 E 关键字过滤技术 |
| 1576 | 内容过滤技术的应用领域包括\_\_\_\_。 |
|  | A 防病毒 B 网页防篡改 C 防火墙 D 入侵检测 E 反垃圾邮件 |

**专业技术人员考试——信息安全技术（单选）**

**Ａ**

\_\_\_\_是在蜜罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个蜜罐，来构成一个黑客诱捕网络体系架构。**A 蜜网**

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 Backup—d命令当备份设备为磁带时使用此选项**

FTP(文件传输协议，File Transfer Protocol，简称FFP)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 21 25 80 443**

iptables中默认的表名是\_\_\_\_。**A filter**

UNIX／Linux操作系统的文件系统是\_\_\_\_结构。**B 树型**

UNIX／Linux系统中，下列命令可以将普通帐号变为root帐号的是\_\_\_\_。**D ／bin／su命令**

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

Windows系统安装完后，默认隋况下系统将产生两个帐号，分别是管理员帐号和\_\_\_\_。**C 来宾帐号**

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**

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\_\_\_\_。**C 用户打开关闭应用程序**

**Ｂ**

包过滤防火墙工作在OSI网络参考模型的\_\_\_\_。**C 网络层**

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

不能防止计算机感染病毒的措施是\_\_\_\_\_。**A 定时备份重要文件**

不需要经常维护的垃圾邮件过滤技术是\_\_\_\_。**B 简单DNS测试**

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**

**Ｃ**

采用“进程注入”可以\_\_\_\_。**C 以其他程序的名义连接网络**

从系统结构上来看，入侵检测系统可以不包括\_\_\_\_。**C 审计**

**D**

代表了当灾难发生后，数据的恢复程度的指标是\_\_\_\_。**A RPO**

代表了当灾难发生后，数据的恢复时间的指标是\_\_\_\_。**B RTO**

当您收到您认识的人发来的电子邮件并发现其中有意外附件，您应该\_\_\_\_。**C 用防病毒软件扫描以后再打开附件**

对电磁兼容性(Electromagnetic Compatibility，简称EMC)标准的描述正确的是\_\_\_\_。**C 各个国家不相同**

**F**

防火墙是\_\_\_\_在网络环境中的应用。**B 访问控制技术**

防火墙提供的接入模式不包括\_\_\_\_。**D 旁路接入模式**

符合复杂性要求的WindowsXP帐号密码的最短长度为\_\_\_\_。**B 6**

**G**

关于NAT说法错误的是\_\_\_\_。**D 动态NAT又叫做网络地址端口转换NAPT**

关于包过滤防火墙说法错误的是\_\_\_\_。**C 包过滤防火墙可以有效防止利用应用程序漏洞进行的攻击**

关于网闸的工作原理，下面说法错误的是\_\_\_\_. **C 网闸工作在OSI模型的二层以上**

关于应用代理网关防火墙说法正确的是\_\_\_\_。**B 一种服务需要一种代理模块，扩展服务较难**

关于用户角色，下面说法正确的是\_\_\_\_。**B 角色与身份认证无关**

**H**

会让一个用户的“删除”操作去警告其他许多用户的垃圾邮件过滤技术是\_\_\_\_。**D 分布式适应性黑名单**

**J**

基于网络的入侵检测系统的信息源是\_\_\_\_。**D 网络中的数据包**

计算机网络组织结构中有两种基本结构，分别是域和\_\_\_\_。**B 工作组**

**M**

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。**C 七**

某病毒利用RPCDCOM缓冲区溢出漏洞进行传播，病毒运行后，在％System％文件夹下生成自身的拷贝nvchip4.exe，添加注册表项，使得自身能够在系统启动时自动运行。通过以上描述可以判断这种病毒的类型为\_\_\_\_。**C 网络蠕虫病毒**

某公司的工作时间是上午8点半至12点，下午1点555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 凌晨l点**

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 磁带**

**N**

内容过滤技术的含义不包括\_\_\_\_。**D 过滤用户的输入从而阻止用户传播非法内容**

**Q**

企业在选择防病毒产品时不应该考虑的指标为\_\_\_\_。**D 产品能够防止企业机密信息通过邮件被传出**

**R**

容灾的目的和实质是\_\_\_\_。**C 保持信息系统的业务持续性**

容灾项目实施过程的分析阶段，需要进行\_\_\_\_。**D 以上均正确**

**R**

如果您认为您已经落入网络钓鱼的圈套，则应采取\_\_\_\_措施。**D 以上全部都是**

**S**

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 kedawuj**

使用漏洞库匹配的扫描方法，能发现\_\_\_\_。**B 已知的漏洞**

**T**

通过添加规则，允许通往192.168.0.2的SSH连接通过防火墙的iptables指令是\_\_\_\_。**C iptables -A FORWARD -d 192.168.0.2 -p tcp--dport22 -j ACCEPT**

通用入侵检测框架(CIDF)模型中，\_\_\_\_的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。**A 事件产生器**

**W**

网络隔离技术，根据公认的说法，迄今已经发展了\_\_\_\_个阶段。**B 五**

我国《重要信息系统灾难恢复指南》将灾难恢复分成了\_\_\_\_级。**B 六**

物理安全的管理应做到\_\_\_\_。**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**

误用入侵检测技术的核心问题是\_\_\_\_的建立以及后期的维护和更新。**C 网络攻击特征库**

**X**

下列不属于垃圾邮件过滤技术的是\_\_\_\_。**A 软件模拟技术**

下列关于启发式病毒扫描技术的描述中错误的是\_\_\_\_。**C 启发式病毒扫描技术不会产生误报，但可能会产生漏报**

下列关于网络钓鱼的描述不正确的是\_\_\_\_。**B 网络钓鱼都是通过欺骗性的电子邮件来进行诈骗活动**

下列行为允许的有\_\_\_\_。**D 爱选包含商业广告内容的互联网电子邮件时，在互联网电子邮件标题信息前部注明“广告”或者“AD'’字样**

下列技术不能使网页被篡改后能够自动恢复的是\_\_\_\_。**A 限制管理员的权限**

下列技术不支持密码验证的是\_\_\_\_。**D SMTP**

下列内容过滤技术中在我国没有得到广泛应用的是\_\_\_\_。**A 内容分级审查**

下列叙述不属于完全备份机制特点描述的是\_\_\_\_。**D 需要存储空间小**

下面\_\_\_\_不包含在MySQL数据库系统中。**B 密钥管理系统**

下面\_\_\_\_不可能存在于基于网络的漏洞扫描器中。**D 阻断规则设置模块**

下面病毒出现的时间最晚的类型是\_\_\_\_. **B 以网络钓鱼为目的的病毒**

下面不是Oracle数据库提供的审计形式的是\_\_\_\_。**A 备份审计**

下面不是Oracle数据库支持的备份形式的是\_\_\_\_。**B 温备份**

下面不是SQL Server支持的身份认证方式的是\_\_\_\_。**D 生物认证**

下面不是UNIX／Linux操作系统的密码设置原则的是\_\_\_\_。**D 一定要选择字符长度为8的字符串作为密码**

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 umask**

下面不是保护数据库安全涉及到的任务是\_\_\_\_。**C 向数据库系统开发商索要源代码，做代码级检查**

下面不是事务的特性的是\_\_\_\_。**A 完整性**

下面不是数据库的基本安全机制的是\_\_\_\_。**D 电磁屏蔽**

下面不属于容灾内容的是\_\_\_\_。**A 灾难预测**

下面对于数据库视图的描述正确的是\_\_\_\_。**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**

下面关于DMZ区的说法错误的是\_\_\_\_。**C DMZ可以访问内部网络**

下面关于防火墙策略说法正确的是\_\_\_\_。**C 防火墙处理人站通信的缺省策略应该是阻止所有的包和连接，除了被指出的允许通过的通信类型和连接**

下面关于隔离网闸的说法，正确的是\_\_\_\_。**C 任何时刻，网闸两端的网络之间不存在物理连接**

下面关于响应的说法正确的是\_\_\_\_。**D 主动响应的方式可以是自动发送邮件给入侵发起方的系统管理员请求协助以识别问题和处理问题**

下面技术中不能防止网络钓鱼攻击的是\_\_\_\_。**C 根据互联网内容分级联盟(ICRA)提供的内容分级标准对网站内容进行分级**

下面说法错误的是\_\_\_\_。**C 基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描**

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NFSDaemon**

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**

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\_\_\_\_和\_\_\_\_。**D 14 8**

**X**

以下不符合防静电要求的是\_\_\_\_。**B 在机房内直接更衣梳理**

以下不会帮助减少收到的垃圾邮件数量的是\_\_\_\_。**C 安装入侵检测软件**

**X**

以下不可以表示电子邮件可能是欺骗性的是\_\_\_\_。**C 通过姓氏和名字称呼您**

有编辑／etc／passwd文件能力的攻击者可以通过把UID变为\_\_\_\_就可以成为特权用户。**B 0**

有关数据库加密，下面说法不正确的是\_\_\_\_。**C 字符串字段不能加密**

在PDRR模型中，\_\_\_\_是静态防护转化为动态的关键，是动态响应的依据。**B 检测**

在正常情况下，Windows 2000中建议关闭的服务是\_\_\_\_。**A TCP／IP NetBIOS Helper Service**

**专业技术人员考试——信息安全技术（多选）**

Oracle数据库的审计类型有\_\_\_\_。**ACD**

PKI提供的核心服务包括\_\_\_\_。**ABCDE**

PKI系统的基本组件包括\_\_\_\_。**ABCDEF**

SQL Server中的预定义服务器角色有\_\_\_\_。**ABCDE**

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\_\_\_\_。**ABC**

UNIX／Linux系统中的密码控制信息保存在／etc／passwd或／ect／shadow文件中，信息包含的内容有\_\_\_\_。**BCD**

Windows系统登录流程中使用的系统安全模块有\_\_\_\_。**ABC**

Windows系统中的审计日志包括\_\_\_\_。**ABC**

Windows系统中的用户组包括\_\_\_\_。**ABC**

按照2000年3月公布的《计算机病毒防治管理办法》对计算机病毒的定义，下列属于计算机病毒的有\_\_\_\_**ABE**。

病毒传播的途径有\_\_\_\_。**ACDE**

操作系统的基本功能有\_\_\_\_。**ABCD**

场地安全要考虑的因素有\_\_\_\_。**ABCDE**

磁介质的报废处理，应采用\_\_\_\_。**CD**

防火墙的局限性包括\_\_\_\_。**ACD**

防火墙的性能的评价方面包括\_\_\_\_。**ABCD**

防火墙通常阻止的数据包包括\_\_\_\_。**ABDE**

防止设备电磁辐射可以采用的措施有\_\_\_\_。**ABCD**

隔离网闸的三个组成部分是\_\_\_\_。**CDE**

根据SahzerJ.H、SchroederM.D的要求，设计安全操作系统应遵循的原则有\_\_\_\_。**ABCD**

会导致电磁泄露的有\_\_\_\_。**ABCDE**

火灾自动报警、自动灭火系统部署应注意\_\_\_\_。**ABCD**

静电的危害有\_\_\_\_。**ABCD**

可能和计算机病毒有关的现象有\_\_\_\_。**ACD**

可以有效限制SQL注入攻击的措施有\_\_\_\_。**ABCDE**

垃圾邮件带来的危害有\_\_\_\_。**ABD**

蜜罐技术的主要优点有\_\_\_\_。**BCD**

目前市场上主流防火墙提供的功能包括\_\_\_\_。**ABCDE**

内容过滤的目的包括\_\_\_\_。**ABCDE**

内容过滤技术的应用领域包括\_\_\_\_。**ACDE**

容灾等级越高，则\_\_\_\_。**ACD**

入侵防御技术面临的挑战主要包括\_\_\_\_。**BCD**

事务的特性有\_\_\_\_。**ABCE**

数据库访问控制的粒度可能有\_\_\_\_。**ABCD**

数据库故障可能有\_\_\_\_。**ABCDE**

数字证书可以存储的信息包括\_\_\_\_。**ABCD**

随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器(sniffer)来监听整个子网的办法不再可行。可选择解决的办法有**BCDE**。

通用操作系统必需的安全性功能有\_\_\_\_。**ABCD**

通用入侵检测框架(CIDF)模型的组件包括\_\_\_\_。**ACDE**

网络安全扫描能够\_\_\_\_。**ABCDE**

网络钓鱼常用的手段有\_\_\_\_。**ABCDE**

网页防篡改技术包括\_\_\_\_。**ABD**

网闸可能应用在\_\_\_\_。**ABCDE**

为了减小雷电损失，可以采取的措施有\_\_\_\_。**ACD**

系统数据备份包括的对象有\_\_\_\_。**ABD**

下列邮件为垃圾邮件的有\_\_\_\_。**ACDE**

下面标准可用于评估数据库的安全级别的有\_\_\_\_。**ABCDE**

下面不是网络端口扫描技术的是\_\_\_\_。**CDE**

下面对于x-scan扫描器的说法，正确的有\_\_\_\_。**ACE**

下面关于防火墙的维护和策略制定说法正确的是\_\_\_\_。**ABCD**

下面技术为基于源的内容过滤技术的是\_\_\_\_。**BCD**

下面软件产品中，\_\_\_\_是漏洞扫描器。**ABC**

信息系统的容灾方案通常要考虑的要点有\_\_\_\_。**ABCDE**

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\_\_\_\_。**ABD**

主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有\_\_\_\_。**ABC**

主机型漏洞扫描器可能具备的功能有\_\_\_\_。**ABCDE**

组成UNIX系统结构的层次有\_\_\_\_。**ACD**

**专业技术人员考试——信息安全技术（判断）**

“安全通道隔离”是一种逻辑隔离。**Ｘ**

DKIM(Domain Keys Identified 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。

Httpd.conf是Web服务器的主配置文件，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。

iptables可配置具有状态包过滤机制的防火墙。

MS SQL Server与Sybase SQL Server的身份认证机制基本相同。

MySQL不提供字段粒度的访问控制。

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。

QQ是与朋友联机聊天的好工具，不必担心病毒。**Ｘ**

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。

SenderlD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。

SQL Server不提供字段粒度的访问控制。**Ｘ**

SQL Server中，权限可以直接授予用户ID。

SQL注入攻击不会威胁到操作系统的安全。**Ｘ**

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。

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

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。**Ｘ**

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。**Ｘ**

UNIX／Linux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。**Ｘ**

UNIX／Linux系统中的／etc／shadow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／etc／passwd文件中)。**Ｘ**

UNIX／Linux系统中一个用户可以同时属于多个用户组。

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只定义了一个操作系统内核。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。**Ｘ**

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。

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。**Ｘ**

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。

Windows文件系统中，只有Administrator组和ServerOperation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。**Ｘ**

Windows系统的用户帐号有两种基本类型：全局帐号(GlobalAccounts)和本地帐号(LocalAccounts)。

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。**Ｘ**

x-scan能够进行端口扫描。

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。

半连接扫描也需要完成TCP协议的三次握手过程。**Ｘ**

包含收件人个人信息的邮件是可信的。**Ｘ**

贝叶斯过滤技术具有自适应、自学习的能力，目前已经得到了广泛的应用。

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。

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。

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。**Ｘ**

标准的UNIX／Linux系统以属主(Owner)、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。

不需要对数据库应用程序的开发者制定安全策略。**Ｘ**

采用Rootkit 技术的病毒可以运行在内核模式中。

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

常见的操作系统包括DOS、0S／2、UNIX、XENIX、Linux、Windows、Netware、Oracle等。**Ｘ**

大部分恶意网站所携带的病毒就是脚本病毒。

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。

对目前大量的数据备份来说，磁带是应用得最广的介质。

对网页请求参数进行验证，可以防止SQL注入攻击。

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。

对于防火墙的管理可直接通过Telnet进行。**Ｘ**

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。

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

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。

防火墙安全策略一旦设定，就不能在再做任何改变。**Ｘ**

防火墙必须要提供VPN、NAT等功能。**Ｘ**

防火墙对用户只能通过用户名和口令进行认证。**Ｘ**

防火墙规则集的内容决定了防火墙的真正功能。

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。

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。

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。

防火墙中不可能存在漏洞。**Ｘ**

隔离网闸采用的是物理隔离技术。

隔离网闸两端的网络之间不存在物理连接。

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。

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。

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。**Ｘ**

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。

机房供电线路和动力、照明用电可以用同一线路。**Ｘ**

机房内的环境对粉尘含量没有要求。**Ｘ**

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。

基于主机的漏洞扫描不需要有主机的管理员权限。**Ｘ**

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。**Ｘ**

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。**Ｘ**

计算机病毒可能在用户打开“txt”文件时被启动。

计算机场地可以选择在公共区域人流量比较大的地方。**Ｘ**

计算机场地可以选择在化工厂生产车间附近。**Ｘ**

计算机场地在正常情况下温度保持在18～28摄氏度。**Ｘ**

家里的计算机没有联网，所以不会感染病毒。**Ｘ**

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。地线做电气连通。

可以采用内容过滤技术来过滤垃圾邮件。

可以将外部可访问的服务器放置在内部保护网络中。**Ｘ**

可以通过技术手段，一次性弥补所有的安全漏洞。**Ｘ**

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。

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。

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。**Ｘ**

漏洞只可能存在于操作系统中，数据库等其他软件系统不会存在漏洞。**Ｘ**

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

蜜罐技术是一种被动响应措施。**Ｘ**

屏蔽室的拼接、焊接工艺对电磁防护没有影响。**Ｘ**

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。

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。**Ｘ**

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。

启发式技术通过查找通用的非法内容特征，来尝诩蝴IJ新形式和已知形式的非法内容。

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。**Ｘ**

容灾等级通用的国际标准SHARE 78将容灾分成了六级。**Ｘ**

容灾就是数据备份。**Ｘ**

容灾项目的实施过程是周而复始的。

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。**Ｘ**

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。**Ｘ**

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BackupOperators组有此权限，而Lois又是该组成员，则Lois也有此权限。

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。

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。**Ｘ**

软件防火墙就是指个人防火墙。**Ｘ**

实时黑名单是简单黑名单的进—步发展，可以从根本上解决垃圾邮件问题。**Ｘ**

使用登录ID登录SQL Server后，即获得了访问数据库的权限。**Ｘ**

使用漏洞库匹配的方法进行扫描，可以发现所有的漏洞。**Ｘ**

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。

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。

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。

数据库安全只依靠技术即可保障。**Ｘ**

数据库的强身份认证与强制访问控制是同一概念。**Ｘ**

数据库管理员拥有数据库的一切权限。

数据库加密的时候，可以将关系运算的比较字段加密。**Ｘ**

数据库加密适宜采用公开密钥密码系统。

数据库视图可以通过INSERT或UPDATE语句生成。**Ｘ**

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。**Ｘ**

数据越重要，容灾等级越高。

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

所有的漏洞都是可以通过打补丁来弥补的。**Ｘ**

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。

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。**Ｘ**

通过网络扫描，可以判断目标主机的操作系统类型。

完全备份就是对全部数据库数据进行备份。

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。

网络钓鱼的目标往往是细心选择的一些电子邮件地址。

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。**Ｘ**

校验和技术只能检测已知的计算机病毒。**Ｘ**

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。

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.

性能“瓶颈”是当前入侵防御系统面临的一个挑战。

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。**Ｘ**

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。

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。

由于传输的内容不同，电力线可以与网络线同槽铺设。**Ｘ**

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。

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。

与Windows系统不一样的是UNIX／Linux操作系统中不存在预置帐号。**Ｘ**

与入侵检测系统不同，入侵防御系统采用在线(inline)方式运行。

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。**Ｘ**

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。**Ｘ**

运行防病毒软件可以帮助防止遭受网页仿冒欺诈。

灾难恢复和容灾具有不同的含义。**Ｘ**

在安全模式下木马程序不能启动。**Ｘ**

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。**Ｘ**

在来自可信站点的电子邮件中输入个人或财务信息是安全的。**Ｘ**

在默认情况下，内置DomainAdmins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。

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。

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。

在早期用集线器(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子网。**Ｘ**

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。**Ｘ**

针对入侵者采取措施是主动响应中最好的响应措施。**Ｘ**

只要使用了防火墙，企业的网络安全就有了绝对的保障。**Ｘ**

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。**Ｘ**

纸介质资料废弃应用碎纸机粉碎或焚毁。

主动响应和被动响应是相互对立的，不能同时采用。**Ｘ**

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(DynamicPacketFilter)。

**计算机网路**

**网络安全部分**

**一、填空**

**1：**宏病毒是利用( )编写的具有复制传染能力的宏。

**答案：宏命令**

**2：**计算机病毒是有破坏性和不可控制的（ ）。

**答案：计算机程序**

**3：**代理服务的主要缺点是（）。

**答案：降低了服务速度**

**4：**包过滤基于包的（）地址及（）端口

**答案：源，源**

**5：**防火墙工作原理是遵循（）的网络通信安全机制。

**答案：数据过滤**

**6：**实现数字签名的主要方法有（），（）和报文摘要。

**答案：秘密密钥算法，公开密钥算法**

**7：**认证分为（ ）认证和（ ）认证两个方面 。

**答案：信息，用户**

**8：**主要的网络安全的威胁来自（ ）、( )与（ ）三个方面。

**答案：非授权访问，信息泄露，拒绝服务**

**9：**密钥管理的主要办法是引进一个密码分发中心KDC，每个用户与KDC之间有一个共享的（）密钥。

**答案：秘密**

**10：**RSA算法的主要优越性在于（ ）

**答案：安全方便**

**11：**在公开密钥算法提出之前，所以密码系统的（）密钥和（）密钥都有很直接的联系。

**答案：解密，加密**

**12：**操作系统的体系结构的不安全因素主要体现在( )

**答案：创建进程机制**

**13：** SNMP管理模型可分为成三大部分：（ ），（ ）和（ ）。

**答案：被管理系统，网络管理系统，管理协议**

**14：**网络管理任务分为：\_\_\_\_\_\_\_\_\_\_\_\_\_、配置管理、性能管理、故障管理、计费管理、安全管理和其他网络管理功能。

**答案：性能管理**

**15：**网络管理层次结构为：网络平台、网络管理协议、网络管理平台、网络管理工具、网络管理应用软件和（ ）

**答案：网络管理员**

**二、判断**

**1：**在网络管理体系中，除了设备上的代理软件可以主动发出警告外，管理实体也可以向被管理设备进行轮询。( )

**答案：对**

**2：**在使用公共密钥加密技术向对方发送一个数据的时候使用对方用户的公共密钥加密，对方用自己的私人密钥解密数据。( )

**答案：对**

**3：**企业级CA申请证书有2种方法。一种是WEB申请，另一种是在证书管理单元中申请。( )

**答案：对**

**4：**在Windows NT中要审核某个文件夹或打印机的访问，必需启动审核对象的访问。( )

**答案：对**

**5：**根据中国国家计算机安全规范，计算机安全大致可分为三类：实体安全，网络安全和应用安全。( )

**答案：对**

**6：**计费管理的目标是衡量网络的利用率，以便使一个或一组网络用户可以更有规则的地利用网络资源。( )

**答案：对**

**7：**数字证书是电子的凭证，它用来验证在线的个人、组织或计算机的合法身份。( )

**答案：对**

**8：**网络安全主要解决数据保密和认证问题( )

**答案：对**

**9：**网络管理平台和网络管理应用程序是一回事( )

**答案：错**

**10：**防火墙只能对IP地址进行限制和过滤。( )

**答案：错**

**三、选择：**

**1：**你配置UNIX下的Ipchains防火墙，你要添加一条规则到指定的chain后面，你应该使用参数：

A、—A

B、—D

C、—S

D、—INPUT

**答案：A**

**2：**以下关于对称加密算法RC4的说法正确的是：

A、它的密钥长度可以从零到无限大

B、在美国一般密钥长度是128位，向外出口时限制到40位

C、RC4算法弥补了RC5算法的一些漏洞

D、最多可以支持40位的密钥

**答案：B**

**3：**以下不属于win2000中的ipsec过滤行为的是：

A、允许

B、阻塞

C、协商

D、证书

**答案：D**

**4：**你是一个公司的网络管理员，你经常在远程不同的地点管理你的网络（如家里），你公司使用win2000操作系统，你为了方便远程管理，在一台服务器上安装并启用了终端服务。最近，你发现你的服务器有被控制的迹象，经过你的检查，你发现你的服务器上多了一个不熟悉的帐户，你将其删除，但第二天却总是有同样的事发生，你应该如何解决这个问题？

A、停用终端服务

B、添加防火墙规则，除了你自己家里的IP地址，拒绝所有3389的端口连入

C、打安全补丁sp4

D、启用帐户审核事件，然后查其来源，予以追究

**答案：C**

**5：**在Linux下umask的八进制模式位6代表：

A、拒绝访问

B、写入

C、 读取和写入

D、读取、写入和执行

**答案：C**

**6：**Window2000域或默认的身份验证协议是：

A、 HTML

B、 Kerberos V5

C、TCP/IP

D、 Apptalk

**答案：B**

**7：**SSL安全套接字协议所使用的端口是：

A、80

B、443

C、1433

D、3389

**答案：B**

**8：**你有一个共享文件夹，你将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有什么样的权限？

A、读取

B、写入

C、修改

D、完全控制

**答案：A**

**9：**以下关于window NT 4.0的服务包的说法正确的是？

A、sp5包含了sp6的所有内容

B、sp6包含了sp5的所有内容

C、sp6不包含sp5的某些内容

D、sp6不包含sp4的某些内容

**答案：C**

**10：**作为一个管理员，把系统资源分为三个级别是有必要的，以下关于级别1的说法正确的是？

A、 对于那些运行至关重要的系统，如，电子商务公司的用户帐号数据库

B、 对于那些必须的但对于日常工作不是至关重要的系统

C、 本地电脑即级别1

D、以上说法均不正确

**答案：A**

**11：**你所使用的系统为UNIX，你通过umask命令求出当前用户的umask值为0023，请问该用户在新建一文件夹，具体有什么样的权限？

A、当前用户读、写和执行，当前组读取和执行，其它用户和组只读

B、当前用户读、写，当前组读取，其它用户和组不能访问

C、当前用户读、写，当前组读取和执行，其它用户和组只读

D、当前用户读、写和执行，当前组读取和写入，其它用户和组只读

**答案：A**

**12：**你所使用的系统为win2000，所有的分区均是NTFS的分区，C区的权限为everyone读取和运行，D区的权限为everyone完全控制，现在你将一名为test的文件夹，由C区移动到D区之后，test文件夹的权限为？

A、everyone读取和运行

B、everyone完全控制

C、everyone读取、运行、写入

D、以上都不对

**答案：B**

**13：**你的window2000开启了远程登陆telnet，但你发现你的window98和unix计算机没有办法远程登陆，只有win2000的系统才能远程登陆，你应该怎么办？

A、重设防火墙规则

B、检查入侵检测系统

C、运用杀毒软件，查杀病毒

D、 将NTLM的值改为0

**答案：D**

**14：**你是一企业网络管理员，你使用的防火墙在UNIX下的IPTABLES，你现在需要通过对防火墙的配置不允许192.168.0.2这台主机登陆到你的服务器，你应该怎么设置防火墙规则？

A、iptables—A input—p tcp—s 192.168.0.2—source—port 23—j DENY

B、iptables—A input—p tcp—s 192.168.0.2—destination—port 23—j DENY

C、iptables—A input—p tcp—d 192.168.0.2—source—port 23—j DENY

D、iptables—A input—p tcp—d 192.168.0.2—destination—port 23—j DENY

**答案：B**

**15：**以下哪个不是属于window2000的漏洞？

A、unicode

B、IIS hacker

C、输入法漏洞

D、单用户登陆

**答案：D**

**16：**下列哪项不属于window2000的安全组件？

A、访问控制

B、强制登陆

C、审计

D、自动安全更新

**答案：D**

**17：**以下关于VPN的说法中的哪一项是正确的？

A、 VPN是虚拟专用网的简称，它只能只好ISP维护和实施

B、 VPN是只能在第二层数据链路层上实现加密

C、IPSEC是也是VPN的一种

D、VPN使用通道技术加密，但没有身份验证功能

**答案：C**

**18：**你想发现到达目标网络需要经过哪些路由器，你应该使用什么命令？

A、ping B、nslookup

C、tracert D、ipconfig

**答案：C**

**19：**小李在使用super scan对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是什么？

A、文件服务器 B、邮件服务器

C、WEB服务器 D、DNS服务器

**答案：B**

**20：**假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包。这时你使用哪一种类型的进攻手段？

A、缓冲区溢出 B、地址欺骗

C、拒绝服务 D、暴力攻击

**答案：A**

**21：**RC4是由RIVEST在1987年开发的，是一种流式的密文，就是实时的把信息加密成一个整体，它在美国一般密钥长度是128位，因为受到美国出口法的限制，向外出口时限制到多少位？

A、64位 B、56位

C、40位 D、32位

**答案：C**

**22：**当你感觉到你的Win2000运行速度明显减慢，当你打开任务管理器后发现CPU的使用率达到了百分之百，你最有可能认为你受到了哪一种攻击。

A、特洛伊木马

B、拒绝服务  
C、欺骗

D、中间人攻击

**答案：B**

**23：**SNMP协议操作命令类型有 ( )

* + - * 1. 读，写，移动，陷阱

B．读，写，修改，陷阱

C．读，写，删除，陷阱

D．读，写，增加，陷阱

**答案：A**

**24：**Windows NT（　）

A.只提供对SNMPv1的支持 B.只提供对SNMPv2的支持

C.同时提供对SNMPv1和SNMPv2的支持 D.两者皆不提供支持

**答案：A**

**25：**下列关于SNMPv1的说法中错误的是（　　　）

A.适合各种规划的数据检索

B.管理信息库的资源有限，不足以完成复杂的管理功能

C.只提供简单的认证机制

D.这完善的陷入机制有可能导制管理信息的丢失

**答案：C**

**26：**Internet的核心传输协议是（　　　）

A.IPX/SPX B.TCP/IP

C.NETBEUI D.SNMP

**答案：A**

**27：**下列网络管理工具中由IBM公司研制开发的是（　）

A. NetView B. SNA

C. SunNet Manager D. OpenView

**答案：A**

**28：**下列叙述 ( ) 是正确的。

A.SNMP 不支持管理站改变管理信息库结构

B.SNMP 管理站不能增加删除管理信息库中的管理对象实例

C.SNMP 管理站不能一次性访问一个子树

D. 以上都正确

**答案：C**

**29：**计算机系统中的信息资源只能被授予权限的用户修改，这是网络安全的 ( ) 。

A. 保密性 B. 数据完整性 C. 可利用性 D. 可靠性

**答案：B**

**30：**互联网中所有端系统和路由器都必须实现 ( ) 协议。

A.SNMP B.SMTP C.TCP D.IP

**答案：C**

**31：**实体认证是通过识别通信对方的身份，防止假冒，可使用的方法是（　）

A.消息认证 B.数字签名

C.消息摘要 D.单向Hash变换

**答案：A**

**32：**假设有一个LAN，每15min轮询所有被管理设备一次，管理报文的处理时间是50ms，网络延迟为1ms，单个轮询需要的时间为0.202s，则管理站最多可支持的设备数是（　）

A.300 B.4500

C.18000 D.150000

**答案：A**

**33：**网络管理软件包括管理专用软件，管理支持软件和（　）

A.用户专用软件 B.用户支持软件

C.用户管理软件 D.用户接口软件

**答案：B**

**34：**ISO定义的系统管理功能域中，测试管理功能属于（　）

A.配置管理 B.故障管理

C.性能管理 D.安全管理

**答案：D**

**35：**下述各功能中，属于性能管理范畴的功能是（ ）

A．网络规划和资源管理功能

B．工作负载监视功能

C．运行日志控制功能

D．测试管理功能

**答案：B**

**36：**防止数据源被假冒，最有效的加密机制是（ ）

A．消息认证 B．消息摘要 C．数字签名 D．替换加密

**答案：C**

**37：**篡改是破坏了数据的（ ）

A．完整性 B．一致性 C．保密性 D．可利用性

**答案：A**

**38：**对一个网络管理员来说，网络管理的目标不是（ ）

A．提高设备的利用率

B．为用户提供更丰富的服务

C．降低整个网络的运行费用

D．提高安全性

**答案：B**

**39：**SNMP协议的直接下层协议是（ ）

A．UDP B．ICMP C．TCP D．IP

**答案：A**

**40：**在Internet网络管理的体系结构中，SNMP协议定义在（ ）

A．链路层 B．网络层 C．传输层 D．应用层

**答案：D**

**四、简答**

**1：**网络管理的五大功能是什么？

**答案：**

**① 性能管理（Performance Management）；**

**② 配置管理（Configuration Management）；**

**③ 记账（计费）管理（Accounting Management）；**

**④ 故障管理（Fault Management）；**

**⑤ 安全管理（Security Management）。**

**2：**网络病毒可以通过哪些网络服务入侵你的计算机？

**答案：**

**在局域网环境下病毒入侵网络的主要途径是通过工作站传播到服务器硬盘，再由服务器的共享目录传播到其它工作站。 用户直接从文件服务器复制已感染的文件到本地并执行它时，病毒就会感染本机器上的其它文件。**

**在因特网环境下，网络病毒也可以通过因特网毫无困难地发送，几乎所有的网络服务都可能有病毒入侵的可能，例如HTTP，FTP，MAIL等服务。**

**3：**简述防火墙的工作原理。

**答案：**

**防火墙（Firewall）是在两个网络之间执行访问控制策略的硬件或软件系统，目的是保护网络不被他人侵扰。本质上，它遵循的是一种数据进行过滤的网络通信安全机制，只允许授权的通信，而禁止非授权的通信。通常，防火墙就是位于内部网或Web站点与因特网之间的一台路由器或计算机。**

**通常，部署防火墙的理由包括：防止入侵者干扰内部网络的正常运行；防止入侵者删除或修改存储再内部网络中的信息；防止入侵者偷窃内部的秘密信息。**

**部署防火墙应该满足以下规则：有进出网络的通信流都应该通过防火墙；所有穿过防火墙的通信流都必须有安全策略和计划的确认和授权。**

**理论上说，防火墙是不会被攻破的。防火墙不是万能的，它不能防范恶意的知情者和不通过它的连接，不能防止内部人员的攻击，也不能防范病毒。**

**五、综合**

**1：**已知明文为RETRIEVE，所对应的64位明文代码为67 5A 69 67 5E 5A 6B 5A（十六进制数，下同）。密钥是FEBRUARY，所对应的64位密钥代码为5B 5A 57 67 6A 56 67 6E。利用DES算法，计算出密文。

**答案：**

**试验证最后得到的密文代码是97 4A FF BF 86 02 2D 1F**

**2：**已知RSA公开密钥密码体制的公开密钥e = 7，n = 55，明文M =10。试求其密文C。

**答案：**

**C=Me(mod n)=107(mod 55)=10**

1. **网络设备**

**一、选择**

**1：**在星型局域网结构中，连接文件服务器与工作站的设备是( )。

A．网卡 B．集线器 C．收发器 D．网关

**答案：B**

**2：**设有下面4条路由：170.18.129.0/24、170.18.130.0/24、170.18.132.0/24和170.18.133.0/24，如果进行路由汇聚，能覆盖这4条路由的地址是( )。

A.170.18.128.0/21 B.170.18.128.0/22 C.170.18.130.0/22 D.170.18.132.0/23

**答案：**

**3：**IP地址中的网络号部分用来识别（ ）。

A．路由器 B.主机 C.网卡 D.网段

**答案：D**

**4：**IP路由器设计的重点是提高接收，处理和转发分组速度，其传统IP路由转发功能主要由( )

A) 软件实现 B) 硬件实现 C)专用ASIC实现 D)操作系统实现

**答案：A**

**5：**在计算机网络中，一方面连接局域网中的计算机，另一方面连接局域网中的传输介质的部件是（  ）。

A．双绞线 B．网卡 C．终结器 D．路由器

**答案：B**

**6：**如果要组建一个快速以太网，那么需要使用以下哪些基本的硬件设备与材料？（ ）

Ⅰ. 100 BASE-T交换机Ⅱ. 100 BASE-T网卡Ⅲ. 双绞线或光缆Ⅳ. 路由器

A)Ⅰ、Ⅱ和Ⅳ B)Ⅰ、Ⅲ和Ⅳ C)Ⅰ、Ⅱ和Ⅲ D)Ⅱ、Ⅲ和Ⅳ

**答案：C**

**7：**针对不同的传输介质，网卡提供了相应的接口。适用于非屏蔽双绞线的网卡应提供（ ）

A)AUI接口 B)光纤F/O接口 C)RJ-45接口 D)BNC接口

**答案：C**

**8：**在交换式局域网中，如果交换机采用直接交换方式，那么帧出错检测任务由( )

结点主机完成 B)交换机完成C)交换机与结点主机共同完成 D)高层协议完成

**答案：A**

**9：**以下哪个地址是Ethernet的物理地址？

A)10.254.1.220 B)00-60-08-00-A6-38C)10-65-08 D)10.0.0.1

**答案：B**

**10：**通过局域网连接到Internet时，计算机上必须有( )。

A)MODEM　　 B)网络适配器　　C)电话　　　　　　 D)USB接口

**答案：B**

**11：**路由器转发分组是根据报文分组的( )

A) 端口号  B) MAC地址 C) IP地址   D) 域名

**答案：C**

**12：**符合802.1标准的网桥是由各网桥自己决定路由选择，局域网上的各站点不负责路由选择，这类网桥被称为( )

A) 第2层交换    B) 网关 C) 源路由网桥 D) 透明网桥

**答案：D**

**13：**实现网络层互连的设备是( )

A) repeater   B) bridge C) router D) gateway

**答案：C**

**14：**按传输介质类型，以太网卡主要分为粗缆网卡、细缆网卡、双绞线网卡与( )

A) RJ-11网卡     B) 光纤网卡 C) CATV网卡  D) ADSL网卡

**答案：B**

**15：**点—点式网络与广播式网络在技术上有重要区别。点—点式网络需要采用分组存储转发与（ ）

A) 路由选择 B) 交换 C) 层次结构 D) 地址分配

**答案：A**

**16：**局域网与广域网、广域网与广域网的互联是通过（ ）网络设备实现的。

A) 服务器   B) 网桥    C) 路由器    D) 交换机

**答案：C**

**17：**主机A运行Unix操作系统，IP地址为202.113.224.35，子网屏蔽码为255.255.255.240；主机B运行Linux操作系统，IP地址为202.113.224.38，子网屏蔽码为255.255.255.240。它们分别连接在同一台局域交换机上，但处于不同的VLAN中。主机A通过ping命令去ping主机B时，发现接收不到正确的响应。请问可能的原因是（ ）：

A) 主机A和主机B的IP地址不同

B) 主机A和主机B处于不同的VLAN中

C) 主机A和主机B使用了不同操作系统

D) 主机A和主机B处于不同的子网中

**答案：B**

**18：**一个校园网与城域网互联，它应该选用的互联设备为( )

A)交换机 B)网桥 C)路由器 D)网关

**答案：C**

**19：**网桥互联的两个局域网可以采用不同的( )

Ⅰ.物理层协议 Ⅱ.数据链路层协议

Ⅲ.网络层协议 Ⅳ.传输层协议

A) Ⅰ和Ⅱ B) Ⅰ、Ⅱ和Ⅲ C) Ⅱ和Ⅲ D) Ⅱ、Ⅲ和Ⅳ

**答案：A**

**20：**局域网交换机首先完整地接收数据帧，并进行差错检测。如果正确，则根据帧目的地址确定输出端口号再转发出去。这种交换方式为( )

A)直接交换 B)改进直接交换 C)存储转发交换 D)查询交换

**答案：C**

**21：**虚拟网络中逻辑工作组的结点组成不受物理位置的限制，逻辑工作组的划分与管理是通过（ ）方式实现的。

A) 硬件方式 B) 存储转发方式 C) 改变接口连接方式 D) 软件方式

**答案：D**

**22：**VLAN在现代组网技术中占有重要地位，同一个VLAN中的两台主机（ ）

A)必须连接在同一交换机上 B)可以跨越多台交换机

C)必须连接在同一集线器上 D)可以跨业多台路由器

**答案：B**

**23：**有一种互连设备工作于网络层，它既可以用于相同（或相似）网络间的互连，也可以用于异构网络间的互连，这种设备是（ ）

A)集线器     B)交换机     C)路由器     D)网关

**答案：C**

**24：**某路由器的路由表如下所示。如果它收到一个目的地址为192.168.10.23的IP数据报，那么它为该数据报选择的下一路由器地址为（ ）

|  |  |
| --- | --- |
| 要达到的网络 | 下一路由器 |
| 192. 168. 1. 0 | 直接投递 |
| 192. 168. 2. 0 | 直接投递 |
| 192. 168. 3. 0 | 192. 168. 1. 35 |
| 0. 0. 0. 0 | 192. 168. 2. 66 |

A) 192.168.10.1  B) 192.168.2.66 C) 192.168.1.35 D) 直接投递

**答案：B**

**25：**某路由器收到了一个IP数据报，在对其首部进行校验后发现该数据报存在错误，路由器最有可能采取的动作是( )

A) 纠正该IP数据报的错误       B) 将该IP数据报返给源主机

C) 抛弃该IP数据报             D) 通知目的主机数据报出错

**答案：C**

**26：**虚拟局域网通常采用交换机端口号、MAC地址、网络层地址或( )

A) 物理网段定义       B) 操作系统定义 C) IP广播组地址定义        D) 网桥定义

**答案：C**

**27：**交换式局域网从根本上改变了“共享介质”的工作方式，它可以通过局域网交换机支持端口之间的多个并发连接。因此，交换式局域网可以增加网络带宽，改善局域网性能与( )

A) 服务质量     B) 网络监控     C) 存储管理     D) 网络拓扑

**答案：A**

**28：**10BASE-T使用标准的RJ-45接插件与3类或5类非屏蔽双绞线连接网卡与集线器。网卡与集线器之间的双绞线长度最大为( )

A) 15米     B) 50米     C) 100米     D) 500米

**答案：C**

**29：**在路由器互联的多个局域网中，通常要求每个局域网的( )

 A.数据链路层协议和物理层协议必须相同

 B.数据链路层协议必须相同，而物理层协议可以不同

 C.数据链路层协议可以不同，而物理层协议必须相同

 D.数据链路层协议和物理层协议都可以不相同

**答案：D**

**30：**传统的交换机作为第二层设备，只能识别并转发（ 1 ）地址，要支持VLAN间的通信只能借助于具有（ 2 ）功能的网络设备。具有这种功能的设备有路由器和三层交换机。当用路由器解决VLAN通信时，路由器得到一个VLAN包后，根据目的IP地址，获得目的MAC地址及相应的（ 3 ），根据（ 4 ）将帧送往目的交换机端口。当用三层交换机解决VLAN通信时，由于交换机具有（ 5 ），交换和路由速度可以达到线速。

（1） A IP B 网络 C 协议 D MAC

（2） A 三层交换 B 通信交换 C 信元交换 D 线路交换

（3）A VLAN ID B 端口 C 虚电路 D 信元

（4）A MAC B IP C VLAN ID D 端口

（5）A 转发 B路由 C 线路交换 D 直通

**答案：DAACB**

**31：**中继器处于（ １ ）；有关智能集线器的说法正确的是（ ２ ）。

（1） A、 物理层      B、数据链路层         C、网络层         D、高层

（2） A、 价格更贵    B、有发现黑客的功能   C、 有内置的智能  D、都不对

**答案：AC**

**32：**连接局域网的两个不同网段应该选用（ 1 ），当有不同网络层地址的两个局域网相连时用（ 2 ）。

（1） A、中继器     B、网桥      C、路由器       D、网关

（2） A、中继器     B、网桥      C、路由器       D、网关

**答案：BC**

**33：**网管员在分析出某网络中部分机器的通信量过大后，决定将他们划分到一个独立的网段上，在路由器上为其分配一个端口进行连接。那么除了为这些机器重新配置IP地址及为路由器配置端口的IP地址之外，还应（ 1 ）。当一个网段上的利用率和冲突都大幅度上升时，解决的办法是（ 2 ）。

（1） A、在路由器中增加每一台所连工作站的MAC地址。

B、在路由表中增加一项此网段的路由表项

C、删除以前这些机器在路由器中的登记信息

D、删除路由表中的所有项

（2） A、延长网络线缆      B、改变传输介质

C、添置中继器        D、为计算机分段，中间通过网桥或路由器连接

**答案：BD**

**34：**路由器是一种常用的网络互连设备，它工作在OSI/RM的（ 1 ）上，在网络中它能够根据网络通信的情况（ 2 ），并识别（ 3 ）。相互分离的网络经路由器互联后（ 4 ）。

（1） A、物理层 B、数据链路层 C、网络层 D、传输层

（2） A、动态选择路由 B、控制数据流量 C、调节数据传输率 D、改变路由结构

（3） A、MAC地址 B、网络地址

C、MAC地址和网络地址 D、MAC地址和网络地址的共同逻辑地址

（4） A、形成了一个更大的物理网络 B、仍然还是原来的网络

C、形成了一个逻辑上单一的网络 D、成为若干个互联的子网

**答案：CABD**

**35：**以太网交换机根据（ ）转发数据包。

A.IP地址 B.MAC地址 C.LLC地址 D.PORT地址

**答案：B**

**二、填空：**

1.交换机转发帧的方式有（ ）、（ ）和（ ）。

**答案：存储转发方式、直通方式、无碎片直通方式**

2.Ethernet交换机实现动态建立和维护端口/MAC地址映射表的方法是( )。

**答案：地址学习**

3.1000BASE-T标准规定网卡与HUB之间的非屏蔽双绞线长度最大为( )m。

**答案：100**

4.IEEE 802.3标准的以太网的物理地址长度为( )bit。

**答案：48**

**5.**所谓最佳路径是指经过的（ ）最少或者（ ）最短。

**答案：节点、传输路径**

**6.**如果一个IP地址为202.93.120.34的主机需要向202.94.120.0网络进行直接广播，那么，它使用的直接广播地址为（ ）。

**答案：202.94.120.255**

**7.**网桥可以在互联的多个局域网之间实现源地址（ ）、地址( )与数据（ ）功能。

**答案：学习、过滤、转发**

**8.**在因特网路由器中，有些路由表项是由网络管理员手工建立的，这些路由表项被称为（ ）路由表项；有一些路由表项是由路由器相互发送路由信息自动形成的，这些路由表项被称为（ ）路由表项。

**答案：静态、动态**

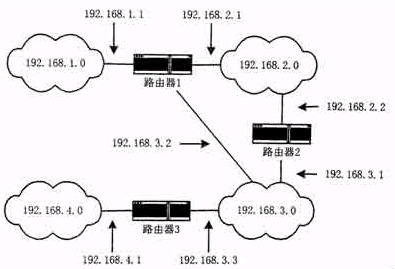
**9.**路由器可以包含一个特殊的路由。如果没有发现到达某一特定网络或特定主机的路由，那么它在转发数据包时使用的路由称为（ ）路由。

**答案：默认**

**10.**有一个虚拟局域网的建立是动态的，它代表了一组IP地址，并由叫做代理的设备对虚拟局域网中的成员进行管理。在这个虚拟局域网中，代理和多个IP结点组成IP( )虚拟局域网。

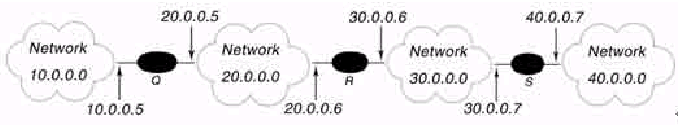
**答案：广播**

**11.**在下面所示的简单互联网中，路由器2的路由表对应目的网络192.168.4.0的下一跳步IP地址应为( )



**答案：192.168.3.3**

**12.**下图为一个简单的互联网示意图。其中，路由器Q的路由表中到达网络40.0.0.1的下一跳步IP地址应为（ ）。



**答案：20.0.0.6**

**13.**典型的以太网交换机允许一部分端口支持10BASE-T，另一部分端口支持100BASE-T。在采用了（ ）技术时，交换机端口可以同时支持10Mbps/100Mbps。

**答案：自动检测;自适应**

**14.**路由器是构成因特网的关键设备。按照OSI参考模型，它工作于( )层。

**答案：网络层**

**三、判断**

**1.**一个广播域一定是一个冲突域( )

**答案：F**

**2.**交换机是根据待传输的数据帧的源地址来建立端口之间的连接关系的。( )

**答案：F**

**3.**交换机是根据“端口号/MAC地址映射表”建立端口之间的连接关系的。( )

**答案：T**

**4.**IP路由器不仅能够分析出IP数据报中的TCP内容，还可以为该数据报选择最佳路径。

**答案：F**

**5.**VLAN中的一个站点可以和另一个VLAN中的站点直接通信。( )

**答案：F**

**6.**当站点在一个VLAN中广播时，其他VLAN中的站点不能收到。( )

**答案：T**

**7.**当站点从一个VLAN转移到另一个VLAN时，一般不需要物理连接。( )

**答案：T**

**8.**在路由器中，为选择路由而利用的路由表是既可以是人工计算出来输入到路由器的，也可是路由器自动计算出来的。( )

**答案：T**

**9.**网络适配器是逻辑上将计算机与网络连接起来的器件( )

**答案：F**

**10.**可以用交换机端口号、MAC地址、网络层地址定义虚拟局域网( )

**答案：T**

**四、综合**

**1.**简述路由器与网桥的区别。

**答案：**

**网桥工作在OSI参考模型的第2层，路由器工作在第3层；路由器的传输性能不如网桥，但适应范围超过网桥；路由器能抑制广播包，但网桥不能；路由器可以拥有不同的子网，而网桥连接的网络具有相同的子网地址；路由器的安装和配置比网桥复杂。**

2.简述计算生成树的步骤。

**答案：**

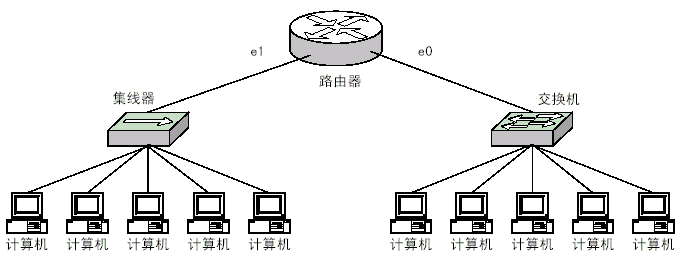
**推选"根网桥"；决定非根网桥的"根端口"；决定"指定网桥"和各网络的"指定端口"。**

**3.**简述透明网桥的工作原理。

**答案：**

**学习源地址，过滤本网段帧，转发异网段帧，广播未知帧。**

**4.**观察以下的网络配置图后，回答问题1至问题2。



**【问题1】**

说明集线器、交换机和路由器工作在OSI的哪个层次上，使用什么样的地址类型。

**【问题2】**

从传输延迟时间的量级来看，路由器和局域网交换机一般为多少微秒？

**【问题3】**

***共有几个广播域，几个冲突域。***

**答案：**

**（1）路由器工作在网络层及以下，网络地址；集线器工作在物理层，无；交换机--数据链路层及以下，MAC地址。**

**（2）路由器一般为几千微妙，交换机为几十微秒。**

**（3）2个广播域，7个冲突域。**

**5.**阅读以下说明，回答问题1至问题4。

**【说明】**

设在某单位路由器上建立了如下的路由表。

|  |  |  |
| --- | --- | --- |
| **目的IP** | **子网掩码** | **转发端口** |
| 128.96.36.0 | 255.255.255.128 | E1 |
| 128.96.36.128 | 255.255.255.128 | E2 |
| 128.96.37.0 | 255.255.255.128 | R2 |
| 128.96.37.128 | 255.255.255.128 | R3 |
| Default | － | R4 |

**【问题1】**

若路由器收到分组的目的IP地址为128.96.37.151，则转发的端口是哪一个，若收到分组的目的IP是128.96.35.151，则转发的端口是哪一个。

**【问题2】**

若该路由器是该单位的与Internet接入路由器，则该单位分得的IP地址是什么。

**【问题3】**

在一个网络中子网数目划分增多时，可供分配给主机的正常IP地址总数目会如何变化。

**【问题4】**

当我们将主机地址设置为192.168.1.2时，则主机访问Internet时需要经过什么样的变化。

**答案：**

**（1）R3、R4**

**（2）128.96.36.0/24**

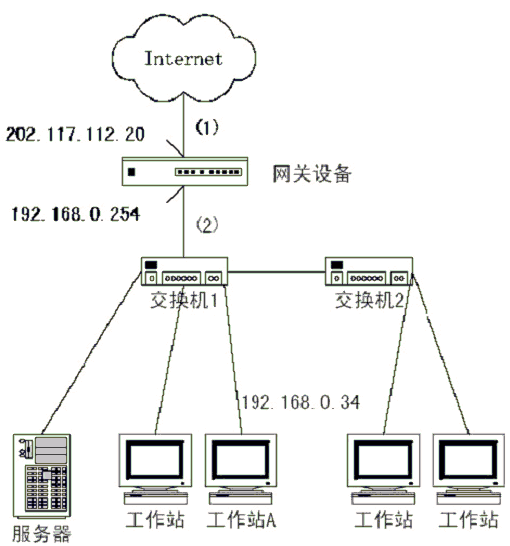
**（3）减少**

**（4）需要经过网关进行地址转换**

**6.**阅读以下说明，回答问题1至问题5。

【说明】

某公司内部的网络的工作站采用100Base-TX 标准与交换机相连，并经网关设备采用NAT技术共享同一公网IP地址接入互联网，如下图所示。



**【问题1】**

连接交换机与工作站的传输介质是什么？介质需要做成直通线还是交叉线？最大长度限制为多少？

**【问题2】**

交换机1与交换机2之间相距20米，采用交换机堆叠方式还是交换机级联方式？

**【问题3】**

在工作站A的网络配置中，网关地址是什么？

**【问题4】**

从以下备选答案中选择两种能够充当网关的网络设备。备选答案：A 路由器 B集线器 C代理服务器 D网桥

**【问题5】**

若工作站A访问外部Web 服务器，发往Internet 的IP包经由（1）和（2）处时源IP 地址分别是什么？

**答案：**

**（1）双绞线，直通，100m**

**（2）级联方式**

**（3）192.168.0.254**

**（4）AC**

**（5）192.168.0.34、202.117.112.20**

1. **网络操作系统**

**一、选择**

**1.：**以下那项功能不属于网络操作系统的基本服务？

A. 文件服务 B. 打印服务

C. 邮件服务 D. 目录服务

**答案：C**

**2：**以下那个操作系统基本不支持“即插即用”?

A. Windows ME B. Windows NT 4.0

C. Redhat Linux 7.0 D. Windows XP

**答案：B**

**3：**在UNIX系统中，用于更新文件操作权限的命令是：\_\_\_\_\_\_\_\_\_\_?

A. chown B. chmod C. chwho D. chpms

**答案：B**

**4：**在UNIX系统中，下列的那种文件权限是不存在的？

A. 读（read） B. 写（write） C. 附加（append） D. 执行（execute）

**答案：C**

**5：**在Windows NT网络操作系统中，不同域之间可以建立\_\_\_\_\_\_\_\_\_\_\_关系。

A. 抚养 B. 信任 C. 合作 D. 授权

**答案：B**

**6：**下列那一项不是对等网的优点？

A. 有功能强大的服务器提供服务 B. 实施简单

C. 易于使用、维护 D. 价格便宜

**答案：A**

**7：**下列那一项不是对等网的优点？

A. 有功能强大的服务器提供服务 B. 实施简单

C. 易于使用、维护 D. 价格便宜

**答案：A**

**8：**下列那个不是客户机/服务器模式？

A. 一个无盘工作站访问文件服务器

B. 一个工作站通过打印服务器打印文件

C. 一个工作站访问服务器上的一个数据库

D. 一个终端访问主机上的数据库

**答案：D**

**9：**对等网适合于：

A. 多于100台计算机的大网络 B. 10台左右计算机的局域网

C. 大量服务器少量客户机的网络 D. 以上都不适合

**答案：B**

**10：**在对等网上，PC机能够同时作为：

A. 文件服务器 B. 打印服务器 C. 工作站 D. 以上都可

**答案：D**

**二、填空**

**1：**为了使得相关用户可以列出目录中的文件名，需要给目录赋予\_\_\_\_\_\_\_\_\_的权限。

**答案：读（read）**

**2.**操作系统的安全性包括：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：登录安全性，资源访问权限控制，服务器安全性**

**3.**大型门户网站，需要构建\_\_\_\_\_\_\_\_\_\_\_\_\_\_来应付大容量的访问。

**答案：服务器集群（cluster）**

**4.**为了在UNIX系统可以为每个用户开辟一个个人网页发布的空间，其默认的目录名是在用户登录主目录下的\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 在UNIX指令中可以用\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_表示。

**答案：public\_html, ~/public\_html**

**5.**在UNIX中，系统将访问资源的用户划分成三类，分别是：\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_。

**答案：资源属主（u），同组者（g），其他（o）**

**6.**在Windows 2000的活动目录中，对用户进行管理的主要逻辑单位包括：\_\_\_\_\_\_\_,\_\_\_\_\_\_,\_\_\_\_\_,\_\_\_\_\_。

**答案：域，组织单元，树，森林**

**7.**在UNIX中对文件进行更名的指令为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：mv**

**8.**普通的双机备份技术的切换时间为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：10秒-30秒**

**9.**可以实现MS Windows和UNIX类操作系统互联和资源共享的软件为\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：Samba**

**10.**在对等式网络中，所有的计算机安装的都是同一系统，即是\_\_\_\_\_\_\_\_\_\_\_，又是\_\_\_\_\_\_\_\_，提供\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_两种功能。

**答案：服务器，客户机，客户机/服务器**

**11.**在客户机/ 服务器网络中，网络操作系统实际上由两部分组成，一部分是\_\_\_\_\_\_\_\_\_\_，另一部分是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，其中\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是网络操作系统中主要组成部分，而\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_要简单得多，主要提供用户访问网络的接口。

**答案：服务器软件，客户机软件，服务器软件，客户端**

**12.**在集中式网络中，网络操作系统\_\_\_\_\_\_\_\_\_\_\_\_\_\_，终端\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：仅用于主机，不需要安装系统**

**13.**可以看成简单网络连接的对等网操作系统产品包括：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_和\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：Novell的NetWare Lite，Microsoft的Windows for Workgroup，Windows 9**

**14.**网络操作系统有三种类型，它们是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：集中式、服务器/客户端模式和对等式**

**15.**网络操作系统有三种类型，它们是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

**答案：简单网络连接，分布式计算**

**三、简答**

**1.**请归纳出MS Windows操作系统与UNIX类操作系统的差别。

**答案：**

**1. 操作界面的不同，Windows着重于图形用户界面（ＧＵＩ），ＵＮＩＸ着重于字符用户界面（ＣＵＩ）；**

**2. 对操作命令和文件名的大小写敏感性，Windows无所谓，ＵＮＩＸ敏感；**

**3. 对文件系统的定义方法：Windows按逻辑盘符划分文件系统，ＵＮＩＸ只有一棵倒置的目录树；**

**4. 应用场合：Windows适用于办公环境，作为桌面系统，ＵＮＩＸ适用于服务器主机，作为后台系统；**

**5. 开发厂商：Windows为单一厂商开发，技术封闭，ＵＮＩＸ存在多方开发，并存在行业标准，可以在开放的环境中开发和应用；**

**2.**网络操作系统的容错能力表现在那些方面？

**答案：**

**一方面通过系统硬件备份来提高系统的容错能力，措施如：磁盘镜像、磁盘双工和双机备份；另一方面，在设计理念上，提供系统的容错能力，例如，Windows NT所设计域控制服务器的备份，使得用户注册服务器的服务，不会因为该服务器的失效而导致网络失败。**

**3.**“即插即用”设备使用的必要条件有哪些？

**答案：**

**支持PnP的硬件设备、操作系统、BIOS和该设备的驱动程序。**

**4.**请简述网络操作系统中“目录服务”的概念，并举例说明。

**答案：**

**这是一种以单一逻辑的方式访问可能位于全球范围内的所有网络服务和资源的技术。无论用户在何处，也无论资源位于什么地方，用户只需通过一次登录就可访问网络服务和资源。如Novell 的NetWare提供的NDS(Novell Directory Service)、微软公司Windows 2000中的活动目录(Active Directory)和Sun的NIS+等。**

**5.**网络操作系统有哪些类型？各自应用在什么场合？

**答案：**

**网络操作系统有三种类型：集中式、客户/服务器模式和对等式。其中集中式网络操作多用于大中型主机和金融、运输和社会服务行业；客户/服务器模式大量应用在中小型企事业单位；对等式用于工作组内几台计算机之间仅需提供简单的通信和资源共享。**

更多自考资料尽在百度贴吧自考乐园俱乐部 （http://tieba.baidu.com/club/5346389）欢迎加入...欢迎交流...止不住的惊喜等着你......... 俱乐部名称：自考乐园;俱乐部 id：5346389（请牢记它哦~在百度贴吧的搜索框中输入俱乐部 id，可以直接 进入俱乐部）；俱乐部 url 地址：http://tieba.baidu.com/club/5346389（您也可以通过此 url 进入俱乐部。） 1 全国 2010 年 4 月自学考试计算机网络安全试题 计算机网络安全试题 计算机网络安全试题 计算机网络安全试题及答案 杨尚杰为你亲情制作.....自考乐园俱乐部首发....（转载请保留此段文字，O(∩\_∩)O 谢谢合 作............） 课程代码：04751 一、单项选择题（本大题共 15 小题，每小题 2 分，共 30 分） 在每小题列出的四个备选项中只有一个是符合题目要求的，请将其代码填写在题后的 括号内。错选、多选或未选均无分。 1．下列对计算机网络的攻击方式中，属于被动攻击的是( A ) A．口令嗅探 B．重放 C．拒绝服务 D．物理破坏 2．OSI 安全体系结构中定义了五大类安全服务，其中，数据机密性服务主要针对的安全威 胁是( B ) A．拒绝服务 B．窃听攻击 C．服务否认 D．硬件故障 3．为了提高电子设备的防电磁泄漏和抗干扰能力，可采取的主要措施是( B ) A．对机房进行防潮处理 B．对机房或电子设备进行电磁屏蔽处理 C．对机房进行防静电处理 D．对机房进行防尘处理 4．为保证计算机网络系统的正常运行，对机房内的三度有明确的要求。其三度是指 ( A ) A．温度、湿度和洁净度 B．照明度、湿度和洁净度 C．照明度、温度和湿度 D．温度、照明度和洁净度 5．下列加密算法中，属于双钥加密算法的是( D ) A．DES B．IDEA C．Blowfish D．RSA 6．公钥基础设施(PKI)的核心组成部分是( A ) A．认证机构 CA B．X.509 标准 C．密钥备份和恢复 D．PKI 应用接口系统 更多自考资料尽在百度贴吧自考乐园俱乐部 （http://tieba.baidu.com/club/5346389）欢迎加入...欢迎交流...止不住的惊喜等着你......... 俱乐部名称：自考乐园;俱乐部 id：5346389（请牢记它哦~在百度贴吧的搜索框中输入俱乐部 id，可以直接 进入俱乐部）；俱乐部 url 地址：http://tieba.baidu.com/club/5346389（您也可以通过此 url 进入俱乐部。） 2 7．下面关于防火墙的说法中，正确的是( C ) A．防火墙可以解决来自内部网络的攻击 B．防火墙可以防止受病毒感染的文件的传输 C．防火墙会削弱计算机网络系统的性能 D．防火墙可以防止错误配置引起的安全威胁 8．包过滤技术防火墙在过滤数据包时，一般不. 关心( D ) A．数据包的源地址 B．数据包的目的地址 C．数据包的协议类型 D．数据包的内容 9．不. 属于 CIDF 体系结构的组件是( C ) A．事件产生器 B．事件分析器 C．自我防护单元 D．事件数据库 10．阈值检验在入侵检测技术中属于( B ) A．状态转换法 B．量化分析法 C．免疫学方法 D．神经网络法 11．由于系统软件和应用软件的配置有误而产生的安全漏洞，属于( C ) A．意外情况处置错误 B．设计错误 C．配置错误 D．环境错误 12．采用模拟攻击漏洞探测技术的好处是( D ) A．可以探测到所有漏洞 B．完全没有破坏性 C．对目标系统没有负面影响 D．探测结果准确率高 13．下列计算机病毒检测手段中，主要用于检测已知病毒的是( A ) A．特征代码法 B．校验和法 C．行为监测法 D．软件模拟法 14．在计算机病毒检测手段中，校验和法的优点是( D ) A．不会误报 B．能识别病毒名称 C．能检测出隐蔽性病毒 D．能发现未知病毒 15．一份好的计算机网络安全解决方案，不仅要考虑到技术，还要考虑的是( C ) A．软件和硬件 B．机房和电源 C．策略和管理 D．加密和认证 更多自考资料尽在百度贴吧自考乐园俱乐部 （http://tieba.baidu.com/club/5346389）欢迎加入...欢迎交流...止不住的惊喜等着你......... 俱乐部名称：自考乐园;俱乐部 id：5346389（请牢记它哦~在百度贴吧的搜索框中输入俱乐部 id，可以直接 进入俱乐部）；俱乐部 url 地址：http://tieba.baidu.com/club/5346389（您也可以通过此 url 进入俱乐部。） 3 二、填空题（本大题共 10 小题，每小题 2 分，共 20 分） 请在每小题的空格中填上正确答案。错填、不填均无分。 16．P2DR (PPDR)模型是一种常用的计算机网络安全模型，包含 4 个主要组成部分，分别是： \_\_安全策略\_\_\_\_\_\_\_\_、防护、检测和响应。 17．对计算机网络安全构成威胁的因素可以概括为：偶发因素、自然因素和\_\_人为因素 \_\_\_\_\_\_\_\_三个方面。 18．物理安全技术主要是指对计算机及网络系统的环境、场地、\_\_\_设备\_\_\_\_\_\_\_和人员等 采取的安全技术措施。 19．密码体制从原理上可分为两大类，即单钥密码体制和\_\_双密钥密码体制\_\_\_\_\_\_\_\_。 20．在加密系统中，作为输入的原始信息称为明文，加密变换后的结果称为\_\_\_密文\_\_\_\_\_\_\_。 21．防火墙的体系结构一般可分为：双重宿主主机体系机构、屏蔽主机体系结构和屏蔽\_\_\_ 子网体系结构\_\_\_\_\_\_\_。 22．就检测理论而言，入侵检测技术可以分为异常检测和\_误用检测\_\_\_\_\_\_\_\_\_。 23．从系统构成上看，入侵检测系统应包括数据提取、\_\_\_\_入侵分析\_\_\_\_\_\_、响应处理和 远程管理四大部分。 24．按照计算机网络安全漏洞的可利用方式来划分，漏洞探测技术可以划分为信息型漏洞 探测和\_\_攻击型漏洞探测\_\_ 25．防范计算机病毒主要从管理和\_\_\_技术\_\_\_\_\_两方面着手。 三、简答题（本大题共 6 小题，每小题 5 分，共 30 分） 26．简述计算机网络安全的定义。 计算机网络安全是指利用管理控制和技术措施，保证在一个网络环境里，信息数据的机密 性、完整性及可使用性受到保护。 27．简述物理安全在计算机网络安全中的地位，并说明其包含的主要内容。 物理安全是整个计算机网络系统安全的前提. 物理安全主要包括：①机房环境安全②通信线路安全③设备安全④电源安全 28．防火墙的五个主要功能是什么？ 防火墙的主要功能：①过滤进、出网络的数据②管理进、出网络的访问行为③封堵某些禁 止的业务④记录通过防火墙的信息和内容⑤对网络攻击检测和告警 29．基于数据源所处的位置，入侵检测系统可以分为哪 5 类？ 更多自考资料尽在百度贴吧自考乐园俱乐部 （http://tieba.baidu.com/club/5346389）欢迎加入...欢迎交流...止不住的惊喜等着你......... 俱乐部名称：自考乐园;俱乐部 id：5346389（请牢记它哦~在百度贴吧的搜索框中输入俱乐部 id，可以直接 进入俱乐部）；俱乐部 url 地址：http://tieba.baidu.com/club/5346389（您也可以通过此 url 进入俱乐部。） 4 基于数据源的分类：按数据源所处的位置，把入侵检测系统分为五类：即基于主机、基于 网络、混合入侵检测、基于网关的入侵检测系统及文件完整性检查系统； 30．什么是计算机网络安全漏洞？ 计算机网络安全漏洞是在硬件、软件和协议的具体实现或系统安全策略上存在的缺陷，从 而可以使攻击者能够在未授权的情况下访问或破坏系统。 31．简述恶意代码的主要防范措施。 恶意代码的防范措施（P228）：①及时更新系统，修补安全漏洞②设置安全策略，限制脚本 程序的运行③开启防火墙，关闭不必要的服务和系统信息；④养成良好的上网习惯。 四、综合分析题（本大题共 2 小题，每小题 10 分，共 20 分） 32．某局域网如下图，其中：1 号设备是路由器，4 号设备是交换机，5 和 6 号设备是 DMZ 区服务器，7、8 和 9 号设备是个人计算机。 请回答下列问题： (1)2 和 3 号设备中，哪个设备是防火墙?哪个设备是交换机? 3 号设备是防火墙；2 设备是交换机 (2)3 套个人防火墙软件最适合安装在哪 3 个设备上?(只能选 3 个设备) 7、8、9 号设备 (3)5 套防病毒软件应该安装在哪 5 个设备上?(只能选 5 个设备) 5 套防病毒软件应该安装在 5、6、7、7、8、9 号设备 更多自考资料尽在百度贴吧自考乐园俱乐部 （http://tieba.baidu.com/club/5346389）欢迎加入...欢迎交流...止不住的惊喜等着你......... 俱乐部名称：自考乐园;俱乐部 id：5346389（请牢记它哦~在百度贴吧的搜索框中输入俱乐部 id，可以直接 进入俱乐部）；俱乐部 url 地址：http://tieba.baidu.com/club/5346389（您也可以通过此 url 进入俱乐部。） 5 33．对给定二进制明文信息“0011010101000101001111010010101110010101”进行两次加密。 第一次，采用 8 位分组异或算法，用密钥“01010101”对明文进行加密运算。第二次， 采用“1→4(读作：位置 l 的数据移到位置 4，以下类推)，2→8，3→1，4→5，5→7， 6→2，7→6，8→3”对第一次加密后的密文进行 8 位分组换位加密运算。请写出两次 加密的密文。 注：异或运算的规则如下表所示。 x y x COR y 0 0 0 0 1 1 1 0 1 1 1 0 更多自考资料尽在百度贴吧自考乐园俱乐部 （http://tieba.baidu.com/club/5346389）欢迎加入...欢迎交流...止不住的惊喜等着你......... 俱乐部名称：自考乐园;俱乐部 id：5346389（请牢记它哦~在百度贴吧的搜索框中输入俱乐部 id，可以直接 进入俱乐部）；俱乐部 url 地址：http://tieba.baidu.com/club/5346389（您也可以通过此 url 进入俱乐部。） 6 第一次，采用 8 位分组异或算法，用密钥“01010101”对明文进行加密运算的密文： 01100000 00010000 01101000 01111110 11000000 第二次，对第一次加密后的密文进行 8 位分组换位加密运算的密文 10000001 00001000 10000011 11001111 00010001 以上资料由百度贴吧： ------------------ ------------------ ------------------ ------------------自考乐园俱乐部杨尚杰为你精心编辑

**网络安全**

**选择题**

1. 网络安全是在分布网络环境中对（ ）

A. 信息载体提供安全保护 B. 信息的处理、传输提供安全保护

C. 信息的存储、访问提供安全保护 D. 上面3项都是

1. 对攻击可能性的分析在很大程度上带有（ ）

A. 客观性 B. 主观性 C. 盲目性 D. 以上3项

1. 机密性服务提供信息的保密，机密性服务包括（ ）

A. 文件机密性 B. 信息传输机密性 C. 通信流的机密性 D. 以上3项

1. 网络协议的关键成分是（ ）

A. 硬件、软件与数据 B. 语法、语义、体系结构

C. 语法、定时、层次结构 D. 语法、语义、定时

1. 可以被数据完整性机制防止的攻击方式是（ ）

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏

1. VPN的加密手段是（ ）

A. 具有加密功能的防火墙

B. 带有加密功能的路由器

C. VPN内的各台主机对各自的信息进行相应的加密

D. 单独的加密设备

1. 通常所说的移动VPN是指（ ）

A. Access VPN B. Intranel VPN C. Extranet VPN D. 以上都不是

8．入侵检测系统的检测分析技术主要有两大类，它们是（ ）

A. 特征检测和模型检测 B. 异常检测和误用检测

C. 异常检测和概率检测 D. 主机检测和网络检测

9．身份鉴别是安全服务中的重要一环，以下关于身份鉴别的叙述不正确的是（ ）

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向认证

C. 目前一跟般采用基于对称密钥或公开密钥加密的方法

D. 数据签名机制是实现身份鉴别的重要机制

10．对动态网络地址转换（NAT），不正确的说法是（ ）

A. 将很多内部地址映射到单个真实地址

B. 外部网络地址和内部地址一对一的映射

C. 最多可有64000个同时的动态NAT连接

D. 每个连接使用一个端口

答案：1.D 2.B 3.D 4.D 5.D 6.C 7.A 8.B 9.B 10.B

1．网络安全的基础属性是（ ）

A. 机密性 B. 可用性 C. 完整性 D. 以上3项都是

2．橘皮书定义了4个安全层次，从D层（最低保护层）到A层（验证性保护层），其中D级的安全保护是最低的，属于D级的系统是不安全的，以下操作系统中属于D级安全的是（ ）

A. 运行非UNIX的Macin tosh机 B. 运行Linnx的PC机

C. UNIX系统 D. XENIX

3．网络安全最终是一个折衷的方案，即安全强度和安全操作代价的折衷除增加安全设施投资外，还应考虑（ ）

A. 用户的方便性 B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持 D. 上面3项都是

4．下列对访问控制影响不大的是（ ）

A. 主体身份 B. 客体身份 C. 访问类型 D. 主体与客体的类型

5．在开放系统互连环境中，两个N层实体进行通信，它们可能用到的服务是（）

A. N-1层是提供的服务 B. N层是提供的服务

C. N+1层是提供的服务 D. 以上3项都不是

6．路由控制机制用以防范（ ）

A. 路由器被攻击者破坏 B. 非法用户利用欺骗性的路由协议

C. 在网络层次进行分析；防止非法信息通过路由 D. 以上3项都不是

7．IpSee协议中负责对IP数据报加密的部分是（ ）

A. 封装安全负载（ESP） B. 鉴别包头（AH）

C. Internet密钥交换（IKE） D. 以上都不是

8．GRE协议（ ）

A. 既封装、又加密 B. 只封装、不加密

C. 不封装、只加密 D. 不封装、不加密

9．数据保密性安全服务的基础是（ ）

A. 数据完整性机制 B. 数字签名机制 C. 访问控制机制 D. 加密机制

10．包过滤的局限性不包括（ ）

A. 不能进行内容控制 B. 过滤规则制定比较复杂

C. 访问控制机制 D. 不支持实现NAT

答案：1.D 2.A 3.D 4.D 5.A 6.B 7.A 8.B 9.D 10.D

1．密码学的目的是（ ）

A. 研究数据加密 B. 研究数据解密 C. 研究数据保密 D. 研究信息安全

2．从安全属性对各种网络攻击进行分类。阻断攻击是针对（ ）

A. 机密性的攻击 B. 可用性的攻击 C. 完整性的攻击 D. 真实性的攻击

3．Kerberos的设计目标不包括（ ）

A. 认证 B. 授权 C. 记账 D. 加密

4．ISO7408-2从体系结构的观点描述了5种可选的安全服务，以下不属于这5种安全服务的是（ ）

A. 身份鉴别 B. 数据包过滤 C. 授权控制 D. 数据完整性

5．CA属于ISO安全体系结构中定义的（ ）

A. 认证交换机制 B. 通信业务填充机制 C. 路由控制机制 D. 公证机制

6．分组过滤型防火墙原理上是基于（ ）

A. 物理层分析的技术 B. 数据链路层分析的技术

C. 网络层分析的技术 D. 应用层分析的技术

7．属于第二层的VPN隧道协议有（ ）

A. IPSec B. PPIP C. GRE D. 以上皆不是

8．GRE协议的乘客协议是（ ）

A. IP B. IPX C. AppleTalk D. 上述皆可

9．误用检测的优点不包括（ ）

A. 检测准确度高 B. 能够检测出新的网络攻击

C. 便于系统维护 D. 技术相对成熟

10．对非军事区DMZ而言，正确的解释是( )

A. DMZ是一个非真正可信的网络部分

B. DMZ网络访问控制策略决定允许或禁止进入DMZ通信

C. 允许外部用户访问DMZ系统上合适的服务

D. 以上3项都是

答案： 1．C 2. B 3. B 4. B 5. D 6. C 7. B 8. D 9. B 10. D

1．一般而言，Internet防火墙建立在一个网络在（ ）

A. 内部子网之间传送信息的中枢 B. 每个子网的内部

C. 内部网络与外部网络的交叉点 D. 部分内部网络与外部内部的接合处

2．从安全属性对各种网络攻击进行分类，截获攻击是针对（ ）

A. 机密性的攻击 B. 可用性的攻击 C. 完整性的攻击 D. 真实性的攻击

3．数字签名要预先使用单向Hash函数进行处理的原因是（ ）

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名的验证签名的运算速度

D. 保证密文能正确的还原成明文

4．一个报文的端到端传递内OSZ模型的（ ）

A. 网络层负责处理 B. 传输层负责处理

C. 会话层负责处理 D. 表示层负责处理

5．ISU7498-2描述了8种特定的安全机制，这8种特定的安全机制是为5种特定的安全服务设置的，以下不属于这8种安全机制的是（ ）

A. 安全标记机制 B. 加密机制 C. 数字签名机制 D. 访问控制机制

6．用于实现身份鉴别的安全机制是（ ）

A. 加密机制的数字签名机制 B. 加密机制的访问控制机制

C. 数字签名机制和路由控制机制 D. 访问控制机制的路由控制机制

7．SSL产生会话密钥的方式是（ ）

A. 从密钥管理数据库中请求获得 B. 每一台客户机分配一个密钥的方式

C. 随机由客户机产生并加密后通知服务器 D. 由服务器产生并分配给客户机

8．PPTP客户端使用（ ）

A. TCP协议建立连接 B. UDP协议建立连接

C. L2TP协议建立连接 D. 以上皆不是

9．拒绝服务攻击的后果是（ ）

A. 信息不可用 B. 应用程序不可用 C. 阻止通信 D. 上面几项都是

10．现在防火墙呢中，最常用的技术是（ ）

A. 代理服务器技术 B. 状态检测包过滤技术

C. 应用网关技术 D. NAT技术

答案：1.C 2.A 3.C 4.B 5.A 6.A 7.C 8.A 9.D 10.B

1．计算机病毒程序隐藏在计算机系统的（ ）

A. 内存中 B. 软盘中 C. 存储介质中 D. 网络中

2．可信计算机系统评估准则（Trusted Computer System Evaluation Criteria TCSEC）共分为4大类（ ）

A. 7级 B.8级 C.5级 D.6级

3．对目标的攻击威胁通常通过代理实现，而代理需要的特性包括（ ）

A. 访问目标的能力 B. 对目标发出威胁的动机

C. 有关目标的知识 D. 上面3项都是

4．从安全属性对各种网络攻击进行分类，截获攻击是针对（ ）

A. 机密性的攻击 B. 攻击性的攻击 C. 完整性的攻击 D. 真实性的攻击

5．身份鉴别是安全服务中心的重要一环，以下关于身份鉴别的叙述不正确的是（ ）

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

6．Web中使用的安全协议有（ ）

A. PEM SSL B. S-HTTP S/MIME

C. SSL S-HTTP D. S/MIME SSL

7．ISO定义的安全体系结构中包含（ ）

A. 4种安全服务 B. 5种安全服务 C. 6种安全服务 D. 7种安全服务

8．传输层保护的网络采用的主要技术是建议在（ ）

A. 可靠的传输服务基础上的安全套接字层SSL协议

B. 不可靠的传输服务基础上的S-HTTP协议

C. 可靠的传输服务基础上的S-HTTP协议

D. 不可靠的传输服务基础上的安全套接字层SSL协议

9．防火墙在网络层中根据数据包中包头信息有选择地实施允许和阻断。这种技术是（ ）

A. 应用网管技术 B. 状态检测技术 C. 包过滤技术 D. 代理服务器技术

10．误用检测的优点不包括（ ）

A. 检测准确度高 B. 能够检测出新的网络攻击

C. 便于系统维护 D. 技术相对成熟的网络攻击

答案：1.C 2.A 3.D 4.A 5.B 6.C 7.B 8.A 9.C 10.B

1. 访问控制需要确定（ ）

A. 用户权限 B. 可给予那些主体访问控制权利

C. 可被用户访问的资源 D. 系统是否遭入侵

1. 威胁是一个可能破坏信息系统环境安全的动作或事件，威胁包括（ ）

A. 目标 B. 代理 C. 事件 D. 上面三项都是

3．完整性服务提供信息的正确性，为了对抗篡改攻击该服务必须和（ ）

A. 机密性服务配合工作 B. 可用性服务配合工作

C. 可审性配合工作 D. 以上三项都是

4．基于通信双方公共拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该机密作为加密和密钥认证是（ ）

A. 公钥认证 B. 零知识认证 C. 共享密钥认证 D. 口令认证

5．ISO安全体系结构中的对象认证安全服务使用（ ）

A. 加密机制完成 B. 数字签名机制完成

C. 访问控制机制完成 D. 数据完整性机制完成

6．在ISO/OSI定义的安全体系结构中没有规定（ ）

A. 对象认证服务 B. 访问控制安全服务

C. 数据保密性安全服务 D. 数据可用性安全服务

7．SSL产生绘画密钥的方式是（ ）

A. 从密钥管理数据库中获得

B. 每一台客户机分配一个密钥的方式

C. 随机由客户机产生并加密后通知服务器

D. 由服务器产生并分配给客户机

8．属于第二层的VPN隧道协议有（ ）

A. IPsec B. PPTP Ｃ. GRE　　 Ｄ. 以上皆不是

9．入侵检测系统的检测分析技术主要有两大类它们是（　）

Ａ. 特征检测和模型推理　 Ｂ. 异常检测和误用检测

Ｃ. 异常检测和概率检测 Ｄ. 主机检测和网络检测

10．为了降低风险不建议使用的Ｉｎｔｅｒｎｅｔ服务是（　）

Ａ. Web服务　 B. 外部访问内部系统　　 C. 内部访问internet D. FTP服务

答案：1.B 2.D 3.C 4.C 5.B 6.D 7.C 8.B 9.B 10.D

1. 风险是丢失需要保护的资产的可能性，风险是（ ）

A. 攻击目标和威胁事件 B. 威胁和漏洞 C. 资产和漏洞 D. 上面3项都不是

2．假设使用一和加密算法，它的加密方法很简单，将每一个字母加5，即a加密成f，b加密成g,这种算法的密钥就是5，那么它属于（ ）

A. 对称密码技术 B. 分组密码技术 C. 公钥密码技术 D. 单向函数技术

3．从安全属性对各种网络攻击来进行分类，截获攻击是针对（ ）

A. 对称密码技术 B. 可用性技术 C. 完整性技术 D. 真实性技术

4．下面不属于PKICA公钥基础设施的组成部分是（ ）

A. 证书主体 B. 使用证书的应用和系统 C. 证书权威机构 D. AS

5．数据完整性安全机制可与（ ）

A. 加密机制使用相同方法实现 B. 公证机制使用相同方法实现

C. 数字签名机制使用相同方法实现 D. 访问控制机制使用相同方法实现

6．第二层保护的网络一般可达到点对点间（ ）

A. 较强的身份认证 B. 保密性 C. 连续的通道认证 D. 以上3项都是

7．分组过滤型防火墙原理上是基于（ ）

A. 物理层进行分析的技术 B. 数据链路层进行分析的技术

C. 网络层进行分析的技术 D. 应用层进行分析的技术

8．PPTP客户端使用（ ）

A. TCP协议建立连接 B. UPP协议建立连接

C. LITP协议建立连接 D. 以上皆不对

9．防火墙在网络层中根据数据包中包头信息有选择地实施允许和阻断，这种技术是（ ）

A. 应用网管技术 B. 状态检测技术 C. 包过滤技术 D. 代理服务器技术

10．异常检测的优点不包括（ ）

A. 较少依赖特定的主机操作系统 B. 能够检测出新的网络攻击

C. 对越权访问行为的检测能力较强 D. 技术相当成熟

答案：1.B 2.A 3.A 4.D 5.C 6.D 7.C 8.A 9.C 10.D

1．为了避免访问控制表过于庞大，通常对访问者（ ）

A. 分类组织成组

B. 严格限制数量

C. 按访问时间排序，并删除一些长期没有访问的用户

D. 不作任何限制

2．一个进程是网络安全是在分步网络环境中对（ ）

A. 信息载体提供安全保护 B. 信息的处理传输提供安全保护

C. 信息的存储访问提供保护 D. 上面三项都是

3．ISO定义的安全体系结构中包括（ ）

A. 4 种安全服务 B. 5种安全服务 C. 6种安全服务 D. 7种安全服务

4．CA属于ISO安全体系结构中定义的（ ）

A. 认证交换机制 B. 通信业务填充机制 C. 路由控制机制 D. 公证机制

5．IPSec协议中负责对IP数据加密部分是（ ）

A. 封装安全负载（ESP） B. 鉴别包头（AH）

C. Internet密钥交换（IKE） D. 以上都不是

6．第三层保护的网络与第二层保护的网络相比在通信成本上占有一定优势，它只需要进行（ ）

A. 认证机制保护 B. 完整性保护 C. 访问控制保护 D. 以上都不是

7．传输保护的网络采用的主要技术是建立在（ ）

A. 可靠的传播服务基础上的安全套接字层SSL协议

B. 不可靠的传输服务基础上的S-HTTP协议

C. 不可靠的传输服务基础上的S-HTTP协议

D. 不可靠的传输服务基础上的安全套接字层SSL协议

8．GRE协议（ ）

A. 既封装又加密 B.只封装不加密 C.不封装只加密 D.不封装不加密

9．对动态网络地址转换（NAT）不正确的说法是（ ）

A. 将很多内部地址映射到单个真实地址

B. 外部网络地址和内部地址一对一映射

C. 最多可有64000个同时的动态NAT 连接

D. 每个连接使用一个端口

10．现在防火墙中，最常用的技术是（ ）

A. 代理服务器技术 B. 状态检测包过滤技术 C. 应用网关技术 D. NAT技术

答案：1.A 2.D 3.B 4.D 5.A 6.C 7.A 8.B 9.B 10.B

选择题：

1.计算机网络是地理上分散的多台（ ）遵循约定的通信协议，通过软硬件互联的系统。

A.计算机 B.主从计算机 C.自主计算机 D.数字设备

2.网络安全是分布网络环境中对（ ）提供安全保护。

A.信息载体 B.信息的处理、传输 C.信息的存储、访问 D.上面3项都是

3.网络安全的基本属性是（ ）。

A.机密性 B.可用性 C.完整性 D. 上面3项都是

4.密码学的目的是（ ）。

A.研究数据加密 B.研究数据解密 C.研究数据保密 D.研究信息安全

5.假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f，b加密成g。这种算法的密钥就是5，那么它属于（ ）。

A.对称密码技术 B.分组密码技术 C.公钥密码技术 D.单向函数密码技术

1 - 5 CDDCA

6.访问控制是指确定（ ）以及实施访问权限的过程。

A.用户权限 B.可给予那些主体访问权利 C.可被用户访问的资源 D.系统是否遭受入侵

7.一般而言，Internet防火墙建立在一个网络的（ ）。

A.内部子网之间传送信息的中枢 B.每个子网的内部

C.内部网络与外部网络的交叉点 D.部分内部网络与外部网络的接合处

8.可信计算机系统评估准则（Trusted Computer System Evaluation Criteria，TCSEC）共分为（ ）大类（ ）级。

A.4 7 B.3 7 C.4 5 D.4 6

9.橘皮书定义了4个安全层次，从D层（最低保护层）到A层（验证性保护层），其中D级的安全保护是最低的，属于D级的系统是不安全的，以下操作系统中属于D级安全的是（ ）。

A.运行非UNIX的Macintosh机 B.运行Linux的PC

C.UNIX系统 D.XENIX

10.计算机病毒是计算机系统中一类隐藏在（ ）上蓄意破坏的捣乱程序。

A.内存 B.软盘 C.存储介质 D.网络

6-10 BCAAC

11.对攻击可能性的分析在很大程度上带有（ ）。

A.客观性 B.主观性 C.盲目性 D.上面3项都不是

12.网络安全最终是一个折中的方案，即安全强度和安全操作代价的折中，除增加安全设施投资外，还应考虑（ ）。

A.用户的方便性 B.管理的复杂性 C.对现有系统的影响及对不同平台的支持 D.上面3项

13.从安全属性对各种网络攻击进行分类，阻断攻击是针对（ ）的攻击。

A.机密性 B.可用性 C.完整性 D.真实性

14.从安全属性对各种网络攻击进行分类，截获攻击是针对（ ）的攻击。

A.机密性 B.可用性 C.完整性 D.真实性

15.从攻击方式区分攻击类型，可分为被动攻击和主动攻击，被动攻击难以（ ），然而（ ）这些攻击是可行的，主动攻击难以（ ），然而（ ）然而（ ）这些攻击是可行的。

A.阻止，检测，阻止，检测 B. 检测，阻止，检测，阻止

C.检测，阻止，阻止，检测 D.上面3项都不是

11-15 BDBAC

16.窃听是一种（ ）攻击，攻击者（ ）将自己的系统插入到发送站和接收站之间。截获是一种（ ）攻击，攻击者（ ）将自己的系统插入到发送站和接受站之间。

A.被动，无须，主动，必须 B.主动，必须，被动，无须

C.主动，无须，被动，必须 D.被动，必须，主动，无须

17.威胁是一个可能破坏信息系统环境安全的动作或事件，威胁包括（ ）。

A.目标 B.代理 C.事件 D.以上三项都是

18.对目标的攻击威胁通常通过代理实现，而代理需要的特性包括（ ）。

A.访问目标能力 B.对目标发出威胁的动机 C.有关目标的知识D.上面三项都是

19．拒绝服务攻击的后果是（ ）。

A.信息不可用 B.应用程序不可用 C.系统宕机 D.阻止通信 E.上面几项都是

20.风险是丢失需要保护的（ ）的可能性，风险是（ ）和（ ）的综合结果。

A.资产，攻击目标，威胁事件 B.设备，威胁，漏洞

C.资产，威胁，漏洞 D.上面三项都不对

16-20 ADDEC

21.机密性服务提供信息的保密，机密性服务包括（ ）。

A.文件的机密性 B.信息传输机密性 C.通信流的机密性 D.以上三项都是

22.完整性服务提供信息的正确性。该服务必须和（ ）服务配合工作，才能对抗篡改攻击。

A.机密性 B.可用性 C.可审性 D.以上三项都是

23.数字签名要预先使用单向Hash函数进行处理的原因是（ ）。

A.多一道加密工序使密文更难破译 B. 保证密文能正确地还原成明文

C.缩小签名密文的长度，加快数字签名和验证签名的运算速度 D.提高密文的计算速度

24. Kerberos的设计目标不包括（ ）。

A.认证 B.授权 C.记账 D.加密

25.身份鉴别是安全服务中的重要一环，以下关于身份鉴别的叙述不正确的是（ ）。

A.身份鉴别是授权控制的基础

B.身份鉴别一般不用提供双向的认证

C.目前一般采用基于对称密钥加密或公开密钥加密的方法

D.数字签名机制是实现身份鉴别的重要机制

21-25 DCCBB

26.基于通信双方共同拥有的但不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（ ）。

A.公钥认证 B.零知识认证 C.共享密钥认证 D.口令认证

27. Kerberos在请求访问应用服务器之前，必须（ ）。

A.向Ticket Granting服务器请求应用服务器ticket

B.向认证服务器发送要求获得“证书”的请求

C.请求获得会话密钥

D.直接与应用服务器协商会话密钥

28.下面不属于PKI（公钥基础设施）的组成部分的是（ ）。

A.证书主体 B.使用证书的应用和系统 C.证书权威机构 D.AS

29.下列对访问控制影响不大的是（ ）。

A.主体身份 B.客体身份 C.访问类型 D.主体与客体的类型

30.为了简化管理，通常对访问者（ ），避免访问控制表过于庞大。

A.分类组织成组 B.严格限制数量

C.按访问事件排序，并删除一些长期没有访问的用户 D.不做任何限制

26-30 CADDA

31.下面是几种对TCB的描述，正确的是（ ）

A.来自橘皮书，和固件有关 B.来自橘皮书，由操作系统事实的安全机制

C.来自橘皮书，是系统的保护机制 D.咋安全环境中系统面熟安全机制的级别

32.下面（ ）的存储提供最高安全。

A.内存映射 B.硬件分段 C.虚拟机 D.保护环

33.基准监控器能确保（ ）。

A.只有授权主体可以访问客体 B.信息流从低安全级别到高安全级别

C.CPU不直接访问内存 D.主体不对较低级别的客体操作

34.保护域的正确定义是（ ）

A.可供主体使用的系统资源 B.在安全便边界外的系统资源

C.在TCB内工作的系统资源 D.工作在保护环1到3的系统资源

35.一种抽象机能保证所有的主体有适当的允许权来访问客体，这种确保客体不被不可信的主体损害的安全控制概念是（ ）。

A.安全核 B.TCB C.基准监控器 D.安全域

31-35 CBAAC

36．CPU和OS有多层自保护，他们用保护环机制通过安全控制边界把关键组件分开，下列（ ）组件应放在最外环。

A.应用和程序 B.I/O驱动器和公用程序 C.操作系统OS核 D.OS的其余部分

37.TCB内有几种的类型部件，下列（ ）不在安全边界内。

A.母板上的固件 B.应用程序 C.保护的硬件组件 D.基准监控器和安全核

38.处理器和系统运行在（ ）状态能处理和硬件的直接通信。

A.问题状态 B.等待状态 C.运行状态 D.特权状态

39.ISO7498-2从体系结构的观点描述了5种可选的安全服务，以下不属于这5种安全服务的是（ ）。

A.身份鉴别 B.数据报过滤 C.授权控制 D.数据完整性

40．ISO7498-2描述了8种特定的安全机制，这8种特定的安全机制是为5类特定的安全服务设置的，以下不属于这8种安全机制的是（ ）。

A.安全标记机制 B.加密机制 C.数字签名机制 D.访问控制机制

36-40 ABDBA

41.用于实现身份鉴别的安全机制是（ ）。

A.加密机制和数字签名机制 B.加密机制和访问控制机制

C.数字签名机制和路由控制机制 D.访问控制机制和路由控制机制

42.ISO7498-2从体系结构的观点描述了5种普遍性的安全机制，这5种安全机制不包括（ ）。

A.可信功能 B.安全标号 C.事件检测 D.数据完整性机制

43.在ISO/OSI定义的安全体系结构中，没有规定（ ）。

A.对象认证服务 B.访问控制安全服务 C.数据保密性安全服务

D.数据完整性安全服务 E.数据可用性安全服务

44.（ ）不属于ISO/OSI安全体系结构的安全机制。

A.访业务流量分析机制 B.访问控制机制 C.数字签名机制 D.审计机制 E.公正机制

45.ISO安全体系结构中的对象认证安全服务，使用（ ）完成。

A.加密机制 B.数字签名机制 C.访问控制机制 D.数据完整性机制

41-45 ADEDB

46.CA属于ISO安全体系结构中定义的（ ）。

A.认证交换机制 B.通信业务填充机制 C.路由控制机制 D.公证机制

47.数据保密性安全服务的基础是（ ）。

A.数据完整性机制 B.数字签名机制 C.访问控制机制 D.加密机制

48.路由器控制机制用以防范（ ）。

A.路由器被攻击破坏 B.非法用户利用欺骗性的路由协议，篡改路由信息、窃取敏感数据

C.在网络层面进行分析，防止非法信息通过路由 D.以上皆非

49.数据完整性安全机制可与（ ）使用相同的方法实现。

A.加密机制 B.公正机制 C.数字签名机制 D.访问控制机制

50.可以被数据完整性机制防止的攻击方式（ ）。

A.假冒源地址或用户的地址欺骗攻击 B.抵赖做过信息的递交行为

C.数据中途被攻击者窃听获取 D.数据在途中被攻击者篡改或破坏

46-50 DDBCD

51.分组过滤型防火墙原理上是基于（ ）进行分析的技术。

A.物理层 B.数据链路层 C.网络层 D.应用层

52.对动态网络地址转换NAT，下面说法不正确的是（ ）。

A.将很多内部地址映射到单个真实地址 B.外部网络地址和内部地址一对一的映射

C.最多可有64 000个同时的动态NAT连接 D.一个内部桌面系统最多可同时打开32个连接

53.ISO/IEC网络安全体系结构的安全层提供网络安全的层次解决方案，下面说法不正确的是（ ）。

A.基础设施安全层支持服务安全层 B.服务安全层支持应用安全层

C.安全层的含义和OSI层次安全的含义是完全相同的 D.应用安全层支持服务安全层

54.ISO/IEC网络安全体系结构的安全维包含（ ）个安全度量，用于实施网络安全的某一特定方面的安全控制措施。

A.5 B.7 C.8 D.3

55.通常所说的移动VPN是指（ ）。

A. Access VPN B. Intranet VPN C. Extranet VPN D.以上皆不是

51-55 CBCCA

56.属于第二层的VPN隧道协议有（ ）。

A. IPSec B. PPTP C. GRE D.以上皆不是

57.GRE协议（ ）。

A.既封装，又加密 B.只封装，不加密 C.不封装，只加密 D.不封装，不加密

58.PPTP客户端使用（ ）建立连接。

A. CP协议 B.UDP协议 C. L2TP协议 D.以上皆不是

59.GRE协议的乘客协议是（ ）。

A. IP B. IPX C. Apple Talk D.以上皆可

60.IPSec协议和（ ）VPN隧道协议处于同一层。

A. PPTP B. L2TP C. GRE D.以上皆是

56-60 BBADC

61.AH协议中必须实现的验证算法是（ ）。

A. HMAC-MD5和HMAC-SHA1 B.NULL

C.HMAC-RIPEMD-160 D.以上皆是

62.ESP协议中不是必须实现的验证算法的是（ ）。

A.HMACMD5 B.HMAC-SHA1 C.NULL D.HMAC-RIPEMD-160

63.ESP协议中必须实现的加密算法是（ ）。

A.仅DES-CBC B.仅NULL C.DES-CBC和NULL D.3DES-CBC

64.（ ）协议必须提供验证服务。

A. AH B. ESP C. GRE D.以上皆是

65.IKE协商的第一阶段可以采用（ ）。

A.主模式、快速模式 B.快速模式、积极模式 C.主模式、积极模式 D.新组模式

61-65 ADCAC

66.IKE协议由（ ）协议混合而成。

A.ISAKMP、Oakley、SKEME B. AH、ESP C. L2TP、GRE D.以上皆不是

67.下列协议中，（ ）协议的数据可以收到IPSec的保护。

A. TCP、UDP、IP B. ARP C. RARP D.以上皆可以

68.“会话侦听与劫持技术”属于（ ）技术。

A.密码分析还原 B.协议漏洞渗透 C.应用漏洞分析与渗透 D. DoS攻击

69.网络应用安全平台WebST是（ ）的实现。

A. CA B. AAs C.应用

70.安全威胁可分为外部安全威胁与内部安全威胁两类。由威胁引起的损失可分为直接损失和间接损失两类。根据美国CSI/FBI的统计资料，大部分严重的经济损失来自（ ）内部安全威胁，而（ ）又占总损失的大部分。

A.外部，间接 B.内部，间接 C.内部，直接 D.外部，直接

66-70 AABBB

71.安全模型的核心组成是（ ）和（ ）。

A.风险评估，安全策略 B.信息分类处理，安全需求

C.风险评估，信息分类处理 D.上面3项都不是

72.（ ）与（ ）能使企业在发生重大破坏事件时保持正常的经营业务的运行。

A. BIA、BCP B. BCP、DRP C. BIA、DRP D.上面3项都是

73.技术安全需求集中在对（ ）的控制上，而技术安全控制的主要目标是保护组织信息资产的（ ）。

A.计算机系统，完整性 B.网络系统，可用性

C.应用程序，机密性 D.上面3项都是

74.计算机系统的鉴别包括（ ）。

A.用户标识认证 B.传输原发点得鉴别 C.内容鉴别及特征检测 D.以上3项都是

75.安全设计是（ ），一个安全基础设施应提供很多安全组件的（ ）使用。

A.一门艺术，各种 B.一门学科，协同 C.一项工程，分别 D.艺术、科学和工程集于一体，协同

71-75CBDDD

76.安全设施的主要组成是（ ）。

A.网络和平台 B.平台和物理设施 C.物理设施和处理过程 D.上面3项都是

77.安全基础设施的基本目标是保护（ ）。

A.企业的网络 B.企业的资产 C.企业的平台 D.企业的知识财产

78.安全基础设施设计指南应包括（ ）。

A.保证企业安全策略和过程和当前经营业务目标一致

B.开发一个计算机事故响应组CIRT

C.设计基础设施安全服务

D.以上三项都是

79.支撑性基础设施是能提供安全服务的一套相互关联的活动与基础设施，最重要的支撑性基础设施是（ ）。

A. KMI/PKI B.PKI以及检查与响应 C.KMI/PKI以及检查与响应 D.以上3项都不是

80.KMI/PKI支持的服务不包括（ ）。

A.非对称密钥技术及证书管理 B.对称密钥的产生和吩咐

C.访问控制服务 D.目录服务

76-80DBDCC

81.PKI的主要组成不包括（ ）。

A.证书授权CA B.SSL C.注册授权RA D.证书存储库CR

82.PKI管理对象不包括（ ）。

A.ID和口令 B.证书 C.密钥 D.证书撤销列表

83.下列基础设施目录服务的特性（ ）是不正确的。

A.优化的数据恢复 B.定义的名字空间 C.高度的集中性 D.提供对多种应用的访问

84.信息系统安全工程ISSE时由美国国家安全局发布的《信息保障技术框架（IATF）》3.0版本中提出的设计和实施信息系统（ ）。

A.安全工程方法 B.安全工程框架 C.安全工程体系结构 D.安全工程标准

81-84 BACA

网络信息安全技术

一、选择题

1. \_\_\_\_B\_\_\_\_情景属于授权（Authorization）。

a. 用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

b. 用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

c. 某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

d. 用户依照系统提示输入用户名和口

2. 入侵检测系统的第一步是：\_\_\_A\_\_\_\_。

a. 信息收集

b. 数据包过滤

c. 数据包检查

d. 信号分析

3. 数据保密性安全服务的基础是\_\_\_C\_\_\_。

a. 数字签名机制

b. 访问控制机制

c. 加密机制

d. 数据完整性机制

4. 下面所列的\_\_B\_\_安全机制不属于信息安全保障体系中的事先保护环节。

a. 防火墙

b. 杀毒软件

c. 数据库加密

d. 数字证书认证

5. 在生成系统帐号时，系统管理员应该分配给合法用户一个\_\_A\_\_，用户在第一次登录时应更改口令。

a. 唯一的口令

b. 登录的位置

c. 系统的规则

d. 使用的说明

6. 在计算机病毒检测手段中，校验和法的优点是\_\_\_\_C\_\_\_\_\_。

a. 不会误

b. 能检测出隐蔽性病毒

c. 能发现未知病毒

d. 能识别病毒名称

7. 为了提高电子设备的防电磁泄漏和抗干扰能力，可采取的主要措施是\_\_\_\_D\_\_\_\_。

a. 对机房进行防静电处理

b. 对机房进行防尘处理

c. 对机房进行防潮处理

d. 对机房或电子设备进行电磁屏蔽处理

8. \_\_\_\_C\_\_\_\_\_不属于ISO/OSI安全体系结构的安全机制。

a. 访问控制机制

b. 通信业务填充机制

c. 审计机制

d. 数字签名机制

9. 对网络层数据包进行过滤和控制的信息安全技术机制是\_C\_\_\_。

a. IDS

b. Sniffer

c. 防火墙

d. IPSec

10. 防火墙通常被比喻为网络安全的大门，但它不能\_\_\_\_B\_\_\_\_\_。

a. 阻止基于IP包头的攻击

b. 阻止病毒入侵

c. 阻止非信任地址的访问

d. 鉴别什么样的数据包可以进出企业内部网

11. 为了防御网络监听，最常用的方法是\_\_\_C\_\_\_。

a. 使用专线传输

b. 无线网

c. 数据加密

d. 采用物理传输（非网络）

12. 应用代理防火墙的主要优点是\_\_A\_\_。

a. 安全控制更细化、更灵活

b. 服务对象更广

c. 安全服务的透明性更好

d. 加密强度更高

13. ISO安全体系结构中的对象认证服务，使用\_\_\_B\_\_\_完成。

a. 访问控制机制

b. 数字签名机制

c. 加密机制

d. 数据完整性机制

14. 下列关于网络防火墙说法错误的是\_\_\_\_D\_\_\_。

a. 网络防火墙不能防止策略配置不当或错误配置引起的安全威胁

b. 网络防火墙不能解决来自内部网络的攻击和安全问题

c. 网络防火墙不能防止本身安全漏洞的威胁

d. 网络防火墙能防止受病毒感染的文件的传输

15. 不属于计算机病毒防治的策略的是\_\_\_C\_\_\_\_。

a. 新购置的计算机软件也要进行病毒检测

b. 及时、可靠升级反病毒产品

c. 整理磁盘

d. 确认您手头常备一张真正"干净"的引导盘

16. \_\_\_B\_\_\_情景属于审计（Audit）。

a. 用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

b. 某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

c. 用户依照系统提示输入用户名和口令

d. 用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

17. ISO 7498-2从体系结构观点描述了5种安全服务，以下不属于这5种安全服务的是\_\_\_B\_\_\_\_。

a. 授权控制

b. 数据报过滤

c. 数据完整性

d. 身份鉴别

18. 计算机病毒的危害性表现\_\_\_\_B\_\_\_\_。

a. 不影响计算机的运行速度

b. 影响程序的执行，破坏用户数据与程序

c. 能造成计算机器件永久性失效

d. 不影响计算机的运算结果，不必采取措施

19. 信息的完整性包含有信息来源的完整以及信息内容的完整，下列安全措施中能保证信息来源的完整性是\_\_\_\_C\_\_\_。

a. 认证

b. 加密、访问控制

c. 数字签名、时间戳

d. 预防、检测、跟踪

20. 由计算机及其相关的好配套设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集加工、存储、传输、检索等处理的人机系统是\_\_\_C\_\_\_\_\_。

a. 计算机工作系统

b. 计算机操作系统

c. 计算机信息系统

d. 计算机联机系统

21. 假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于＿B＿＿。

a. 分组密码技术

b. 古典密码技术

c. 对称加密技术

d. 公钥加密技术

22. 以下关于计算机病毒的特征说法正确的是：\_\_\_B\_\_\_\_。

a. 计算机病毒只具有传染性，不具有破坏性

b. 破坏性和传染性是计算机病毒的两大主要特征

c. 计算机病毒具有破坏性，不具有传染

d. 计算机病毒只具有破坏性，没有其他特征

23. 下列计算机病毒检测手段中，主要用于检测已知病毒的是\_\_\_\_B\_\_\_\_。

a. 校验和法

b. 特征代码法

c. 行为监测法

d. 软件模拟法

24. 确保授权用户或者实体对于信息及资源的正常使用不会被异常拒绝，允许其可靠而且及时地访问信息及资源的特性是\_\_A\_\_。

a. 可用性

b. 可靠性

c. 完整性

d. 保密性

25. 在被屏蔽的主机体系中，堡垒主机位于\_\_\_A\_\_\_\_中，所有的外部连接都经过滤路由器到它上面去。

a. 内部网络

b. 周边网络

c. 自由连接

d. 外部网络

26. 社会发展三要素是指：物质、能源和\_\_B\_\_\_。

a. 计算机网络

b. 信息

c. 互联网

d. 数据

27. 网络信息未经授权不能进行改变的特性是\_\_B\_\_。

a. 可用性

b. 完整性

c. 可靠性

d. 保密性

28. 对口令进行安全性管理和使用，最终是为了\_\_A\_\_。

a. 防止攻击者非法获得访问和操作权限

b. 规范用户操作行为

c. 口令不被攻击者非法获得

d. 保证用户帐户的安全性

29. 信息安全问题是一个\_\_\_D\_\_\_问题

a. 硬件

b. 软件

c. 综合

d. 系统

30. 数据在存储过程中发生了非法访问行为，这破坏了信息安全的\_\_C\_\_属性。

a. 完整性

b. 不可否认性

c. 保密性

d. 可用性

31. 防火墙能够\_\_D\_\_。

a. 防范恶意的知情者

b. 防备新的网络安全问题

c. 完全防止传送已被病毒感染的软件和文件

d. 防范通过它的恶意连接

32. 编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码是\_\_D\_\_\_\_\_.。

a. 计算机游戏

b. 计算机系统

c. 计算机程序

d. 计算机病毒

33. 以下哪一项不属于入侵检测系统的功能：\_\_\_A\_\_\_\_\_。

a. 过滤非法的数据包

b. 监视网络上的通信数据流

c. 提供安全审计报告

d. 捕捉可疑的网络活动

34. Internet的影响越来越大，人们常把它与报纸、广播、电视等传统媒体相比较，称之为\_\_\_B\_\_\_。

a. 交流媒体

b. 第四媒体

c. 交互媒体

d. 全新媒体

35. 以下哪一项不在证书数据的组成中\_\_D\_\_\_\_\_。

a. 有效使用期限

b. 版本信息

c. 签名算法

d. 版权信息

36. 保证用户和进程完成自己的工作而又没有从事其他操作可能，这样能够使失误出错或蓄意袭击造成的危害降低，这通常被称为\_\_D\_\_。

a. 适度安全原则

b. 分权原则

c. 木桶原则

d. 授权最小化原则

37. \_\_\_C\_\_\_是目前信息处理的主要环境和信息传输的主要载体

a. WAN

b. 信息网络

c. 计算机网络

d. 互联网

38. 定期对系统和数据进行备份，在发生灾难时进行恢复。该机制是为了满足信息安全的\_\_C\_\_属性。

a. 不可否认

b. 完整性

c. 可用性

d. 真实性

39. 针对操作系统安全漏洞的蠕虫病毒根治的技术措施是\_\_A\_\_。

a. 安装安全补丁程序

b. 专用病毒查杀工具

c. 防火墙隔离

d. 部署网络入侵检测系统

40. 机房中的三度不包括\_C\_\_\_\_。

a. 湿度

b. 温度

c. 可控度

d. 洁净度

41. 以下哪一项属于基于主机的入侵检测方式的优势：\_\_\_A\_\_\_\_。

a. 不要求在大量的主机上安装和管理软件

b. 适应交换和加密

c. 具有更好的实时性

d. 监视整个网段的通信

42. 关于双钥密码体制的正确描述是\_\_\_\_A\_\_\_。

a. 双钥密码体制中加解密密钥不相同，从一个很难计算出另一个

b. 双钥密码体制中加密密钥与解密密钥相同，或是实质上等同

c. 双钥密码体制中加解密密钥虽不相同，但是可以从一个推导出另一个

d. 双钥密码体制中加解密密钥是否相同可以根据用户要求决定

43. 统计数据表明，网络和信息系统最大的人为安全威胁来自于\_A\_\_\_。

a. 内部人员

b. 互联网黑客

c. 第三方人

d. 恶意竞争对手

44. 关于审计跟踪技术的描述，\_\_\_B\_\_\_\_是错误的。

a. 操作系统必须能生成、维护和保护审计过程。

b. 所有用户都能开启和关闭审计跟踪服务。

c. 审计过程一般是一个独立的过程，它应与系统其他功能隔离开。

d. 好的审计跟踪系统可以进行实时监控和报警。

45. PKI是\_\_A\_\_。

a. Public Key lnstitute

b. Private Key lnfrastructure

c. Public Key lnfrastructure

d. Private Key lnstitute

46. 计算机病毒的结构不包括\_\_\_\_A\_\_\_\_\_部分。

a. 隐藏部分

b. 激发部分

c. 传染部

d. 引导部分

47. \_\_D\_\_是最常用的公钥密码算法。

a. DSA

b. 椭圆曲线

c. 量子密码

d. RSA

48. 向有限的空间输入超长的字符串是一种\_\_B\_\_\_\_攻击手段。

a. 拒绝服务

b. 缓冲区溢出

c. IP欺骗

d. 网络监

49. 20世纪70年代后期，特别是进入90年代以来，美国、德国、英国、加拿大、澳大利亚、法国等西方发达国家为了解决计算机系统及产品的安全评估问题，纷纷制订并实施了一系列安全标准。如：美国国防部制订的"彩虹"系列标准，其中最具影响力的是"可信计算机系统标准评估准则"（简称TCSEC，\_\_B\_\_\_）

a. 白皮书

b. 桔皮书

c. 黄皮书

d. 黑皮书

50. 包过滤的基本思想是：对所接收的每个数据包进行检查，根据\_\_A\_\_\_\_\_，然后决定转发或者丢弃该包

a. 过滤规则

b. 用户需要

c. 安全策略

d. 数据流向

51. 黑客在程序中设置了后门，这体现了黑客的\_\_\_C\_\_\_\_\_目的。

a. 利用有关资源

b. 窃取信息

c. 非法获取系统的访问权限

d. 篡改数据

52. 使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于\_\_\_C\_\_攻击类型。

a. BIND漏洞

b. 远程过程调用

c. 拒绝服务

d. 文件共享

53. 文件被感染上病毒之后，其基本特征是\_\_\_B\_\_\_\_。

a. 文件长度变短

b. 文件长度加长

c. 文件照常能执行

d. 文件不能被执行

54. 以下方法中，不适用于检测计算机病毒的是\_\_\_D\_\_\_\_

a. 软件模拟法

b. 特征代码法

c. 校验和法

d. 加密

55. 以下哪项技术不属于预防病毒技术的范畴\_\_\_\_A\_\_\_。

a. 加密可执行程序

b. 校验文件

c. 引导区保护

d. 系统监控与读写控制

56. 我国正式公布了电子签名法，数字签名机制用于实现\_\_A\_\_需求。

a. 不可抵赖性

b. 保密性

c. 完整性

d. 可用性

57. 关于A类机房应符合的要求，以下选项不正确的是\_\_\_C\_\_\_\_\_。

a. 供电电源设备的容量应具有一定的余量

b. .计算站应设专用可靠的供电线路

c. 计算机系统应选用铜芯电缆

d. 计算站场地宜采用开放式蓄电池

58. \_\_\_\_D\_\_\_功能属于操作系统中的日志记录功能。

a. 以合理的方式处理错误事件，而不至于影响其他程序的正常运行

b. 保护系统程序和作业，禁止不合要求的对程序和数据的访问

c. 控制用户的作业排序和运行

d. 对计算机用户访问系统和资源的情况进行记录

59. 关于安全审计目的描述错误的是\_\_A\_\_。

a. 实现对安全事件的应急响应

b. 识别和分析未经授权的动作或攻击

c. 将动作归结到为其负责的实体

d. 记录用户活动和系统管理

60. PKI所管理的基本元素是\_B\_\_\_。

a. 用户身份

b. 数字证书

c. 数字签名

d. 密钥

61. 拒绝服务攻击造成的后果是\_\_\_D\_\_\_。

a. 硬盘被格式化

b. 硬件损坏

c. 文件被删除

d. 系统无法提供正常的服务

62. 防火墙最主要被部署在\_B\_\_\_位置。

a. 重要服务器

b. 网络边界

c. 桌面终端

d. 骨干线路

63. 关于防火墙的错误说法是\_\_C\_\_。

a. 防火墙工作在网络层

b. 对IP数据包进行分析和过滤

c. 部署防火墙，就解决了网络安全问题

d. 重要的边界保护机制

64. 能够有效地防御未知的新病毒对信息系统造成破坏的安全措施是\_\_C\_\_。

a. 安装安全补丁程序

b. 专用病毒查杀工具

c. 防火墙隔离

d. 部署网络入侵检测系统

65. \_\_C\_\_\_\_不是计算机病毒所具有的特点。

a. 潜伏性

b. 传染性

c. 可预见性

d. 破坏性

66. 在每天下午5点使用计算机结束时断开终端的连接属于\_\_B\_\_\_\_\_。

a. 网络地址欺骗

b. 外部终端的物理安全

c. 窃听数据

d. 通信线的物理安全

67. PGP（Pretty Good Privacy）是用于\_\_\_A\_\_\_\_传输安全的。

a. 用于邮件的传输安全

b. 用于WEB 服务器的数据安全

c. 用于FTP传输的安全

d. 浏览器传输的安全

68. 我国在1999年发布的国家标准\_\_A\_\_为信息安全等级保护奠定了基础。

a. GB 17859

b. GB 17799

c. GB 15408

d. GB 14430

69. 用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于\_C\_\_\_手段。

a. DDOS攻击

b. 暗门攻击

c. 钓鱼攻击

d. 缓存溢出攻击

70. PKI的主要理论基础是\_\_A\_\_。

a. 公钥密码算法

b. 对称密码算法

c. 摘要算法

d. 量子密码

71. 堡垒主机是一种配置了安全防范措施的网络上的计算机，堡垒主机为网络之间的通信提供了一个\_\_\_D\_\_\_\_，也就是说如果没有堡垒主机，网络之间将不能相互访问。

a. 连接点

b. 桥梁

c. 交换接口

d. 阻塞点

72. 可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯：\_\_\_A\_\_\_。

a. 防火墙

b. 防病毒产品

c. 加密机

d. CA中心

73. 以下关于宏病毒说法正确的是：\_\_A\_\_\_\_。

a. 宏病毒仅向办公自动化程序编制的文档进行传染

b. 宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区

c. CIH病毒属于宏病毒

d. 宏病毒主要感染可执行文件

74. Windows的日志文件很多，但主要是\_\_\_\_C\_\_\_、应用程序日志和安全日志三个

a. 事件日志

b. 用户日志

c. 系统日志

d. 审计日志

75. 文件型病毒传染的对象主要是\_\_\_C\_\_\_。

a. PRG

b. DBF

c. COM和EXE

d. C

76. 一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于\_\_\_A\_\_\_\_\_基本原则。

a. 最小特权

b. 防御多样化

c. 阻塞点

d. 失效保护状态

77. 阈值检验在入侵检测技术中属于\_\_\_A\_\_\_。

a. 量化分析法

b. 免疫学方法

c. 神经网络法

d. 状态转换法

78. 防火墙用于将Internet和内部网络隔离，＿A＿＿。

a. 是网络安全和信息安全的软件和硬件设施

b. 是起抗电磁干扰作用的硬件设施

c. 是防止Internet火灾的硬件设施

d. 是保护线路不受破坏的软件和硬件设施

79. 确保信息在存储、使用、传输过程中不会泄露给非授权的用户或者实体的特性是\_D\_\_\_。

a. 完整性

b. 可用性

c. 可靠性

d. 保密性

80. 信息保障阶段中将信息安全体系归结为四个主要环节，\_\_B\_\_是正确的。

a. 加密、认证、保护、检测

b. 保护、检测、响应、恢复

c. 策略、网络攻防、密码学、备份

d. 策略、保护、响应、恢复

81. 常见的认证技术包括：数字签名、报文认证和\_\_C\_\_\_\_

a. 私钥密钥

b. 公钥密钥

c. 数字水印

d. 签名算法

82. 入侵检测技术可以分为误用检测和\_\_D\_\_两大类。

a. 病毒检测

b. 漏洞检测

c. 详细检测

d. 异常检测

83. \_\_\_\_\_A\_\_\_\_情景属于身份验证（Authentication）过程。

a. 用户依照系统提示输入用户名和口令

b. 用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

c. 某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

d. 用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

84. 网上银行系统的一次转账操作过程中发生了转账金额被非法篡改的行为，这破坏了信息安全的\_\_A\_\_属性。

a. 完整性

b. 保密性

c. 不可否认性

d. 可用性

85. 可以被数据完整性机制防止的攻击方式是\_\_\_\_\_C\_\_。

a. 数据中途被攻击者窃听获取

b. 抵赖做过信息的递交行为

c. 数据在途中被攻击者篡改或破坏

d. 假冒源地址或用户的地址欺骗攻击

86. 突破网络系统的第一步是\_\_\_\_C\_\_\_。

a. 源路由选择欺骗

b. 口令破解

c. 各种形式的信息收集

d. 利用TCP/IP协议的攻击

87. OSI 安全体系结构中定义了五大类安全服务，其中，数据机密性服务主要针对的安全威胁是\_\_\_C\_\_\_\_\_。

a. 拒绝服务

b. 服务否认

c. 窃听攻击

d. 硬件故障

88. 等级保护标准GB l7859主要是参考了\_\_A\_\_而提出。

a. 美国TCSEC

b. CC

c. BS 7799

d. 欧洲ITSEC

89. 为保证计算机网络系统的正常运行，对机房内的三度有明确的要求。其三度是指\_\_D\_\_\_\_。

a. 照明度、湿度和洁净度

b. 照明度、温度和湿度

c. 温度、照明度和洁净度

d. 温度、湿度和洁净度

90. 以下哪一项不是入侵检测系统利用的信息：\_\_A\_\_\_。

a. 数据包头信息

b. 系统和网络日志文件

c. 目录和文件中的不期望的改变

d. 程序执行中的不期望行为

91. 入侵检测系统在进行信号分析时，一般通过三种常用的技术手段，以下哪一种不属于通常的三种技术手段\_\_\_A\_\_\_\_\_。

a. 密文分析

b. 模式匹配

c. 统计分

d. 完整性分析

92. \_\_\_\_\_B\_\_\_\_\_没有在通常的访问控制策略之中。

a. 基于角色的访问控制

b. 被动访问控制

c. 强制访问控制

d. 自主访问控制

93. 在以下认证方式中，最常用的认证方式是\_\_\_\_A\_\_\_\_。

a. 基于账户名／口令认证

b. 基于摘要算法认证

c. 基于数据库认证

d. 基于PKI认证

94. ISO 7498-2描述了8种特定的安全机制，以下不属于这8种安全机制的是\_\_\_D\_\_\_。

a. 加密机制

b. 数字签名机制

c. 访问控制机制

d. 安全标记机制

95. 许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是\_\_\_\_D\_\_\_。

a. 安装入侵检测系统

b. 安装防火墙

c. 安装防病毒软件

d. 给系统安装最新的补丁

96. 在短时间内向网络中的某台服务器发送大量无效连接请求，导致合法用户暂时无法访问服务器的攻击行为是破坏了\_\_\_B\_\_\_\_\_。

a. 机密性

b. 可用性

c. 可控性

d. 完整性

97. 通过对硬件设备、网络线路、电源、空调等的破坏，使系统无法正常工作，甚至导致程序和数据无法恢复，称之为\_\_\_A\_\_\_\_\_\_\_。

a. 物理破坏

b. 硬件破坏

c. 故意损坏

d. 硬件攻击

98. 公钥密码基础设施PKI解决了信息系统中的\_\_C\_\_问题。

a. 权限管理

b. 安全审计

c. 身份信任

d. 加密

99. 下列四项中不属于计算机病毒特征的是\_\_A\_\_。

a. 免疫性

b. 潜伏性

c. 传染性

d. 破坏性

100. 计算机病毒的核心是\_\_\_\_C\_\_\_\_。

a. 发作模块

b. 表现模块

c. 引导模块

d. 传染模块

101. 安全审计跟踪是\_\_B\_\_。

a. 安全审计系统收集易于安全审计的数据

b. 安全审计系统检测并追踪安全事件的过程

c. 对计算机系统中的某种行为的详尽跟踪和观察

d. 人利用日志信息进行安全事件分析和追溯的过程

102. 安全审计包括：个人职能、事件重建、入侵检测和\_\_D\_\_\_\_。

a. 事件跟踪

b. 安全审核

c. 应用程序跟踪

d. 故障分析

103. 病毒的运行特征和过程是\_\_\_\_C\_\_\_\_。

a. 传播、运行、驻留、激活、破坏

b. 入侵、运行、传播、扫描、窃取

c. 设计、传播、潜伏、触发、破坏

d. 复制、撤退、检查、运行、破坏

104. 通常所说的"病毒"是指\_\_C\_\_\_\_\_。

a. 生物病毒感染

b. 被损坏的程序

c. 特制的具有破坏性的程序

d. 细菌感染

105. 下列行为不属于攻击的是\_\_C\_\_\_\_\_。

a. 发送带病毒和木马的电子邮件

b. 用字典猜解服务器密码

c. 从FTP服务器下载一个10GB的文件

d. 对一段互联网IP进行扫描

106. 针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，这是\_\_A\_\_\_防火墙的特点。

a. 代理服务型

b. 应用级网关型

c. 包过滤型

d. 复合型防火墙

107. 中华人民共和国《计算机信息系统安全保护等级划分准则》GB17859-1999中，将计算机安全等级划分为\_\_\_A\_\_\_。

a. 5级

b. 8级

c. 10级

d. 3级

108. CA属于ISO安全体系结构中定义的\_\_\_C\_\_\_\_。

a. 通信业务填充机制

b. 认证交换机制

c. 公证机制

d. 路由控制机制

109. 计算机会将系统中可使用内存减少，这体现了病毒的\_\_\_\_B\_\_\_\_。

a. 传染性

b. 破坏性

c. 潜伏性

d. 隐藏性

110. 关于RSA算法下列说法不正确的是\_\_A\_\_\_\_\_。

a. RSA算法是一种对称加密算法

b. RSA算法可用于某种数字签名方案。

c. RSA算法的运算速度比DES慢。

d. RSA算法的安全性主要基于素因子分解的难度

111. PDRR模型中的D 代表的含义是\_\_\_A\_\_\_\_。

a. 检测

b. 安全

c. 关系

d. 响应

112. \_\_A\_\_最好地描述了数字证书。

a. 等同于在网络上证明个人和公司身份的身份证

b. 浏览器的一标准特性，它使得黑客不能得知用户的身份

c. 伴随在线交易证明购买的收据

d. 网站要求用户使用用户名和密码登陆的安全机制

113. ISO定义的安全体系结构中包含\_\_A\_\_\_种安全服务。

a. 5

b. 6

c. 4

d. 7

114. 黑客攻击过程是：确定目标、\_\_\_\_\_C\_\_\_\_和实施攻击

a. 入侵系统

b. 暴力破解用户口

c. 收集与攻击目标相关信息

d. 准备有关攻击工具

115. 关于用户口令说法错误的是\_B\_\_\_。

a. 口令不能设置为空

b. 复杂口令安全性足够高，不需要定期修改

c. 口令长度越长，安全性越高

d. 口令认证是最常见的认证机制

116. 为了数据传输时不发生数据截获和信息泄密，采取了加密机制。这种做法体现了信息安全的\_\_D\_\_属性。

a. 可靠性

b. 可用性

c. 完整性

d. 保密性

117. 互联网的"无序、无界、\_C\_\_\_"三大基本特征决定了网络信息的不安全。

a. 木马入侵

b. 黑客攻击

c. 匿名

d. 操作系统漏洞

118. 传统的文件型病毒以计算机操作系统作为攻击对象，而现在越来越多的网络蠕虫病毒将攻击范围扩大到了\_\_C\_\_等重要网络资源。

a. 数据包

b. LINUX

c. 网络带宽

d. 防火墙

119. Windows 2003系统能设置为在几次无效登录后锁定帐号，这可以防止\_\_\_A\_\_\_\_\_。

a. 暴力攻击

b. 木马

c. IP欺骗

d. 缓存溢出攻击

120. 入侵检测系统(IDS，Intrusion Detection System)是对\_\_\_C\_\_\_的合理补充，帮助系统对付网络攻击。

a. 路由器

b. 交换机

c. 防火墙

d. 服务器

121. 软件驻留在用户计算机中，侦听目标计算机的操作，并可对目标计算机进行特定操作的黑客攻击手段是\_\_\_\_B\_\_\_\_\_。

a. 暴力破解

b. 木马

c. 拒绝服务

d. 缓冲区溢出

122. 以下哪一种方式是入侵检测系统所通常采用的：\_\_\_A\_\_\_。

a. 基于网络的入侵检测

b. 基于域名的入侵检测

c. 基于IP的入侵检测

d. 基于服务的入侵检测

123. 在各种防火墙结构中，就其本质而言，主要有以下四种：屏蔽路由器、双宿/多宿主机模式、\_\_\_A\_\_\_和屏蔽子网模式

a. 屏蔽主机模式

b. 堡垒主机模式

c. 代理服务器模式

d. 应用级网关模式

124. 用于实现身份鉴别的安全机制是\_\_B\_\_\_\_。

a. 访问控制机制和路由控制机制

b. 加密机制和数字签名机制

c. 加密机制和访问控制机制

d. 数字签名机制和路由控制机制

125. 以下不属于代理服务技术优点的是\_\_\_D\_\_\_\_\_\_

a. 可以实现身份认证

b. 可以实现访问控制

c. 内部地址的屏蔽和转换功能

d. 可以防范数据驱动侵袭

126. 未经授权的方式使用网络资源，称之为\_\_A\_\_\_

a. 非法访问

b. 窃取

c. 非法入侵

d. 冒充

127. 包过滤技术与代理服务技术相比较\_\_\_C\_\_\_\_\_。

a. 包过滤技术安全性较弱、但会对网络性能产生明显影响

b. 代理服务技术安全性高，对应用和用户透明度也很

c. 包过滤技术对应用和用户是绝对透明的

d. 代理服务技术安全性较高、但不会对网络性能产生明显影

128. 下列不属于防火墙核心技术的是\_C\_\_\_。

a. 应用代理技术

b. NAT技术

c. 日志审计

d. (静态／动态)包过滤技术

129. 下列对计算机网络的攻击方式中，属于被动攻击的是\_\_\_\_C\_\_\_。

a. 拒绝服务

b. 物理破坏

c. 口令嗅探

d. 重放

130. 计算机网络安全的目标不包括\_A\_\_\_\_。

a. 免疫性

b. 不可否认性

c. 完整性

d. 保密性

131. 计算机网络是地理上分散的多台\_\_\_A\_\_\_遵循约定的通信协议，通过软硬件互联的系统。

a. 自主计算机

b. 数字设备

c. 主从计算机

d. 计算机

132. 下列有关计算机病毒分类的说法，\_D\_\_\_\_\_是正确的。

a. 没有分类之说

b. 病毒分为十二类

c. 病毒分为操作系统型和文件型

d. 病毒分为外壳型和入侵型

133. 关于入侵检测技术，下列描述错误的是\_\_D\_\_。

a. 入侵检测信息的统计分析有利于检测到未知的入侵和更为复杂的入侵

b. 审计数据或系统日志信息是入侵检测系统的一项主要信息来源

c. 基于网络的入侵检测系统无法检查加密的数据流

d. 入侵检测系统不对系统或网络造成任何影响

134. 防火墙是指\_\_\_D\_\_\_。

a. 一批硬件的总

b. 一个特定软件

c. 一个特定硬件

d. 执行访问控制策略的一组系统

135. 以下关于DOS攻击的描述，正确的是\_\_\_A\_\_\_\_\_。

a. 导致目标系统无法处理正常用户的请求

b. 不需要侵入受攻击的系统

c. 以窃取目标系统上的机密信息为目

d. 如果目标系统没有漏洞，远程攻击就不可能成功

136. 不属于常见的危险密码是\_\_\_D\_\_\_\_。

a. 跟用户名相同的密码

b. 只有4位数的密码

c. 使用生日作为密码

d. 8位的数字+字符+符号的混合型密码

137. 计算机病毒造成的危害是\_\_\_\_B\_\_\_\_。

a. 使计算机系统突然掉电

b. 破坏计算机系统

c. 使磁盘发霉

d. 使计算机内存芯片损坏

138. 数字签名要预先使用单向Hash函数进行处理的原因是＿＿C＿。

a. 保证密文能正确还原成明文

b. 多一道加密工序使密文更难破译

c. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

d. 提高密文的计算速度

139. 使用Windows2000的组策略，可以限制用户对系统的操作权限，该实例是\_\_\_B\_\_的应用。

a. 执行控制列表

b. 访问控制列表

c. 身份验证

d. 数据加密

140. 下列不属于系统安全的技术是\_\_\_A\_\_\_\_。

a. 加密狗

b. 防病毒

c. 防火墙

d. 认证

141. 访问控制一般包括自主访问控制、强制访问控制和\_\_\_\_D\_\_\_\_3种类型：

a. 安全组访问控制

b. 用户访问控制

c. 基于域的访问控制

d. 基于角色的访问控制

142. 根据ISO的信息安全定义，下列选项中\_D\_\_\_是信息安全五个基本属性之一。

a. 可靠性

b. 可审计性

c. 真实性

d. 可用性

143. 身份认证的含义是\_\_A\_\_。

a. 验证一个用户

b. 标识一个用户

c. 授权一个用户

d. 注册一个用户

144. 下面入侵检测技术当中，哪一种是基于模式匹配技术的\_\_\_A\_\_\_。

a. 误用检测

b. 基于统计的检测

c. 异常检测

d. 基于数据挖掘的检测

145. Unix和Windows NT操作系统是符合那个级别的安全标准：\_\_D\_\_\_\_。

a. D级

b. A级

c. B级

d. C级

二、填空题

1. 计算机病毒有\_\_隐蔽性\_\_、潜伏性、传染性和破坏性四个特点。

2. 物理安全技术主要是指对计算机及网络系统的环境、场地、\_\_设备\_\_和人员等采取的安全技术措施。

3. 攻击者可以直接接触到信息与网络系统的硬件、软件和周边环境设备。通过对硬件设备、网络线路、电源、空调等的破坏，使系统无法正常工作，甚至导致程序和数据无法恢复。这种破坏是\_\_物理破坏\_\_\_\_\_\_

4. 防火墙对于的\_\_连入\_连接往往会进行非常严格的过滤，但是对于\_连出\_\_的连接却疏于防范

5. 对网络系统的攻击可分为：\_主动\_攻击和\_被动\_\_攻击两类。

6. 物理安全在整个计算机网络信息系统安全中占有重要地位。它主要包括：\_机房环境安全\_\_、通信线路安全、设备安全和电源安全

7. 密码体制目前分为\_\_对称密钥密码体制\_\_\_\_\_\_\_\_\_和\_\_\_非对称密钥密码\_\_\_\_\_\_体制。

8. ACL的中文含义为\_\_访问控制列表\_\_\_\_\_。

9. IDS的物理实现不同，按检测的监控位置划分，入侵检测系统可分为基于\_\_主机\_、基于\_网络\_和\_分布式系统\_\_。

10. 野蛮攻击包括\_字典攻击\_和穷举攻击

11. 屏蔽子网结构采用了两个包过滤路由器和一个堡垒主机，在内外网络之间建立了一个被隔离的子网，定义为"\_非军事区\_\_"网络，

12. 服务器端每间隔一定时间就发出连接控制端的请求，这个请求一直循环到与控制端成功连接。这种技术称之为\_反弹技术\_。

13. 通过篡改、删除和插入等方式破坏信息的\_完整性\_。

14. \_计算机网络\_\_是目前信息处理的主要环境和信息传输的主要载体

15. 机房安全技术包括计算机机房的安全保卫技术 ，计算机机房的温度、湿度等环境条件保持技术 ，计算机机房的用电安全技术和计算机机房\_安全管理技术\_\_等。

16. \_\_访问控制\_\_的目的是为了限制访问主体对访问客体的访问权限。

17. 物理安全是整个计算机网络系统安全的\_\_前提\_\_\_\_\_

18. 木马通常是利用蠕虫病毒、\_黑客入侵\_\_\_或者使用者的疏忽将服务器程序安装到主机上的。

19. 计算机病毒传染部分的主要作用是将病毒程序进行\_自我复制\_\_\_\_。

20. 认证的目的有三个：\_\_消息完整性认证\_\_\_\_、身份认证和报文的序号性、时间性认证。

21. 计算机系统的CPU、ROM、RAM等关键部件大都采用MOS工艺的大规模集成电路，对\_静电\_\_极为敏感，容易因此而损坏。

22. 密码学是关于\_加密\_和\_解密\_\_变换的一门科学，是保护数据和信息的有力武器。

23. 对于一个真正的黑客，如果想进入一个主机，就会不择手段的\_\_探索\_\_这个主机的信息，

24. 计算机病毒可分为引导型病毒和\_文件型\_\_病毒两类。

25. 如果攻击者组织多个攻击点对一个或多个目标同时发动DoS攻击，就可以极大地提高DoS攻击的威力，这种方式称为DDoS（Distributed Denial of Service，\_\_分布式拒绝服务\_）攻击。

26. 包过滤防火墙中包过滤器一般安装在\_路由器上\_，工作在\_网络层\_\_\_\_\_\_。

27. \_网络安全\_\_是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，网络服务不中断。

28. 网络安全涉及的内容既有\_\_技术\_\_方面的问题，也有管理方面的问题。

29. 当一个账号被创建时，Windows系统为它分配一个\_\_SID\_\_\_，并与其他账号信息一起存入SAM数据库。

30. 解密算法D是加密算法E的\_\_逆运算\_\_\_\_\_\_ 。

31. \_\_数字签名\_\_\_\_\_\_可以解决否认、伪造、篡改及冒充等问题。

32. 对计算机网络安全构成威胁的因素可以概括为：偶发因素、自然因素和\_人为因素\_三个方面。

33. 网络安全的目标包括：保密性、完整性、\_可用性\_\_、可控性和不可抵赖性。

34. 密码系统包括以下4个方面：\_明文空间\_\_、密文空间、密钥空间和密码算法。

35. \_Sniffer\_\_\_\_\_\_\_是指能解读、监视、拦截网络数据交换并且阅读数据包的程序或设备。

36. 蠕虫是通过\_计算机网络\_\_进行传播的。

37. 网络安全包括：实体安全、运行安全、\_数据安全\_\_和内容安全

38. 数字水印应"透明"、"\_健壮\_"和"安全"。

39. 在TCP／IP网络中，测试连通性的常用命令是\_\_ping\_。

40. 如果加密密钥和解密密钥\_\_相同\_\_，这种密码体制称为对称密码体制。

41. 网络安全是一个系统性概念，不仅包括网络信息的存储安全，还要涉及信息的产生、传输和\_使用过程\_\_\_\_\_\_中的安全。

42. 防抵赖技术的常用方法是\_\_数字签名\_\_。

43. Windows的日志文件很多，但主要是\_\_系统日志\_\_\_、应用程序日志和安全日志三个。网络安全主要涉及网络安全威胁的主要类型、网络攻击的手段、网络安全机制、网络安全技术以及\_\_信息安全等级标准\_\_等方面内容。

44. 在屏蔽主机结构中，屏蔽路由器使用包过滤技术，它只允许\_\_堡垒主机\_\_与外部通信，

45. 防范计算机病毒主要从管理和\_技术\_两方面着手。

46. 黑客对网络的攻击方式是多种多样的，一般来讲，攻击总是利用"\_系统配置的缺陷\_"，"操作系统的安全漏洞"或"通信协议的安全漏洞"来进行的。

47. GB/T 9387.2-1995定义了5大类 \_安全服务\_\_，提供这些服务的8种\_安全机制\_\_以及相应的开放系统互连的安全管理，并可根据具体系统适当地配置于OSI模型的七层协议中。

48. 从明文到密文的变换过程称为\_加密\_。

49. PKI的核心部分是\_CA\_\_\_ ，它同时也是数字证书的签发机构。

50. \_堡垒主机\_\_是一种配置了安全防范措施的网络上的计算机，

51. 应该说网络节点处的安全和\_\_通信链路\_\_\_\_\_上的安全共同构成了网络系统的安全体系。

52. 信息保障不仅包含安全防护的概念，更重要的是增加了主动和积极的\_\_防御\_\_\_\_观念。

53. 以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求就无法通过，这种攻击称之为\_带宽攻击\_\_。

54. 常规密钥密码体制又称为\_\_对称密钥密码体制\_\_，是在公开密钥密码体制以前使用的密码体制。

三、判断题

1. 为使机房内的三度达到规定的要求，空调系统、去湿机、除尘器是必不可少的设备。对

2. 恶意代码包括计算机病毒、蠕虫病毒、特洛伊木马程序、移动代码及间谍软件等。对

3. 安全管理从范畴上讲，涉及物理安全策略、访问控制策略、信息加密策略和网络安全管理策略。对

4. 防火墙既可以是一台路由器、一台计算机，也可以是由多台主机构成的体系。对

5. 在信息保障的概念下，信息安全保障的PDRR模型的内涵已经超出了传统的信息安全保密的范畴。对

6. 漏洞是指任何可以造成破坏系统或信息的弱点。对

7. 用户的密码一般应设置为8位以上。对

8. 公共密钥密码体制在密钥管理上比对称密钥密码体制更为安全。 对

9. 按计算机病毒的传染方式来分类，可分为良性病毒和恶性病毒。对

10. 最小特权、纵深防御是网络安全原则之一。对

11. TCSEC是美国的计算机安全评估机构和安全标准制定机构。对

12. 计算机病毒的传染和破坏主要是动态进行的。对

13. 认证技术是防止不法分子对信息系统进行主动攻击的一种重要技术。对

14. 可用性是指授权用户在需要时能不受其他因素的影响，方便地使用所需信息。 对

15. 国标GB2887－2000将供电方式分为了3类。对

16. 安全审计技术是网络安全的关键技术之一。对

17. 计算机信息系统的安全威胁同时来自内、外两个方面。对

18. 计算机病毒也是一种程序，它在某些条件下激活，起干扰破坏作用，并能传染到其他程序中。对

19. PGP使用的是非对称密钥技术。 对

20. 木马不是病毒。 对

21. 发起大规模的DDoS攻击通常要控制大量的中间网络或系统。对

22. 在设计系统安全策略时要首先评估可能受到的安全威胁。对

23. 计算机数据恢复在实际生活当中可以百分百恢复。错

24. 用杀病毒程序可以清除所有的病毒。错

25. 在计算机系统安全中，人的作用相对于软件，硬件和网络而言，不是很重要。错

26. 统计表明，网络安全威胁主要来自内部网络，而不是Internet。错

27. 电脑运行速度明显变慢一定是中病毒了。错

28. 我的计算机在网络防火墙之内，所以其他用户不可能对我计算机造成威胁。错

29. 蠕虫、特洛伊木马和病毒其实是一回事。错

30. 网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。错

31. 系统安全的责任在于IT技术人员，最终用户不需要了解安全问题。错

32. 格式化过后的计算机，原来的数据就找不回来了。错

33. 密码保管不善属于操作失误的安全隐患。错

34. 只要设置了足够强壮的口令，黑客不可能侵入到计算机中。错

35. 实体安全又称之为运行安全。错

36. 计算机机房的安全等级分为A、B、C、D等四个等级。错

37. 目前入侵检测系统可以及时的阻止黑客的攻击。错

38. "特洛伊木马"（Trojan Horse）程序是黑客进行IP欺骗的病毒程序。错

39. 工作人员的服装和鞋最好用化纤材料制作。错

40. 为了防御网络监听，最常用的方法是采用物理传输。错

41. C类机房必须配备防水设备。错

42. 使用最新版本的网页浏览器软件可以防御黑客攻击。错

43. 在Winodws NT操作系统中每一个对象（如文件，用户等）都具备多个SID。错

44. 病毒攻击是危害最大、影响最广、发展最快的攻击技术。错

45. 只要选择一种最安全的操作系统，整个系统就可以保障安全。错

46. 安全审计就是日志的记录。错

47. 拒绝服务是一种系统安全机制，它保护系统以防黑客对计算机网络的攻击。错

48. 对于一个计算机网络来说，依靠防火墙即可以达到对网络内部和外部的安全防护。错

49. PGP在只能对文件、邮件加密，不能实现身份验证的功能。错

50. 可用性是指信息在整个生命周期内都可由合法拥有者加以安全的控制。错

51. 在使用计算机时，最常见的病毒传播媒介是软盘。错

52. 能够达到C2级别的常见操作系统有： WindowsNT、Windows2000和Windows XP。错

53. 计算机病毒只会破坏磁盘上的数据和文件。错

54. 网络安全服务所需的网络安全机制包括数据真实性机制。错

55. 计算机病毒是计算机系统中自动产生的。错

56. 造成计算机不能正常工作的原因若不是硬件故障，就是计算机病毒。错

信息技术模拟考试题

1、计算机预防病毒感染有效的措施是( D )。

A.定期对计算机重新安装系统

B.不要把U盘和有病毒的U盘放在一起

C.不准往计算机中拷贝软件

D.给计算机安装防病毒的软件，并常更新

2、一个512MB的U盘能存储 B 字节(Byte)的数据量。

A.512×8

B.512×1024×1024

C.512×1024

D.512×1024×8

3、计算机病毒是 (B )。

A.计算机系统自生的

B.一种人为特制的计算机程序

C.主机发生故障时产生的

D.可传染疾病给人体

4、在计算机内部，数据是以 (A )形式加工、处理和传送的。

A.二进制码

B.八进制码

C.十进制码

D.十六进制码

5、下面列出的四种存储器中，断电后正在处理的信息会丢失的存储器是 (A) 。

A.RAM

B.ROM

C.PROM

D.EPROM

6、信息技术的四大基本技术是计算机技术、传感技术、控制技术和 (C) 。

A.生物技术

B.媒体技术

C.通信技术

D.传播技术

7、内存和外存相比，其主要特点是( C )。

A.能存储大量信息

B.能长期保存信息

C.存取速度快

D.能同时存储程序和数据

8、二十世纪末，人类开始进入 ( C )。

A. 电子时代

B. 农业时代

C. 信息时代

D. 工业时代

9、关于信息的说法，以下叙述中正确的是(D)。

A. 收音机就是一种信息

B. 一本书就是信息

C. 一张报纸就是信息

D. 报上登载的足球赛的消息是信息

10、下列不属于信息的是( C　 )。

A.报上登载的举办商品展销会的消息

B.电视中的计算机产品广告

C.计算机

D.各班各科成绩

11、多媒体信息不包括( 　D )。

A.影像、动画

B.文字、图形

C.音频、视频

D.硬盘、网卡

12、信息技术包括计算机技术、传感技术和(　C　 )。

A.编码技术

B.电子技术

C.通信技术

D.显示技术

13、使用大规模和超大规模集成电路作为计算机元件的计算机是( D　 )。

A.第一代计算机

B.第二代计算机

C.第三代计算机

D.第四代计算机

14、计算机系统由哪几部分组成( 　B )。

A.主机和外部设备

B.软件系统和硬件系统

C.主机和软件系统

D.操作系统和硬件系统

15、计算机的软件系统包括( 　B )。

A.程序和数据

B.系统软件与应用软件

C.操作系统与语言处理程序

D.程序、数据与文档

16、微型计算机中，I/O设备的含义是( 　C )。

A .输入设备

B.输出设备

C.输入输出设备

D.控制设备

17、在以下所列设备中,属于计算机输入设备的是( A　 )。

A.键盘

B.打印机

C.显示器

D.绘图仪

18、下列软件属于系统软件的是( 　D ) 。

A.PowerPoint

B.Word2007

C.Excel 2007

D.Windows 2007

19、某单位的人事档案管理程序属于( B　 )。

A.图形处理软件

B.应用软件

C.系统软件

D.字处理软件

20、以下哪一组软件都是应用软件( 　C )。

A.DOS、WINDOWS、WORD、EXCEL、VFP

B.WORD、EXCEL、UNIX、游戏、杀毒软件

C.游戏、POWERPOINT、WORD、EXCEL

D.WORD、DOS、EXCEL、声音编辑软件

1. 信息安全策略的制定和维护中，最重要是要保证其\_\_\_\_和相对稳定性。A

A 明确性 B 细致性 C 标准性 D 开放性

2. \_\_\_\_是企业信息安全的核心。C

A 安全教育 B 安全措施 C 安全管理 D 安全设施

3.编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码是\_\_\_\_。A

A 计算机病毒 B 计算机系统 C 计算机游戏 D 计算机程序

4.许多与PKI相关的协议标准(如PKIX、S/MIME、SSL、TLS、IPSec)等都是在\_\_\_\_基础上发展起来的。B

A X.500 B X.509 C X.519 D X.505

5. \_\_\_\_是PKI体系中最基本的元素，PKI系统所有的安全操作都是通过该机制采实现的。2016年三级信息安全技术考试试题及答案2016年三级信息安全技术考试试题及答案。D

A SSL B IARA C RA D 数字证书

6. 基于密码技术的访问控制是防止\_\_\_\_的主要防护手段。A

A 数据传输泄密 B 数据传输丢失 C 数据交换失败 D 数据备份失败

7. 避免对系统非法访问的主要方法是\_\_\_\_。C

A 加强管理 B 身份认证 C 访问控制 D 访问分配权限

8. 对保护数据来说，功能完善、使用灵活的\_\_\_\_必不可少。B

A 系统软件 B 备份软件 C 数据库软件 D 网络软件

9.信息安全PDR模型中，如果满足\_\_\_\_，说明系统是安全的。A

A Pt>Dt+Rt B Dt>Pt+Rt C Dt< font> D Pt< font>

10. 在一个信息安全保障体系中，最重要的核心组成部分为\_\_\_\_。B

A 技术体系 B 安全策略 C 管理体系 D 教育与培训

11. 《计算机信息系统安全保护条例》规定，计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的\_\_\_\_的安全。2016年三级信息安全技术考试试题及答案文章2016年三级信息安全技术考试试题及答案出自http://www.gkstk.com/article/wk-46339052596301.html，转载请保留此链接！。C

A 计算机 B 计算机软件系统 C 计算机信息系统 D 计算机操作人员

12. 《计算机信息系统安全保护条例》规定，国家对计算机信息系统安全专用产品的销售实行\_\_\_\_。A

A 许可证制度 B 3C认证 C IS09000认证 D 专卖制度

13. 《互联网上网服务营业场所管理条例》规定，互联网上网服务营业场所经营单位\_\_\_\_。C

A 可以接纳未成年人进入营业场所 B 可以在成年人陪同下，接纳未成年人进入营业场所

C 不得接纳未成年人进入营业场所 D 可以在白天接纳未成年人进入营业场所

14. \_\_\_\_是一种架构在公用通信基础设施上的专用数据通信网络，利用IPSec等网络层安全协议和建立在PKI的加密与签名技术来获得私有性。C

A SET B DDN C VPN D PKIX

15. 《计算机信息系统安全保护条例》规定，运输、携带、邮寄计算机信息媒体进出境的，应当如实向\_\_。B

A 国家安全机关申报 B 海关申报 C 国家质量检验监督局申报 D 公安机关申报

16. 《计算机信息系统安全保护条例》规定，故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以\_\_\_\_的罚款、对单位处以\_\_\_\_的罚款。A

A 5000元以下 15000元以下 B 5000元 15000元

C 2000元以下 10000元以下 D 2000元 10000元

17. 计算机犯罪，是指行为人通过\_\_\_\_所实施的危害\_\_\_\_安全以及其他严重危害社会的并应当处以刑罚的行为。2016年三级信息安全技术考试试题及答案计算机等级考试题库。A

A 计算机操作 计算机信息系统 B 数据库操作 计算机信息系统

C 计算机操作 应用信息系统 D 数据库操作 管理信息系统

18. 策略应该清晰，无须借助过多的特殊一通用需求文档描述，并且还要有具体的\_\_\_\_。C

A 管理支持 C 实施计划 D 补充内容 B 技术细节

19.系统备份与普通数据备份的不同在于，它不仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速\_\_\_\_。A

A 恢复整个系统B 恢复所有数据 C 恢复全部程序 D 恢复网络设置

20.在一个企业网中，防火墙应该是\_\_\_\_的一部分，构建防火墙时首先要考虑其保护的范围。D

A 安全技术 B 安全设置 C 局部安全策略 D 全局安全策略

有效管理TCP/IP网络 样题

单选题

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1:您的一台WINS服务器出现复制故障。您希望检查“计算机管理”控制台中的WINS统计资料。下列各项统计信息中，哪一项所显示的信息是关于WINS服务器在最后一次指定复制间隔到来时所启动的复制过程的？( 2 分)

A:最后一次周期复制。

B:最后一次手动复制。

C:最后一次网络复制更新。

D:以上都不对。

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2:已知目标计算机的IP地址却不知道其MAC地址时，应该通过哪个协议来解决？( 2 分)

A:IP

B:ARP

C:RARP

D:BOOTP

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3:以下哪种协议可以允许用户通过Internet进行相互通信？( 2 分)

A:NetBEUI

B:IPX/SPX

C:TCP/IP

D:AppleTalk

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4:TCP滑动窗口的功能是什么？( 2 分)

A:使得窗口尺寸更大，以便一次可以发送更多的数据，从而更加有效地利用带宽。

B:窗口的尺寸根据每个数据报进行滑动以接收数据，从而更有效地利用带宽。

C:在TCP会话过程中，允许动态协商窗口尺寸的大小，从而更加有效地利用带宽。

D:限制进入的数据，使得分段必须逐个发送，不是有效的带宽的利用方式。

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5:下列对于传输控制协议（TCP）和用户数据报协议（UDP）的陈述哪一个是正确的？( 2 分)

A:由于存在像数据包排序和数据包确认一样的高层处理，所以UDP速度较慢

B:由于发送的数据包不会被确认，而且丢失的数据包不会被要求重新发送，所以TCP是不可靠的

C:如果要求两台主机之间必须建立可靠、安全的通信连接，而且应当保证传输正确的话，通常使用TCP

D:如果不要求实时通信，但是却要求两台主机之间使用安全通路的话，通常使用UDP

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6:如果企业使用ADSL技术接入互联网，那么在请求拨号连接向导中应该选择：( 2 分)

A:使用调制解调器、ISDN适配器或其它设备接入

B:使用虚拟专用网络连接（VPN）

C:使用以太网上的PPP连接

D:以上均不正确

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7:下面有关DNS安装，正确的是：( 2 分)

A:可以安装在Windows2000 Professional上

B:DNS属于Windows2000的网络服务

C:安装好DNS后需要授权

D:DNS服务无法和WINS服务共存

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8:关于TCP/IP连接过程中的第二次握手中，描述最贴切的是：( 2 分)

A:源主机A发给目的的主机序号为1234567，那目的主机回复给源主机的确认序号为1234566。源主机收到目的主机的回复报文并记录下目的的主机序号

B:源主机A发给目的的主机序号为1234567，那目的主机回复给源主机的确认序号为1234568。源主机收到目的主机的回复报文并记录下目的的主机序号

C:源主机A发送给目的主机的序号为1234567，目的主机收到报文后记录该序号

D:源主机A发送给目的主机的序号为1234567，目的主机收到报文后开始建立通讯

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9:你是公司网管，网络中包括一个单独的IP子网，使用DHCP分配IP。你安装了WINS服务以减少名称解析中的广播交通。

过了一些天，用户报告网络太慢了。你调查发现广播没有减少。下一步应如何查看？( 2 分)

A:检查WINS服务器是否有客户机的注册记录

B:检查WINS服务器是否有其他WINS服务器的注册记录

C:检查WINS服务器服务是否开启

D:检查WINS服务器是否存在静态记录

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10:某部分DNS服务运行于一台支持动态更新的Unix服务器上。Windows 2000 Professional和Windows NT 4.0工作站的客户使用一台安装了Windows 2000成员服务器版的DHCP服务器以例获取TCP/IP配置。如果从DHCP客户上发送主机(A)记录和指针(PTR)记录的动态更新信息到DNS服务器，以下哪种方式最容易?( 2 分)

A:根据运行Unix的DNS服务器的IP地址配置每一台DHCP客户机

B:根据DHCP服务器的服务器选项(Server Options)配置运行Unix的DNS服务器的IP地址，并配置DHCP服务器的DNS属性发送来自所有DHCP客户的动态更新信息

C:什么也不用做。主机(A)记录和指针(PTR)记录将被自动更新

D:以上都不对。Unix的DNS服务器不接受Windows DHCP客户的动态更新

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11:下面哪一项没有正确描述TCP/IP协议族？( 2 分)

A:与OSI参考模型的上层进行严格的映射。

B:支持所有标准的物理层和数据链路层协议。

C:通过数据报序列传送信息。

D:在接收端将数据报重新组装成完整的信息。

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12:ICMP测试的目的是什么( 2 分)

A:确定消息是否能到达其目的地，如果不能，则确定可能的原因。

B:保证网络中的所有活动都是受检测的。

C:确定网络是否是根据模型建立的。

D:确定网络是处于控制模型还是用户模型。

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

13:使用哪种方法可以将客户机的IP地址由静态设置修改为动态设置？( 2 分)

A:ipconfig/release

B:ipconfig/renew

C:禁用后再启用网卡

D:修改网卡的TCP/IP属性

答案:D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

14:某台客户机手工静态设置了WINS服务器的地址，但同时在DHCP服务器中，又通过服务器选项、作用域选项和客户保留选项分别指定了不同WINS服务器的地址。在客户机进行名称解析时，会采用哪个配置的WINS服务器的地址？( 2 分)

A:手工静态设置的WINS服务器地址

B:服务器选项指定的WINS服务器地址

C:作用域选项指定的WINS服务器地址

D:客户保留选项指定的WINS服务器地址

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

15:在DNS区域中创建邮件交换记录时，需要设置优先级来指明邮件服务器的优先选择顺序。请问，哪个数字表示服务器具有最高的优先级？( 2 分)

A:10

B:9

C:1

D:0

答案:D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

16:当你使用cache服务器发现网络流量非常大，查看是DNS解析的交通，如何？( 2 分)

A:增大服务器中DNS记录的SOA记录

B:减小服务器中DNS记录的SOA记录

C:增大服务器中DNS记录的PTR记录

D:减小服务器中DNS记录的PTR记录

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

17:在OSI模型中表示层的功能由对应TCP/IP层次模型的哪一层完成：( 2 分)

A:应用层

B:传输层

C:网络层

D:物理层

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

18:某部门的网络上有若干Windows 2000和Windows NT 4.0服务器。域控制器、DNS服务器和DHCP服务器上个月已全部升级为Windows 2000。为了建立DHCP服务器的容错能力，重新启用了一台已不再使用但仍然在网上的旧的Windows NT 4.0服务器。为了测试DHCP功能，创建了若干虚设的作用域并激活了它们。相信在活动目录中对该DHCP服务器授权之前，它将不会有效。但是在第二天上午，就有大量用户抱怨说不能连接到网络。那么，原因是什么呢?( 2 分)

A:Windows 2000域控制器已自动为Windows NT 4.O DHCP服务器授权

B:Windows NT.4.0 DHCP服务器已自动在活动上当中为自己授权

C:Windows 2000 DHCP服务器已将Windows NT 4.0作为辅助DHCP服务器

D:Windows NT4.0 DHCP服务器不需在活动目录中授权即可开始工作

答案:D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

19:安装Windows 2000时，TCP/IP网络协议是默认安装的。按照OSI协议，有关该协

议的工作层，下面的哪项描述是正确的？( 2 分)

A:TCP在会话层进行工作，IP在传输层进行工作

B:TCP在传输层进行工作，IP在网络层进行工作

C:TCP在网络层进行工作，IP在传输层进行工作

D:TCP和IP都在传输层进行工作

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

20:以下有关DHCP授权，正确的是:( 2 分)

A:没有授权DHCP无法正常工作

B:只有存在AD的情况下才要求授权

C:只有域管理员可以授权

D:授权只是一个法律问题，与技术无关

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

21:您的一位同事按照下图对Windows 2000 WINS客户的TCP/IP属性做了配置： 当该客户试图连接网络上的其他计算机时，他可能面临着以下哪种故障（请选择所有正确选项）？( 2 分)

A:他将无法用主机名连接远程网段上的其他计算机。

B:他将无法用主机名连接本网段上的其他计算机。

C:他将无法在网络上运行任何NetBIOS应用程序。

D:以上都不对。

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

22:在下列给出的协议中，哪个不是TCP/IP的应用层协议？( 2 分)

A:HTTP

B:FTP

C:TCP

D:POP3

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

23:某企业申请了一个NIC已分配的C类网段 206.0.125.0，该企业有三个部门要接入网络，此时管理员欲划分三个可用的子网，每个子网最少有25个可用的节点，在下列的选项中不能正常使用的一组是：( 2 分)

A:有效IP范围：206.0.125.33－206.0.125.62广播地址：206.0.125.63

B:有效IP范围：206.0.125.65－206.0.125.94广播地址：206.0.125.95

C:有效IP范围：206.0.125.163－206.0.125.190广播地址：206.0.125.191

D:有效IP范围：206.0.125.129－206.0.125.158广播地址：206.0.125.159

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

24:你是公司网管，公司内包含3个子网。你希望你的DNS服务器允许客户使用主机名浏览同一子网内的Web服务器。所有的Web服务器的主机名相同，不管它在哪个子网里。你要做的工作是？( 2 分)

A:在主DNS上，创建三个A记录指向同一主机名的三个网段的Web服务器

B:在主DNS上，创建1个A记录指向同一主机名的本网段的Web服务器

C:在主DNS上，创建三个A记录指向不同主机名的三个网段的Web服务器

D:在主DNS上，创建1个A记录指向同一主机名的1个网段的Web服务器，另外两个使用CNAME名

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

25:DHCP服务器配置了多个地址作用域为多个网络段提供IP地址，同时需要为所有客户机配置DNS服务器选项。如果网络中公用一台DNS服务器，使用以下哪中选项配置最简单？( 2 分)

A:服务器选项

B:作用域选项

C:类选项

D:客户机保留选项

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

26:你是公司网管，网络中包括2台Win2k Server和50台windows2000 professional。 你使用DHCP动态分配IP。你配置DNS服务器自动更新DHCP客户端的正向和反向查找区域。你发现在反向查找区域PTR记录涉及15台客户机，而另外35台没有PTK记录。如何解决？( 3 分)

A:配置客户机使他们向DNS注册A记录

B:配置客户机是他们不在DNS服务器上注册域名

C:配置DHCP服务器更新那些不支持动态更新的客户机

D:配置DHCP服务器更新DNS，即使客户机没有提出请求

答案:D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

27:在企业网络的防火墙上拒绝所有发往外网接口的SYN包，那么，下列说法中正确的是：( 3 分)

A:网络内部将不可以聊OICQ

B:到外网的DNS解析将失效

C:不能让外网的任何主机主动建立连接

D:网络内部的访问将受到限制

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

28:你是Win2k网络网管，在单域中有三台Win2k域控制器。主DNS服务器安装在域控制器dc1.contoso.com上，从DNS服务安装在成员服务器srv1.contoso.com和srv2.contoso.com上。你希望提高DNS的容错性能并优化复制和区域传递的管理。你要做的工作是？( 3 分)

A:升级从DNS所在成员控制器为域控制器

B:将成员控制器加入主DNS服务器通知名单中

C:将DNS从成员控制器删除，在域控制器上安装DNS，将当前的zone转换为AD集成zone

D:设置在SOA记录中的TTL为最小值

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

29:你是网管，你配置Win2k服务器为网络中的DNS服务器。你创建了Staandard primary forward lookup zone（标准主ZONE）和reverse lookup zone（反向ZONE)。

你发现当使用nslookup命令时，你无法将IP地址解析为主机名。你还发现运行Tracert.exe,你得到如下错误信息：‘Unable to resolve target system name’如何做？( 3 分)

A:为正向查找创建A记录

B:为反向查找创建A记录

C:为正向查找创建PTR记录

D:为反向查找创建PTR记录

答案:D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

30:在查看路由信息时，“通讯协议”字段列显示为“本地”的路由条目表示的是何种含义？( 3 分)

A:手工添加的静态路由

B:通过路由协议学习到的路由

C:网络接口直连及默认的路由条目

D:路由表范例，无路由用途

答案:C

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

多选题

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

31:从网络上删除WINS服务器后，其拥有的记录通常继续分布于复制WINS环境的其他服务器上。在某些情况下WINS不会删除不在网络上活动的服务器拥有的项目，可能造成这种情况的原因有：( 2 分)

A:由非活动WINS服务器创建的静态映射将继续在网络上的其他活动的WINS服务器之间进行复制

B:WINS服务器会从其他活动的服务器上拉记录

C:在非活动WINS服务器上注册的动态映射不会立即从WINS数据库中删除

D:WINS服务的记录已经失效

答案:AC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

32:以下为Internet层协议是:( 2 分)

A:IP

B:ARP

C:ICMP

D:IGMP

答案:ABCD

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

33:某网络的一台Windows 2000成员服务器上已安装了DNS服务。在安装服务时，即创建了名为Testdomain.com的正向搜索区。下列哪些资源记录是自动在Testdomain.com区中创建的?( 2 分)

A:SOA

B:NS

C:MX

D:CNAME

答案:AB

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

34:IP路由表能够用来存储下列哪些类型的路由：( 2 分)

A:主机路由

B:网络路由

C:默认路由

D:除此之外的其它类型的路由

答案:ABC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

35:以下哪种情况下，WINS客户机会向WINS服务器发送名称释放请求？( 2 分)

A:WINS客户机网卡禁用时

B:WINS客户机关闭系统时

C:WINS客户机停止已注册的网络服务时

D:WINS客户机宕机时

答案:BC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

36:以下哪些为DNS的记录类型?( 3 分)

A:A记录

B:PTR记录

C:Netbios记录

D:SOA记录

答案:ABD

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

37:当一个用户无法使用网络中的DNS服务器解析外部域名时，管理员可以采取哪些办法来查找故障原因：( 3 分)

A:查看DNS服务器的类型是否为主DNS

B:查看DNS服务器能否与公网上的DNS通讯

C:使用路由跟踪命令查看到外部DNS的链路是否存在故障

D:使用nslookup命令查看DNS解析的结果

答案:BC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

38:在配置DNS和WINS集成查找功能时，需要在哪些计算机上进行相应的配置工作才能实现？( 3 分)

A:DNS服务器

B:WINS服务器

C:客户机

D:域控制器

答案:AC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

39:以下有关域名解析，正确的是：( 3 分)

A:可以分为正向查询和反向查询

B:可以分为反复查询和第归查询

C:可以分为区域查询和全面查询

D:可以分为即时查询和等待查询

答案:AB

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

40:如果WINS客户端A和非WINS客户端B位于不同的网段，为了使其可以相互解析名称并通讯，应使用哪些方法来解决这个问题：( 3 分)

A:利用静态映射

B:使用WINS代理

C:再建立一个独立的WINS服务器

D:修改WINS客户端的设置

答案:AB

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

判断题

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

41:静态的IP地址和DHCP服务器提供给DHCP客户端的永久租用的IP地址是一种方式。( 2 分)

A:正确

B:错误

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

42:出于对网络安全管理的考虑，在Windows 2000中安装了DHCP功能后可以直接使用。( 2 分)

A:正确

B:错误

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

43:使用动态IP地址时，网络中必须要有一台以上的DHCP服务器。( 2 分)

A:正确

B:错误

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

44:DHCP服务器不一定使用静态IP地址，也就是说DHCP服务器的IP地址是不固定的。( 2 分)

A:正确

B:错误

答案:B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

45:TCP/IP大致分为4个层次：应用层、传输层、互联网层和网络接口层。( 2 分)

A:正确

B:错误

答案:A

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

信息技术模拟考试题

1、计算机预防病毒感染有效的措施是( D )。

A.定期对计算机重新安装系统

B.不要把U盘和有病毒的U盘放在一起

C.不准往计算机中拷贝软件

D.给计算机安装防病毒的软件，并常更新

2、一个512MB的U盘能存储 B 字节(Byte)的数据量。

A.512×8

B.512×1024×1024

C.512×1024

D.512×1024×8

3、计算机病毒是 (B )。

A.计算机系统自生的

B.一种人为特制的计算机程序

C.主机发生故障时产生的

D.可传染疾病给人体

4、在计算机内部，数据是以 (A )形式加工、处理和传送的。

A.二进制码

B.八进制码

C.十进制码

D.十六进制码

5、下面列出的四种存储器中，断电后正在处理的信息会丢失的存储器是 (A) 。

A.RAM

B.ROM

C.PROM

D.EPROM

6、信息技术的四大基本技术是计算机技术、传感技术、控制技术和 (C) 。

A.生物技术

B.媒体技术

C.通信技术

D.传播技术

7、内存和外存相比，其主要特点是( C )。

A.能存储大量信息

B.能长期保存信息

C.存取速度快

D.能同时存储程序和数据

8、二十世纪末，人类开始进入 ( C )。

A. 电子时代

B. 农业时代

C. 信息时代

D. 工业时代

9、关于信息的说法，以下叙述中正确的是(D)。

A. 收音机就是一种信息

B. 一本书就是信息

C. 一张报纸就是信息

D. 报上登载的足球赛的消息是信息

10、下列不属于信息的是( C　 )。

A.报上登载的举办商品展销会的消息

B.电视中的计算机产品广告

C.计算机

D.各班各科成绩

11、多媒体信息不包括( 　D )。

A.影像、动画

B.文字、图形

C.音频、视频

D.硬盘、网卡

12、信息技术包括计算机技术、传感技术和(　C　 )。

A.编码技术

B.电子技术

C.通信技术

D.显示技术

13、使用大规模和超大规模集成电路作为计算机元件的计算机是( D　 )。

A.第一代计算机

B.第二代计算机

C.第三代计算机

D.第四代计算机

14、计算机系统由哪几部分组成( 　B )。

A.主机和外部设备

B.软件系统和硬件系统

C.主机和软件系统

D.操作系统和硬件系统

15、计算机的软件系统包括( 　B )。

A.程序和数据

B.系统软件与应用软件

C.操作系统与语言处理程序

D.程序、数据与文档

16、微型计算机中，I/O设备的含义是( 　C )。

A .输入设备

B.输出设备

C.输入输出设备

D.控制设备

17、在以下所列设备中,属于计算机输入设备的是( A　 )。

A.键盘

B.打印机

C.显示器

D.绘图仪

18、下列软件属于系统软件的是( 　D ) 。

A.PowerPoint

B.Word2007

C.Excel 2007

D.Windows 2007

19、某单位的人事档案管理程序属于( B　 )。

A.图形处理软件

B.应用软件

C.系统软件

D.字处理软件

20、以下哪一组软件都是应用软件( 　C )。

A.DOS、WINDOWS、WORD、EXCEL、VFP

B.WORD、EXCEL、UNIX、游戏、杀毒软件

C.游戏、POWERPOINT、WORD、EXCEL

D.WORD、DOS、EXCEL、声音编辑软件

1. 信息安全策略的制定和维护中，最重要是要保证其\_\_\_\_和相对稳定性。A

A 明确性 B 细致性 C 标准性 D 开放性

2. \_\_\_\_是企业信息安全的核心。C

A 安全教育 B 安全措施 C 安全管理 D 安全设施

3.编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码是\_\_\_\_。A

A 计算机病毒 B 计算机系统 C 计算机游戏 D 计算机程序

4.许多与PKI相关的协议标准(如PKIX、S/MIME、SSL、TLS、IPSec)等都是在\_\_\_\_基础上发展起来的。B

A X.500 B X.509 C X.519 D X.505

5. \_\_\_\_是PKI体系中最基本的元素，PKI系统所有的安全操作都是通过该机制采实现的。2016年三级信息安全技术考试试题及答案2016年三级信息安全技术考试试题及答案。D

A SSL B IARA C RA D 数字证书

6. 基于密码技术的访问控制是防止\_\_\_\_的主要防护手段。A

A 数据传输泄密 B 数据传输丢失 C 数据交换失败 D 数据备份失败

7. 避免对系统非法访问的主要方法是\_\_\_\_。C

A 加强管理 B 身份认证 C 访问控制 D 访问分配权限

8. 对保护数据来说，功能完善、使用灵活的\_\_\_\_必不可少。B

A 系统软件 B 备份软件 C 数据库软件 D 网络软件

9.信息安全PDR模型中，如果满足\_\_\_\_，说明系统是安全的。A

A Pt>Dt+Rt B Dt>Pt+Rt C Dt< font> D Pt< font>

10. 在一个信息安全保障体系中，最重要的核心组成部分为\_\_\_\_。B

A 技术体系 B 安全策略 C 管理体系 D 教育与培训

11. 《计算机信息系统安全保护条例》规定，计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的\_\_\_\_的安全。2016年三级信息安全技术考试试题及答案文章2016年三级信息安全技术考试试题及答案出自http://www.gkstk.com/article/wk-46339052596301.html，转载请保留此链接！。C

A 计算机 B 计算机软件系统 C 计算机信息系统 D 计算机操作人员

12. 《计算机信息系统安全保护条例》规定，国家对计算机信息系统安全专用产品的销售实行\_\_\_\_。A

A 许可证制度 B 3C认证 C IS09000认证 D 专卖制度

13. 《互联网上网服务营业场所管理条例》规定，互联网上网服务营业场所经营单位\_\_\_\_。C

A 可以接纳未成年人进入营业场所 B 可以在成年人陪同下，接纳未成年人进入营业场所

C 不得接纳未成年人进入营业场所 D 可以在白天接纳未成年人进入营业场所

14. \_\_\_\_是一种架构在公用通信基础设施上的专用数据通信网络，利用IPSec等网络层安全协议和建立在PKI的加密与签名技术来获得私有性。C

A SET B DDN C VPN D PKIX

15. 《计算机信息系统安全保护条例》规定，运输、携带、邮寄计算机信息媒体进出境的，应当如实向\_\_。B

A 国家安全机关申报 B 海关申报 C 国家质量检验监督局申报 D 公安机关申报

16. 《计算机信息系统安全保护条例》规定，故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以\_\_\_\_的罚款、对单位处以\_\_\_\_的罚款。A

A 5000元以下 15000元以下 B 5000元 15000元

C 2000元以下 10000元以下 D 2000元 10000元

17. 计算机犯罪，是指行为人通过\_\_\_\_所实施的危害\_\_\_\_安全以及其他严重危害社会的并应当处以刑罚的行为。2016年三级信息安全技术考试试题及答案计算机等级考试题库。A

A 计算机操作 计算机信息系统 B 数据库操作 计算机信息系统

C 计算机操作 应用信息系统 D 数据库操作 管理信息系统

18. 策略应该清晰，无须借助过多的特殊一通用需求文档描述，并且还要有具体的\_\_\_\_。C

A 管理支持 C 实施计划 D 补充内容 B 技术细节

19.系统备份与普通数据备份的不同在于，它不仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速\_\_\_\_。A

A 恢复整个系统B 恢复所有数据 C 恢复全部程序 D 恢复网络设置

20.在一个企业网中，防火墙应该是\_\_\_\_的一部分，构建防火墙时首先要考虑其保护的范围。D

A 安全技术 B 安全设置 C 局部安全策略 D 全局安全策略

一、单项选择题

1. 非法接收者在截获密文后试图从中分析出明文的过程称为（ A ）

A. 破译 B. 解密 C. 加密 D. 攻击

2. 以下有关软件加密和硬件加密的比较，不正确的是（ B ）

A. 硬件加密对用户是透明的，而软件加密需要在操作系统或软件中写入加密程序

B. 硬件加密的兼容性比软件加密好

C. 硬件加密的安全性比软件加密好

D. 硬件加密的速度比软件加密快

3. 下面有关3DES的数学描述，正确的是（ B ）

A. C=E(E(E(P, K1), K1), K1) B. C=E(D(E(P, K1), K2), K1)

C. C=E(D(E(P, K1), K1), K1) D. C=D(E(D(P, K1), K2), K1)

4. PKI无法实现（ D ）

A. 身份认证 B. 数据的完整性 C. 数据的机密性 D. 权限分配

5. CA的主要功能为（ D ）

A. 确认用户的身份

B. 为用户提供证书的申请、下载、查询、注销和恢复等操作

C. 定义了密码系统的使用方法和原则

D. 负责发放和管理数字证书

6. 数字证书不包含（ B ）

A. 颁发机构的名称 B. 证书持有者的私有密钥信息

C. 证书的有效期 D. CA签发证书时所使用的签名算法

7. “在因特网上没有人知道对方是一个人还是一条狗”这个故事最能说明（ A ）

A. 身份认证的重要性和迫切性 B. 网络上所有的活动都是不可见的

C. 网络应用中存在不严肃性 D. 计算机网络是一个虚拟的世界

8. 以下认证方式中，最为安全的是（ D ）

A. 用户名+密码 B. 卡+密钥 C. 用户名+密码+验证码 D. 卡+指纹

9. 将通过在别人丢弃的废旧硬盘、U盘等介质中获取他人有用信息的行为称为（ D ）

A. 社会工程学 B. 搭线窃听 C. 窥探 D. 垃圾搜索

10. ARP欺骗的实质是（ A ）

A. 提供虚拟的MAC与IP地址的组合 B. 让其他计算机知道自己的存在

C. 窃取用户在网络中传输的数据 D. 扰乱网络的正常运行

11. TCP SYN泛洪攻击的原理是利用了（ A ）

A. TCP三次握手过程 B. TCP面向流的工作机制

C. TCP数据传输中的窗口技术 D. TCP连接终止时的FIN报文

12. DNSSEC中并未采用（ C ）

A. 数字签名技术 B. 公钥加密技术 C. 地址绑定技术 D. 报文摘要技术

13. 当计算机上发现病毒时，最彻底的清除方法为（ A ）

A. 格式化硬盘 B. 用防病毒软件清除病毒

C. 删除感染病毒的文件 D. 删除磁盘上所有的文件

14. 木马与病毒的最大区别是（ B ）

A. 木马不破坏文件，而病毒会破坏文件

B. 木马无法自我复制，而病毒能够自我复制

C. 木马无法使数据丢失，而病毒会使数据丢失

D. 木马不具有潜伏性，而病毒具有潜伏性

15. 经常与黑客软件配合使用的是（ C ）

A. 病毒 B. 蠕虫 C. 木马 D. 间谍软件

16. 目前使用的防杀病毒软件的作用是（ C ）

A. 检查计算机是否感染病毒，并消除已感染的任何病毒

B. 杜绝病毒对计算机的侵害

C. 检查计算机是否感染病毒，并清除部分已感染的病毒

D. 查出已感染的任何病毒，清除部分已感染的病毒

17. 死亡之ping属于（ B ）

A. 冒充攻击 B. 拒绝服务攻击 C. 重放攻击 D. 篡改攻击

18. 泪滴使用了IP数据报中的（ A ）

A. 段位移字段的功能 B. 协议字段的功能

C. 标识字段的功能 D. 生存期字段的功能

19. ICMP泛洪利用了（ C ）

A. ARP命令的功能 B. tracert命令的功能

C. ping命令的功能 D. route命令的功能

20. 将利用虚假IP地址进行ICMP报文传输的攻击方法称为（ D ）

A. ICMP泛洪 B. LAND攻击 C. 死亡之ping D. Smurf攻击

21. 以下哪一种方法无法防范口令攻击（A ）

A. 启用防火墙功能 B. 设置复杂的系统认证口令

C. 关闭不需要的网络服务 D. 修改系统默认的认证名称

22． 以下设备和系统中，不可能集成防火墙功能的是（ A ）

A.集线器 B. 交换机 C. 路由器 D. Windows Server 2003操作系统

23. 对“防火墙本身是免疫的”这句话的正确理解是（ B ）

A. 防火墙本身是不会死机的

B. 防火墙本身具有抗攻击能力

C. 防火墙本身具有对计算机病毒的免疫力

D. 防火墙本身具有清除计算机病毒的能力

24. 以下关于传统防火墙的描述，不正确的是（ A ）

A. 即可防内，也可防外

B. 存在结构限制，无法适应当前有线网络和无线网络并存的需要

C. 工作效率较低，如果硬件配置较低或参数配置不当，防火墙将成形成网络瓶颈

D. 容易出现单点故障

25. 下面对于个人防火墙的描述，不正确的是（ C ）

A. 个人防火墙是为防护接入互联网的单机操作系统而出现的

B. 个人防火墙的功能与企业级防火墙类似，而配置和管理相对简单

C. 所有的单机杀病毒软件都具有个人防火墙的功能

D. 为了满足非专业用户的使用，个人防火墙的配置方法相对简单

26.VPN的应用特点主要表现在两个方面，分别是（ A ）

A. 应用成本低廉和使用安全 B. 便于实现和管理方便

C. 资源丰富和使用便捷 D. 高速和安全

27. 如果要实现用户在家中随时访问单位内部的数字资源，可以通过以下哪一种方式实现（ C ）

A. 外联网VPN B. 内联网VPN C. 远程接入VPN D. 专线接入

28. 在以下隧道协议中，属于三层隧道协议的是（ D ）

A. L2F B. PPTP C. L2TP D. IPSec

29.以下哪一种方法中，无法防范蠕虫的入侵。（ B ）

A. 及时安装操作系统和应用软件补丁程序

B. 将可疑邮件的附件下载等文件夹中，然后再双击打开

C. 设置文件夹选项，显示文件名的扩展名

D. 不要打开扩展名为VBS、SHS、PIF等邮件附件

30. 以下哪一种现象，一般不可能是中木马后引起的（ B ）

A. 计算机的反应速度下降，计算机自动被关机或是重启

B. 计算机启动时速度变慢，硬盘不断发出“咯吱，咯吱”的声音

C. 在没有操作计算机时，而硬盘灯却闪个不停

D. 在浏览网页时网页会自动关闭，软驱或光驱会在无盘的情况下读个不停

31.下面有关DES的描述，不正确的是 （A）

A. 是由IBM、Sun等公司共同提出的 B. 其结构完全遵循Feistel密码结构

C. 其算法是完全公开的 D. 是目前应用最为广泛的一种分组密码算法

32． “信息安全”中的“信息”是指 （C）

A、以电子形式存在的数据 B、计算机网络

C、信息本身、信息处理过程、信息处理设施和信息处理都

D、软硬件平台

33. 下面不属于身份认证方法的是（ C）

A. 口令认证 B. 智能卡认证 C. 姓名认证 D. 指纹认证

34. 数字证书不包含 （ B）

A. 颁发机构的名称 B. 证书持有者的私有密钥信息

C. 证书的有效期 D. CA签发证书时所使用的签名算法

35. 套接字层（Socket Layer）位于（B ）

A. 网络层与传输层之间 B. 传输层与应用层之间

C. 应用层 D. 传输层

36. 下面有关SSL的描述，不正确的是（ D）

A. 目前大部分Web浏览器都内置了SSL协议

B. SSL协议分为SSL握手协议和SSL记录协议两部分

C. SSL协议中的数据压缩功能是可选的

D. TLS在功能和结构上与SSL完全相同

37. 在基于IEEE 802.1x与Radius组成的认证系统中，Radius服务器的功能不包括（ D ）

A. 验证用户身份的合法性 B. 授权用户访问网络资源

C. 对用户进行审计 D. 对客户端的MAC地址进行绑定

38. 在生物特征认证中，不适宜于作为认证特征的是（ D ）

A. 指纹 B. 虹膜 C. 脸像 D. 体重

39. 防止重放攻击最有效的方法是（ B ）

A. 对用户账户和密码进行加密 B. 使用“一次一密”加密方式

C. 经常修改用户账户名称和密码 D. 使用复杂的账户名称和密码

40. 计算机病毒的危害性表现在（ B ）

A. 能造成计算机部分配置永久性失效 B. 影响程序的执行或破坏用户数据与程序

C. 不影响计算机的运行速度 D. 不影响计算机的运算结果

41. 下面有关计算机病毒的说法，描述正确的是（ C ）

A. 计算机病毒是一个MIS程序

B. 计算机病毒是对人体有害的传染性疾病

C. 计算机病毒是一个能够通过自身传染，起破坏作用的计算机程序

D. 计算机病毒是一段程序，只会影响计算机系统，但不会影响计算机网络

42 计算机病毒具有（ A ）

A. 传播性、潜伏性、破坏性 B. 传播性、破坏性、易读性

C. 潜伏性、破坏性、易读性 D. 传播性、潜伏性、安全性

43. 目前使用的防杀病毒软件的作用是（C ）

A. 检查计算机是否感染病毒，并消除已感染的任何病毒

B. 杜绝病毒对计算机的侵害

C. 检查计算机是否感染病毒，并清除部分已感染的病毒

D. 查出已感染的任何病毒，清除部分已感染的病毒

44 在DDoS攻击中，通过非法入侵并被控制，但并不向被攻击者直接发起攻击的计算机称为（ B）

A. 攻击者 B. 主控端 C. 代理服务器 D. 被攻击者

45. 对利用软件缺陷进行的网络攻击，最有效的防范方法是（ A ）

A. 及时更新补丁程序 B. 安装防病毒软件并及时更新病毒库

C. 安装防火墙 D. 安装漏洞扫描软件

46. 在IDS中，将收集到的信息与数据库中已有的记录进行比较，从而发现违背安全策略的行为，这类操作方法称为（ A ）

A. 模式匹配 B. 统计分析 C. 完整性分析 D. 不确定

47. IPS能够实时检查和阻止入侵的原理在于IPS拥有众多的（ C ）

A. 主机传感器 B. 网络传感器 C. 过滤器 D. 管理控制台

48. 将利用虚假IP地址进行ICMP报文传输的攻击方法称为（ D ）

A. ICMP泛洪 B. LAND攻击 C. 死亡之ping D. Smurf攻击

49. 以下哪一种方法无法防范口令攻击（ A ）

A. 启用防火墙功能 B. 设置复杂的系统认证口令

C. 关闭不需要的网络服务 D. 修改系统默认的认证名称

50. 在分布式防火墙系统组成中不包括（ D ）

A. 网络防火墙 B. 主机防火墙 C. 中心管理服务器 D. 传统防火墙

51 下面对于个人防火墙未来的发展方向，描述不准确的是（ D ）

A. 与xDSL Modem、无线AP等网络设备集成

B. 与防病毒软件集成，并实现与防病毒软件之间的安全联动

C. 将个人防火墙作为企业防火墙的有机组成部分

D. 与集线器等物理层设备集成

52. 在以下各项功能中，不可能集成在防火墙上的是（ D ）

A. 网络地址转换（NAT） B. 虚拟专用网（VPN）

C. 入侵检测和入侵防御 D. 过滤内部网络中设备的MAC地址

53. 当某一服务器需要同时为内网用户和外网用户提供安全可靠的服务时，该服务器一般要置于防火墙的（ C ）

A. 内部 B. 外部 C. DMZ区 D. 都可以

54. 以下关于状态检测防火墙的描述，不正确的是（ D ）

A. 所检查的数据包称为状态包，多个数据包之间存在一些关联

B. 能够自动打开和关闭防火墙上的通信端口

C. 其状态检测表由规则表和连接状态表两部分组成

D. 在每一次操作中，必须首先检测规则表，然后再检测连接状态表

55. 在以下的认证方式中，最不安全的是（ A ）

A. PAP B. CHAP C. MS-CHAP D. SPAP

56. 以下有关VPN的描述，不正确的是（ C）

A. 使用费用低廉 B. 为数据传输提供了机密性和完整性

C. 未改变原有网络的安全边界 D. 易于扩展

57. 目前计算机网络中广泛使用的加密方式为（ C ）

A. 链路加密 B. 节点对节点加密 C. 端对端加密 D. 以上都是

58. 以下有关软件加密和硬件加密的比较，不正确的是（ B ）

A. 硬件加密对用户是透明的，而软件加密需要在操作系统或软件中写入加密程序

B. 硬件加密的兼容性比软件加密好

C. 硬件加密的安全性比软件加密好

D. 硬件加密的速度比软件加密快

59 对于一个组织，保障其信息安全并不能为其带来直接的经济效益，相反还会付出较大的成本，那么组织为什么需要信息安全？ （ D ）

A. 有多余的经费 B. 全社会都在重视信息安全，我们也应该关注

C. 上级或领导的要求 D. 组织自身业务需要和法律法规要求

二、填空题

1. 根据密码算法对明文处理方式的标准不同，可以将密码系统分为 序列密码 和分组密码。

2. PKI的技术基础包括 公开密钥体制 和 加密机制 两部分。

3. 零知识身份认证分为 交互式和 非交互式两种类型。

4 DNS同时调用了TCP和UDP的53端口，其中 udp53 端口用于DNS客户端与DNS服务器端的通信，而 TCP53端口用于DNS区域之间的数据复制。

5. 与病毒相比，蠕虫的最大特点是消耗 计算机内存和 网络带宽。

6. 在网络入侵中，将自己伪装成合法用户来攻击系统的行为称为冒充；复制合法用户发出的数据，然后进行重发，以欺骗接收者的行为称为 重放；中止或干扰服务器为合法用户提供服务的行为称为 服务拒绝。

7. 在LAND攻击中，LAND攻击报文的 源IP地址和 目的IP地址是相同的。

8. 防火墙将网络分割为两部分，即将网络分成两个不同的安全域。对于接入Internet的局域网，其中 局域网属于可信赖的安全域，而 Internet属于不可信赖的非安全域。

9. 防火墙一般分为路由模式和透明模式两类。当用防火墙连接同一网段的不同设备时，可采用 透明模式防火墙；而用防火墙连接两个完全不同的网络时，则需要使用

路由模式防火墙。

10 VPN系统中的身份认证技术包括 用户身份认证和 信息认证两种类型。

11用公钥加密数据，然后用私钥解密数据的过程称为 加密 ；利用私钥加密数据，然后用公钥解密数据的过程称为 数字签名 。

12 在PKI/PMI系统中，一个合法用户只拥有一个唯一的 公钥证书 ，但可能会同时拥有多个不同的 属性证书 。

13 计算机网络安全领域的3A是指认证、 授权 和 审计 。

14 SSL是一种综合利用 对称加密 和 非对称加密 技术进行安全通信的工业标准。

15 扫描技术主要分为 主机扫描安全和 网络安全扫描 两种类型。

16. 在IDS的报警中，可以分为错误报警和正确的报警两种类型。其中错误报警中，将IDS工作于正常状态下产生的报警称为 误报 ；而将IDS对已知的入侵活动未产生报警的现象称为 漏报 。

17. 状态检测防火墙是在传统包过滤防火墙的基础上发展而来的，所以将传统的包过滤防火墙称为 静态包过滤 防火墙，而将状态检测防火墙称为 动态包过滤 防火墙。

18. VPN是利用Internet等 公共网络 的基础设施，通过 隧道 技术，为用户提供一条与专网相同的安全通道。公共网络 隧道

19. VPN系统中的三种典型技术分别是 隧道技术、 身份认证技术 、 和加密技术。

20. 目前身份认证技术可分为PKI和非PKI两种类型，其中在VPN的用户身份认证中一般采用 非PKI 认证方式，而信息认证中采用 PKI 认证方式。

三、判断题

1． 链路加密方式适用于在广域网系统中应用。（ N ）

2. “一次一密”属于序列密码中的一种。（ Y ）

3. 当通过浏览器以在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（ Y ）

4. PKI和PMI在应用中必须进行绑定，而不能在物理上分开。（ N ）

5.在网络身份认证中采用审计的目的是对所有用户的行为进行记录，以便于进行核查。（ Y）

6. 由于在TCP协议的传输过程中，传输层需要将从应用层接收到的数据以字节为组成单元划分成多个字节段，然后每个字节段单独进行路由传输，所以TCP是面向字节流的可靠的传输方式。（Y ）

7. ARP缓存只能保存主动查询获得的IP和MAC的对应关系，而不会保存以广播形式接收到的IP和MAC的对应关系。（ N ）

8.计算机病毒只会破坏计算机的操作系统，而对其他网络设备不起作用。（ N ）

9. 脚本文件和ActiveX控件都可以嵌入在HTML文件中执行。（Y ）

10. 要实现DDoS攻击，攻击者必须能够控制大量的计算机为其服务。（ Y ）

11．Feistel是密码设计的一个结构，而非一个具体的密码产品。（ Y ）

12. 暴力破解与字典攻击属于同类网络攻击方式，其中暴力破解中所采用的字典要比字典攻击中使用的字典的范围要大。（ Y ）

13. DHCP服务器只能给客户端提供IP地址和网关地址，而不能提供DNS服务器的IP地址。（ N ）

14. 间谍软件能够修改计算机上的配置文件。（ N ）

15. 蠕虫既可以在互联网上传播，也可以在局域网上传播。而且由于局域网本身的特性，蠕虫在局域网上传播速度更快，危害更大。（ Y ）

16. 与IDS相比，IPS具有深层防御的功能。（ Y ）

17. 当硬件配置相同时，代理防火墙对网络运行性能的影响要比包过滤防火墙小。（N）

18. 在传统的包过滤、代理和状态检测3类防火墙中，只有状态检测防火墙可以在一定程度上检测并防止内部用户的恶意破坏。（ Y ）

19. 防火墙一般采用“所有未被允许的就是禁止的”和“所有未被禁止的就是允许的”两个基本准则，其中前者的安全性要比后者高。（ Y ）

20. 在利用VPN连接两个LAN时，LAN中必须使用TCP/IP协议。（ N ）

四、名词解释

1、DNS缓存中毒

答：DNS为了提高查询效率，采用了缓存机制，把用户查询过的最新记录存放在缓存中，并设置生存周期（Time To Live，TTL）。在记录没有超过TTL之前，DNS缓存中的记录一旦被客户端查询，DNS服务器（包括各级名字服务器）将把缓存区中的记录直接返回给客户端，而不需要进行逐级查询，提高了查询速率。DNS缓存中毒利用了DNS缓存机制，在DNS服务器的缓存中存入大量错误的数据记录主动供用户查询。由于缓存中大量错误的记录是攻击者伪造的，而伪造者可能会根据不同的意图伪造不同的记录。由于DNS服务器之间会进行记录的同步复制，所以在TTL内，缓存中毒的DNS服务器有可能将错误的记录发送给其他的DNS服务器，导致更多的DNS服务器中毒。

2．机密性、完整性、可用性、可控性

答：机密性是确保信息不暴露给未经授权的人或应用进程；完整性是指只有得到允许的人或应用进程才能修改数据，并且能够判别出数据是否已被更改；可用性是指只有得到授权的用户在需要时才可以访问数据，即使在网络被攻击时也不能阻碍授权用户对网络的使用；可控性是指能够对授权范围内的信息流向和行为方式进行控制

3．PMI

答：PMI（授权管理基础设施）是在PKI发展的过程中为了将用户权限的管理与其公钥的管理分离，由IETF提出的一种标准。PMI的最终目标就是提供一种有效的体系结构来管理用户的属性。PMI以资源管理为核心，对资源的访问控制权统一交由授权机构统一处理。同PKI相比，两者主要区别在于PKI证明用户是谁，而PMI证明这个用户有什么权限、能干什么。PMI需要PKI为其提供身份认证。PMI实际提出了一个新的信息保护基础设施，能够与PKI紧密地集成，并系统地建立起对认可用户的特定授权，对权限管理进行系统的定义和描述，完整地提供授权服务所需过程。

4．防火墙

答：防火墙是指设置在不同网络（如可信赖的企业内部局域网和不可信赖的公共网络）之间或网络安全域之间的一系列部件的组合，通过监测、限制、更改进入不同网络或不同安全域的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以防止发生不可预测的、潜在破坏性的入侵，实现网络的安全保护。

5．VPN

答：VPN（虚拟专用网）是利用Internet等公共网络的基础设施，通过隧道技术，为用户提供一条与专用网络具有相同通信功能的安全数据通道，实现不同网络之间以及用户与网络之间的相互连接。从VPN的定义来看，其中“虚拟”是指用户不需要建立自己专用的物理线路，而是利用Internet等公共网络资源和设备建立一条逻辑上的专用数据通道，并实现与专用数据通道相同的通信功能；“专用网络”是指这一虚拟出来的网络并不是任何连接在公共网络上的用户都能够使用的，而是只有经过授权的用户才可以使用。同时，该通道内传输的数据经过了加密和认证，从而保证了传输内容的完整性和机密性。

6．对称加密与非对称加密

答：在一个加密系统中，加密和解密使用同一个密钥，这种加密方式称为对称加密，也称为单密钥加密（2分）。如果系统采用的是双密钥体系，存在两个相互关联的密码，其中一个用于加密，另一个用于解密，这种加密方法称为非对称加密，也称为公钥加密。（2分）

7． PKI

答：PKI（公钥基础设施）是利用密码学中的公钥概念和加密技术为网上通信提供的符合标准的一整套安全基础平台。PKI能为各种不同安全需求的用户提供各种不同的网上安全服务所需要的密钥和证书，这些安全服务主要包括身份识别与鉴别（认证）、数据保密性、数据完整性、不可否认性及时间戳服务等，从而达到保证网上传递信息的安全、真实、完整和不可抵赖的目的（2分）。PKI的技术基础之一是公开密钥体制（1分）；PKI的技术基础之二是加密机制（1分）

8． DNSSEC

答：DNSSEC（域名系统安全扩展）是在原有的域名系统（DNS）上通过公钥技术，对DNS中的信息进行数字签名，从而提供DNS的安全认证和信息完整性检验（2分）。发送方首先使用Hash函数对要发送的DNS信息进行计算，得到固定长度的“信息摘要”，然后对“信息摘要”用私钥进行加密，此过程实现了对“信息摘要”的数字签名；最后将要发送的DNS信息、该DNS信息的“信息摘要”以及该“信息摘要”的数字签名，一起发送出来（1分）。接收方首先采用公钥系统中的对应公钥对接收到的“信息摘要”的数字签名进行解密，得到解密后的“信息摘要”；接着用与发送方相同的Hash函数对接收到的DNS信息进行运算，得到运算后的“信息摘要”；最后，对解密后的 “信息摘要”和运算后的“信息摘要”进行比较，如果两者的值相同，就可以确认接收到的DNS信息是完整的，即是由正确的DNS服务器得到的响应

9． DoS攻击

答：DoS（拒绝服务）攻击是一种实现简单但又很有效的攻击方式。DoS攻击的目的就是让被攻击主机拒绝用户的正常服务访问，破坏系统的正常运行，最终使用户的部分Internet连接和网络系统失效（2分）。最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。（2分）

10．蜜罐

答：是一种计算机网络中专门为吸引并“诱骗”哪些试图入侵他人计算机系统的人而设计的陷阱系统，设置蜜罐的目的主要是用于被侦听,被攻击，从而研究网络安全的相关技术和方法。

11．DDoS攻击

答：分布式拒绝服务（Distributed Denial of Service，DDoS）攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。

五、简答题

1．简述ARP欺骗的实现原理及主要防范方法

答：由于ARP协议在设计中存在的主动发送ARP报文的漏洞，使得主机可以发送虚假的ARP请求报文或响应报文，报文中的源IP地址和源MAC地址均可以进行伪造（2分）。在局域网中，即可以伪造成某一台主机（如服务器）的IP地址和MAC地址的组合，也可以伪造成网关的IP地址和MAC地址的组合，ARP即可以针对主机，也可以针对交换机等网络设备（2分），等等。

目前，绝大部分ARP欺骗是为了扰乱局域网中合法主机中保存的ARP表，使得网络中的合法主机无法正常通信或通信不正常，如表示为计算机无法上网或上网时断时续等。（2分）

针对主机的ARP欺骗的解决方法：主机中静态ARP缓存表中的记录是永久性的，用户可以使用TCP/IP工具来创建和修改，如Windows操作系统自带的ARP工具，利用“arp -s 网关IP地址 网关MAC地址”将本机中ARP缓存表中网关的记录类型设置为静态（static）。（2分）

针对交换机的ARP欺骗的解决方法：在交换机上防范ARP欺骗的方法与在计算机上防范ARP欺骗的方法基本相同，还是使用将下连设备的MAC地址与交换机端口进行一一绑定的方法来实现。

2． 如下图所示，简述包过滤防火墙的工作原理及应用特点。

答：包过滤（Packet Filter）是在网络层中根据事先设置的安全访问策略（过滤规则），检查每一个数据包的源IP地址、目的IP地址以及IP分组头部的其他各种标志信息（如协议、服务类型等），确定是否允许该数据包通过防火墙（2分）。

包过滤防火墙中的安全访问策略（过滤规则）是网络管理员事先设置好的，主要通过对进入防火墙的数据包的源IP地址、目的IP地址、协议及端口进行设置，决定是否允许数据包通过防火墙。（2分）

如图所示，当网络管理员在防火墙上设置了过滤规则后，在防火墙中会形成一个过滤规则表。当数据包进入防火墙时，防火墙会将IP分组的头部信息与过滤规则表进行逐条比对，根据比对结果决定是否允许数据包通过。（2分）

包过滤防火墙主要特点：过滤规则表需要事先进行人工设置，规则表中的条目根据用户的安全要求来定；防火墙在进行检查时，首先从过滤规则表中的第1个条目开始逐条进行，所以过滤规则表中条目的先后顺序非常重要；由于包过滤防火墙工作在OSI参考模型的网络层和传输层，所以包过滤防火墙对通过的数据包的速度影响不大，实现成本较低。但包过滤防火墙无法识别基于应用层的恶意入侵。另外，包过滤防火墙不能识别IP地址的欺骗，内部非授权的用户可以通过伪装成为合法IP地址的使用者来访问外部网络，同样外部被限制的主机也可以通过使用合法的IP地址来欺骗防火墙进入内部网络。（4分）

3． 根据实际应用，以个人防火墙为主，简述防火墙的主要功能及应用特点

答：防火墙是指设置在不同网络（如可信赖的企业内部局域网和不可信赖的公共网络）之间或网络安全域之间的一系列部件的组合，通过监测、限制、更改进入不同网络或不同安全域的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以防止发生不可预测的、潜在破坏性的入侵，实现网络的安全保护。

个人防火墙是一套安装在个人计算机上的软件系统，它能够监视计算机的通信状况，一旦发现有对计算机产生危险的通信就会报警通知管理员或立即中断网络连接，以此实现对个人计算机上重要数据的安全保护。

个人防火墙是在企业防火墙的基础上发展起来，个人防火墙采用的技术也与企业防火墙基本相同，但在规则的设置、防火墙的管理等方面进行了简化，使非专业的普通用户能够容易地安装和使用。

为了防止安全威胁对个人计算机产生的破坏，个人防火墙产品应提供以下的主要功能。防止Internet上用户的攻击、阻断木马及其他恶意软件的攻击、为移动计算机提供安全保护、与其他安全产品进行集成。

4．简述L2TP协议操作过程

6． 如图所示，描述DDoS攻击的实现方法。

答：DDoS攻击是利用一批受控制的主机向一台主机发起攻击，其攻击的强度和造成的威胁要比DoS攻击严重得多，当然其破坏性也要强得多。（2分）

在整个DDoS攻击过程中，共有四部分组成：攻击者、主控端、代理服务器和被攻击者，其中每一个组成在攻击中扮演的角色不同。

（1） 攻击者。攻击者是指在整个DDoS攻击中的主控台，它负责向主控端发送攻击命令。与DoS攻击略有不同，DDoS攻击中的攻击者对计算机的配置和网络带宽的要求并不高，只要能够向主控端正常发送攻击命令即可。（2分）

（2） 主控端。主控端是攻击者非法侵入并控制的一些主机，通过这些主机再分别控制大量的代理服务器。攻击者首先需要入侵主控端，在获得对主控端的写入权限后，在主控端主机上安装特定的程序，该程序能够接受攻击者发来的特殊指令，并且可以把这些命令发送到代理服务器上。 （2分）

（3） 代理服务器。代理服务器同样也是攻击者侵入并控制的一批主机，同时攻击者也需要在入侵这些主机并获得对这些主机的写入权限后，在上面安装并运行攻击器程序，接受和运行主控端发来的命令。代理服务器是攻击的直接执行者，真正向被攻击主机发送攻击。（2分）

（4）被攻击者。是DDoS攻击的直接受害者，目前多为一些大型企业的网站或数据库系统。（2分）

7．简述IPSec隧道处理流程

8．简述GRE隧道处理流程

9、设 选择 ，利用RSA密钥算法，对26个字母中的第12个字母（L）加密，请问公开密钥与私有密钥分别是什么？加密后的密文字母是什么？（要求有计算过程）

10、试分析下列公钥密码分配体制可能受到的攻击，就如何改进可使该密钥分配具有保密和认证功能。

① A向B发送自己产生的公钥和A的身份；

② B收到消息后，产生会话密钥Ks，用公钥加 密后传送给A；

③ A用私钥解密后得到Ks

福师《TCP/IP协议原理与编程》在线作业一

一、单选题（共 40 道试题，共 80 分。）

[V](http://learn.open.com.cn/StudentCenter/OnLineJob/DoHomework.aspx?CourseExerciseID=225607&key=f7ebdcb43be9086b&SubmitCount=3)

1. 下列不属于通信子网层次的是（）。

A. 物理层

B. 数据链路层

C. 传输层

D. 网络层

满分：2 分

2. 以下哪个IP地址可以在Internet上使用（）。

A. 202．100．5．6

B. 127．0．0．1

C. 192．168．1．3

D. 10．20．5．5

满分：2 分

3. IP地址为172.16.101.20，子网掩码为255.255.255.0，则该IP地址中，网络地址占前（）位。

A. 19

B. 21

C. 20

D. 24

满分：2 分

4. 关于网络协议，下列（）选项是正确的。

A. 是网民们签订的合同

B. 协议，简单的说就是为了网络信息传递，共同遵守的约定

C. TCP/IP协议只是用于Internet，不能用于局域网

D. 拨号网络对应的协议是IPX/SPX

满分：2 分

5. 下面哪一项没有正确描述TCP/IP协议族？

A. 与OSI参考模型的上层进行严格的映射。

B. 支持所有标准的物理层和数据链路层协议。

C. 通过数据报序列传送信息。

D. 在接收端将数据报重新组装成完整的信息。

满分：2 分

6. 以下哪种协议可以允许用户通过Internet进行相互通信？

A. NetBEUI

B. IPX/SPX

C. TCP/IP

D. AppleTalk

满分：2 分

7. 下面协议是动态路由协议的是（）。

A. UDP

B. RIP

C. ARP

D. TCP

满分：2 分

8. 为了保证连接的可靠建立，TCP通常采用（）。

A. 3次握手法

B. 窗口控制机制

C. 自动重发机制

D. 端口机制

满分：2 分

9. 当你使用cache服务器发现网络流量非常大，查看是DNS解析的交通，如何？

A. 增大服务器中DNS记录的SOA记录

B. 减小服务器中DNS记录的SOA记录

C. 增大服务器中DNS记录的PTR记录

D. 减小服务器中DNS记录的PTR记录

满分：2 分

10. Intranet技术主要由一系列的组件和技术构成，Intranet的网络协议核心是（）。

A. ISP/SPX

B. PPP

C. TCP/IP

D. SLIP

满分：2 分

11. TCP/IP协议中，在本地机上对远程机进行文件读取操作所采用的协议是（）。

A. DNS

B. SMTP

C. TELNET

D. FTP

满分：2 分

12. 在OSI参考模型的各层次中，（）的数据传送单位是报文。

A. 物理层

B. 数据链路层

C. 网络层

D. 运输层

满分：2 分

13. 你是公司网管，网络中包括一个单独的IP子网，使用DHCP分配IP。你安装了WINS服务以减少名称解析中的广播交通。过了一些天，用户报告网络太慢了。你调查发现广播没有减少。下一步应如何查看？

A. 检查WINS服务器是否有客户机的注册记录

B. 检查WINS服务器是否有其他WINS服务器的注册记录

C. 检查WINS服务器服务是否开启

D. 检查WINS服务器是否存在静态记录

满分：2 分

14. IP头部中，"目的IP地址"字段的长度是（）。

A. 8位

B. 16位

C. 32位

D. 64位

满分：2 分

15. TCP/IP协议是Internet中计算机之间通信所必须共同遵循的一种（）。

A. 信息资源

B. 通信规定

C. 软件

D. 硬件

满分：2 分

16. 以下有关DHCP授权，正确的是:

A. 没有授权DHCP无法正常工作

B. 只有存在AD的情况下才要求授权

C. 只有域管理员可以授权

D. 授权只是一个法律问题，与技术无关

满分：2 分

17. 传输数据时，FTP服务器和FTP客户机之间建立了（）连接。

A. 1个

B. 2个

C. 3个

D. 4个

满分：2 分

18. 接收端发现有差错时，设法通知发送端重发，直到正确的码字收到为止，这种差错控制方法称为（）

A. 前向纠错

B. 自动请求重发

C. 冗余检验

D. 混合差错控制

满分：2 分

19. "TimeToLive"字段的最大值是（）。

A. 127

B. 128

C. 255

D. 256

满分：2 分

20. 标明WWW中超链接的定位信息的是（）。

A. 超文本标记语言HTML

B. 统一资源定位器URL

C. 简单网络管理协议SNMP

D. IP协议

满分：2 分

21. 关于ARP的说法错误的是（）。

A. 使用询问/回答机制

B. 缓存用于减少地址解析需要的通信

C. 从物理地址到IP地址的映射

D. 在同一个物理网络中使用

满分：2 分

22. C类IP地址中，每个网络最多有主机数是（）。

A. 128

B. 254

C. 64516

D. 192

满分：2 分

23. 网络层协议的主要用途是什么？（）。

A. 通过物理链路传送比特流

B. 通过物理链路传送帧

C. 通过网络传送分组（包）

D. 在进程间传送报文

满分：2 分

24. 已知目标计算机的IP地址却不知道其MAC地址时，应该通过哪个协议来解决？

A. IP

B. ARP

C. RARP

D. BOOTP

满分：2 分

25. 域名服务器上存放有internet主机的()。

A. 域名

B. IP地址

C. 域名和IP地址

D. E-mail地址

满分：2 分

26. 浏览器和WWW服务器之间传输网页使用的协议是（）。

A. IP

B. HTTP

C. FTP

D. Telnet

满分：2 分

27. 关于PPP协议, 下列哪一句（或几句）话是错误的？

A. 支持IPX及AppleTalk协议

B. 提供面向连接服务

C. 支持身份认证

D. 动态IP地址分配可由NCP完成

满分：2 分

28. 下列说法错误的是（）。

A. OSI的发展比TCP/IP早10年左右

B. TCP/IP现已成为Internet的主流协议

C. OSI架构很少有实际运行的系统

D. OSI具有完整的七层结构

满分：2 分

29. 在DNS区域中创建邮件交换记录时，需要设置优先级来指明邮件服务器的优先选择顺序。请问，哪个数字表示服务器具有最高的优先级？

A. 10

B. 9

C. 1

D. 0

满分：2 分

30. 一个网络中的计算机要与其他计算机直接通信，必须有什么？（）。

A. 使用相同的操作系统

B. 使用相同的硬件

C. 使用相同的协议

D. 在同一公司内部

满分：2 分

31. FTP是TCP/IP协议簇的()协议。

A. 网络层

B. 运输层

C. 应用层

D. 网络接口层

满分：2 分

32. 哪类IP地址是用作多播地址（）。

A. B类

B. C类

C. D类

D. A类

满分：2 分

33. IP头部中，"总长"字段指的是（）。

A. 数据长度

B. 头部长度+选项长度

C. 头部长度+数据长度

D. 选项长度

满分：2 分

34. 安装Windows 2003时，TCP/IP网络协议是默认安装的。按照OSI协议，有关该协议的工作层，下面的哪项描述是正确的？

A. TCP在会话层进行工作，IP在传输层进行工作

B. TCP在传输层进行工作，IP在网络层进行工作

C. TCP在网络层进行工作，IP在传输层进行工作

D. TCP和IP都在传输层进行工作

满分：2 分

35. 在通常情况下,下列哪一种说法是错误的（）。

A. ICMP协议的报文与IP数据报的格式一样

B. ICMP协议位于TCP/IP协议的互联层

C. ICMP协议的报文是作为IP数据报的数据部分传输的

D. ICMP协议不仅用于传输差错报文，还用于传输控制报文

满分：2 分

36. 哪类IP地址是用作多播地址（）发展而来的。

A. D类

B. C类

C. B类

D. A类

满分：2 分

37. ping命令就是利用（）协议来测试网络的连通性。

A. TCP

B. ICMP

C. ARP

D. IP

满分：2 分

38. ICMP测试的目的是什么

A. 确定消息是否能到达其目的地，如果不能，则确定可能的原因。

B. 保证网络中的所有活动都是受检测的。

C. 确定网络是否是根据模型建立的。

D. 确定网络是处于控制模型还是用户模型。

满分：2 分

39. 停-等协议的主要缺点是（）。

A. 通信不可靠

B. 信道利用率不高

C. 不能进行全双工通信

D. 需要大容量的存储器

满分：2 分

40. 下列哪个协议不是TCP/IP的应用层协议?（）

A. TELNET

B. PPP

C. FTP

D. SMTP

满分：2 分

**二、判断题（共 5 道试题，共 10 分。）**

[**V**](http://learn.open.com.cn/StudentCenter/OnLineJob/DoHomework.aspx?CourseExerciseID=225607&key=f7ebdcb43be9086b&SubmitCount=3&SectionIndex=2)

1. OSI参考模型并不是一个具体的计算机设备或网络，而是一个逻辑结构。

A. 错误

B. 正确

满分：2 分

2. 路由器要有路由协议处理功能，决定信息传递的最佳路径。

A. 错误

B. 正确

满分：2 分

3. 静态的IP地址和DHCP服务器提供给DHCP客户端的永久租用的IP地址是一种方式。

A. 错误

B. 正确

满分：2 分

4. 网络层的主要任务是寻址，以保证发送信息能到达目的地。

A. 错误

B. 正确

满分：2 分

5. 电子邮件在Internet上的传送则是通过SMTP实现的。

A. 错误

B. 正确

满分：2 分

**三、多选题（共 5 道试题，共 10 分。）**

[**V**](http://learn.open.com.cn/StudentCenter/OnLineJob/DoHomework.aspx?CourseExerciseID=225607&key=f7ebdcb43be9086b&SubmitCount=3&S&SectionIndex=3)

1. IP路由表能够用来存储下列哪些类型的路由：

A. 主机路由

B. 网络路由

C. 默认路由

D. 除此之外的其它类型的路由

满分：2 分

2. 在配置DNS和WINS集成查找功能时，需要在哪些计算机上进行相应的配置工作才能实现？

A. DNS服务器

B. WINS服务器

C. 客户机

D. 域控制器

满分：2 分

3. 以下为Internet层协议是:

A. IP

B. ARP

C. ICMP

D. IGMP

满分：2 分

4. 以下哪种情况下，WINS客户机会向WINS服务器发送名称释放请求？

A. WINS客户机网卡禁用时

B. WINS客户机关闭系统时

C. WINS客户机停止已注册的网络服务时

D. WINS客户机宕机时

满分：2 分

5. 某网络的一台Windows 2000成员服务器上已安装了DNS服务。在安装服务时，即创建了名为Testdomain.com的正向搜索区。下列哪些资源记录是自动在Testdomain.com区中创建的?

A. SOA

B. NS

C. MX

D. CNAME

满分：2 分

信息安全技术试题及答案

信息安全网络基础：

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. 由于传输的内容不同，电力线可以与网络线同槽铺设。×

8. 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. √

9. 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。√

10. 机房内的环境对粉尘含量没有要求。×

11. 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。√

12. 纸介质资料废弃应用碎纸机粉碎或焚毁。√

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，磁带是应用得最广的介质。√

4. 增量备份是备份从上次完全备份后更新的全部数据文件。×

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。×

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. 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

4. 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

5. 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

6. 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

7. 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

8、IBM TSM Fastback 是一款什么软件（ ）

A、防病毒产品； B、入侵防护产品； C、上网行为管理产品； D、数据存储备份产品

9、IBM TSM Fastback产品使用的什么技术（ )

A、磁盘快照； B、文件拷贝； C、ISCSI技术； D、磁盘共享

12、IBM TSM Fastback产品DR（远程容灾）功能备份的是什么（ ）

A、应用系统； B、本地备份的数据； C、文件系统； D、数据库

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

4、数据安全备份有几种策略（ ）

A、全备份； B、增量备份； C、差异备份； D、手工备份

5、建立Disaster Recovery（容灾系统）的前提是什么（ ）多选

A、自然灾害（地震、火灾，水灾...)； B、人为灾害（错误操作、黑客攻击、病毒发作...)

C、技术风险（设备失效、软件错误、电力失效...）

6、IBM TSM Fastback 可以支持数据库系统包括（ ）多选

A、MS SQL； B、Oracle； C、DB2； D、MY SQL

7、IBM TSM Fastback 可以支持的存储介质包括（ ）

A、磁带介质； B、磁盘介质； C、磁带库； D、磁盘柜

基础安全技术

系统安全

一、判断题

1. 常见的操作系统包括 DOS 、UNIX 、Linux、Windows 、 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 Microsoft Windows 、 UNIX 、 Linux 等 ); 另一些的内核与壳关系紧 密 ( 如 UNIX 、 Linux 等内核及壳只是操作层次上不同而已。×

3. 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。×

4.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√

5. 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。×

6. 数据库安全只依靠技术即可保障。×

7. 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。×

8. 数据库管理员拥有数据库的一切权限。√

9. 完全备份就是对全部数据库数据进行备份。√

二、单选题

1.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

2.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

3. 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

4. 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

5 、.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

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.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

3.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

4. 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

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. 软件防火墙就是指个人防火墙。×

3. 防火墙必须要提供 VPN 、 NAT 等功能。×

4. 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。√

5. 只要使用了防火墙，企业的网络安全就有了绝对的保障。×

6. 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。√

7. 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 。√

8. 所有的漏洞都是可以通过打补丁来弥补的。×

9. 通过网络扫描，可以判断目标主机的操作系统类型。√

10. 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。×

11. 计算机病毒可能在用户打开 "txt" 文件时被启动。√

12. 在安全模式下木马程序不能启动。×

13. 大部分恶意网站所携带的病毒就是脚本病毒。√

14. 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。√

二、单选题

1. 防火墙提供的接入模式不包括一一一。

A. 网关模式 B.透明模式 C. 混合模式 D.旁路接入模式

2. 下面关于 DMZ 区的说法错误的是

A. 通常 DMZ 包含允许来自互联网的通信可进入的设备，如 Web 服务器、 FTP 服务器、 SMTP 服务器和 DNS 服务器等

B. 内部网络可以无限制地访问外部网络以及 DMZ

C.DMZ 可以访问内部网络

D. 有两个 DMZ 的防火墙环境的典型策略是主防火墙采用 NAT 方式工作，而内部防 火墙采用透明模式工作以减少内部网络结构的复杂程度

3. 下面病毒出现的时间最晚的类型是

A. 携带特洛伊术马的病毒 B. 以网络钓鱼为目的的病毒

C. 通过网络传播的蠕虫病毒 D.OEice 文档携带的宏病毒

4. 不能防止计算机感染病毒的措施是

A. 定时备份重要文件

B. 经常更新操作系统

C. 除非确切知道附件内容，否则不要打开电子邮件附件

D. 重要部门的计算机尽量专机专用与外界隔绝

5. 企业在选择防病毒产品时不应该考虑的指标为

A. 产品能够从一个中央位置进行远程安装、升级 '

B. 产品的误报、漏报率较低

C. 产品提供详细的病毒活动记录

D. 产品能够防止企业机密信息通过邮件被传出

6. 病毒传播的途径有

A. 移动硬盘 B. 内存条

C. 电子邮件 D. 聊天程序

E 网络浏览

7. 可能和计算机病毒有关的现象有

A. 可执行文件大小改变了

B. 在向写保护的 U 盘复制文件时屏幕上出现 U 盘写保护的提示

C. 系统频繁死机

D. 内存中有来历不明的进程

E. 计算机主板损坏

应用安全

一、判断题

1. 运行防病毒软件可以帮助防止遭受网页仿冒欺诈。√

2. 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。√

3. 网络钓鱼的目标往往是细心选择的一些电子邮件地址。√

4. 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。×

5. 在来自可信站点的电子邮件中输入个人或财务信息是安全的。×

6. 可以采用内容过滤技术来过滤垃圾邮件。√

7. 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。√

8. 随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模块成为信息安全领域的一个发展趋势√

9 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才肤内容。√

10. 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。√

11. 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。×

二、单选题

1. 以下不会帮助减少收到的垃圾邮件数量的是一一一。

A. 使用垃圾邮件筛选器帮助阻止垃圾邮件 .

B. 共享电子邮件地址或即时消息地址时应小心谨慎

C. 安装入侵检测软件

D. 收到垃圾邮件后向有关部门举报

三、多选题

1. 下列邮件为垃圾邮件的有

A. 收件人无法拒收的电子邮件

B. 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件 C. 含有病毒、色情、反动等不良信息或有害信息的邮件

D. 隐藏发件人身份、地址、标题等信息的电子邮件

E. 含有虚假的信息源、发件人、路由等信息的电子邮件

2. 垃圾邮件带来的危害有

A. 垃圾邮件占用很多互联网资源

B. 垃圾邮件浪费广大用户的时间和精力

C. 垃圾邮件提高了某些公司做广告的效益

D. 垃圾邮件成为病毒传播的主要途径

E. 垃圾邮件迫使企业使用最新的操作系统

3. 网页防篡改技术包括

A. 网站采用负载平衡技术 B. 防范网站、网页被篡改

C. 访问网页时需要输入用户名和口令 D. 网页被篡改后能够自动恢复

E 采用 HITPS 协议进行网页传输主

4. 网络钓鱼常用的手段有

A. 利用垃圾邮件 B. 利用假冒网上银行、网上证券网站

C. 利用虚假的电子商务 D. 利用计算机病毒

E. 利用社会工程学

5. 内容过滤的目的包括

A. 阻止不良信息对人们的侵害

B. 规范用户的上网行为，提高工作效率

C. 防止敏感数据的泄漏

D. 遏制垃圾邮件的蔓延

E. 减少病毒对网络的侵害

7. 内容过滤技术的应用领域包括

A. 防病毒 B.网页防篡改 C. 防火墙 D.入侵检测 E. 反垃圾邮件

信息安全技术教程试题

1282 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.

A 正确 B 错误

1283 计算机场地可以选择在公共区域人流量比较大的地方。

A 正确 B 错误

1284 计算机场地可以选择在化工厂生产车间附近。

A 正确 B 错误

1285 计算机场地在正常情况下温度保持在18～28摄氏度。

A 正确 B 错误

1286 机房供电线路和动力、照明用电可以用同一线路。

A 正确 B 错误

1287 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。

A 正确 B 错误

1288 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。

A 正确 B 错误

1289 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。

A 正确 B 错误

1290 屏蔽室的拼接、焊接工艺对电磁防护没有影响。

A 正确 B 错误

1291 由于传输的内容不同，电力线可以与网络线同槽铺设。

A 正确 B 错误

1292 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。地线做电气连通。

A 正确 B 错误

1293 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。

A 正确 B 错误

1294 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。

A 正确 B 错误

1295 机房内的环境对粉尘含量没有要求。

A 正确 B 错误

1296 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。

A 正确 B 错误

1297 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。

A 正确 B 错误

1298 纸介质资料废弃应用碎纸机粉碎或焚毁。

A 正确 B 错误

1299 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

1300 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

1301 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

1302 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

1303 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

1304 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 具有自动和手动两种触发装置

1305 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

1306 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

1307 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 专用强磁工具清除

1308 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

1309 防止设备电磁辐射可以采用的措施有\_\_\_\_。

A 屏蔽 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

1310 灾难恢复和容灾具有不同的含义。

A 正确 B 错误

1311 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。

A 正确 B 错误

1312 对目前大量的数据备份来说，磁带是应用得最广的介质。

A 正确 B 错误

1313 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。

A 正确 B 错误

1314 容灾等级通用的国际标准SHARE 78将容灾分成了六级。

A 正确 B 错误

1315 容灾就是数据备份。

A 正确 B 错误

1316 数据越重要，容灾等级越高。

A 正确 B 错误

1317 容灾项目的实施过程是周而复始的。

A 正确 B 错误

1318 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。

A 正确 B 错误

1319 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。

A 正确 B 错误

1320 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。

A 正确 B 错误

1321 代表了当灾难发生后，数据的恢复程度的指标是\_\_\_\_。

A RPO B RTOC NROD SDO

1322 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 NROD SDO

1323 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

1324 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

1325 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

1326 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\_\_\_\_。

A 磁盘 B 磁带 C 光盘D 软盘

1327 下列叙述不属于完全备份机制特点描述的是\_\_\_\_。

A 每次备份的数据量较大B 每次备份所需的时间也就较长C 不能进行得太频繁 D 需要存储空间小

1328 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

1329 信息系统的容灾方案通常要考虑的要点有\_\_\_\_。

A 灾难的类型 B 恢复时间 C 恢复程度 D 实用技术 E 成本

1330 系统数据备份包括的对象有\_\_\_\_。

A 配置文件 B 日志文件 C 用户文档 D 系统设备文件

1331 容灾等级越高，则\_\_\_\_。

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

1332 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。

A 正确 B 错误

1333 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。

A 正确 B 错误

1334 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。

A 正确 B 错误

1335 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。

A 正确 B 错误

1336 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。

A 正确 B 错误

1337 PKI系统的基本组件包括\_\_\_\_。

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

1338 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

1339 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

1340 常见的操作系统包括DOS、0S／2、UNIX、XENIX、Linux、Windows、Netware、Oracle等。

A 正确 B 错误

1341 操作系统在概念上一般分为两部分：内核(Kernel)以及壳(Shell)，有些操作系统的内核与壳完全分开(如Microsoft Windows、UNIX、Linux等)；另一些的内核与壳关系紧密(如UNIX、Linux等)，内核及壳只是操作层次上不同而已。

A 正确 B 错误

1342 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。

A 正确 B 错误

1343 Windows系统的用户帐号有两种基本类型：全局帐号(GlobalAccounts)和本地帐号(LocalAccounts)。

A 正确 B 错误

1344 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。

A 正确 B 错误

1345 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。

A 正确 B 错误

1346 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。

A 正确 B 错误

1347 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。

A 正确 B 错误

1348 在默认情况下，内置DomainAdmins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。

A 正确 B 错误

1349 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。

A 正确 B 错误

1350 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BackupOperators组有此权限，而Lois又是该组成员，则Lois也有此权限。

A 正确 B 错误

1351 Windows文件系统中，只有Administrator组和ServerOperation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。

A 正确 B 错误

1352 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。

A 正确 B 错误

1353 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。

A 正确 B 错误

1354 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。

A 正确 B 错误

1355 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。

A 正确 B 错误

1356 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。

A 正确 B 错误

1357 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。

A 正确 B 错误

1358 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只定义了一个操作系统内核。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。

A 正确 B 错误

1359 每个UNIX／Linux系统中都只有一个特权用户，就是root帐号。

A 正确 B 错误

1360 与Windows系统不一样的是UNIX／Linux操作系统中不存在预置帐号。

A 正确 B 错误

1361 UNIX／Linux系统中一个用户可以同时属于多个用户组。

A 正确 B 错误

1362 标准的UNIX／Linux系统以属主(Owner)、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。

A 正确 B 错误

1363 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。

A 正确 B 错误

1364 UNIX／Linux系统和Windows系统类似，每一个系统用户都有一个主目录。

A 正确 B 错误

1365 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。

A 正确 B 错误

1366 UNIX／Linux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。

A 正确 B 错误

1367 Httpd.conf是Web服务器的主配置文件，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。

A 正确 B 错误

1368 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。

A 正确 B 错误

1369 UNIX／Linux系统中的／etc／shadow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／etc／passwd文件中)。

A 正确 B 错误

1370 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。

A 正确 B 错误

1371 数据库安全只依靠技术即可保障。

A 正确 B 错误

1372 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。

A 正确 B 错误

1373 数据库的强身份认证与强制访问控制是同一概念。

A 正确 B 错误

1374 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。

A 正确 B 错误

1375 数据库视图可以通过INSERT或UPDATE语句生成。

A 正确 B 错误

1376 数据库加密适宜采用公开密钥密码系统。

A 正确 B 错误

1377 数据库加密的时候，可以将关系运算的比较字段加密。

A 正确 B 错误

1378 数据库管理员拥有数据库的一切权限。

A 正确 B 错误

1379 不需要对数据库应用程序的开发者制定安全策略。

A 正确 B 错误

1380 使用登录ID登录SQL Server后，即获得了访问数据库的权限。

A 正确 B 错误

1381 MS SQL Server与Sybase SQL Server的身份认证机制基本相同。

A 正确 B 错误

1382 SQL Server不提供字段粒度的访问控制。

A 正确 B 错误

1383 MySQL不提供字段粒度的访问控制。

A 正确 B 错误

1384 SQL Server中，权限可以直接授予用户ID。

A 正确 B 错误

1385 SQL注入攻击不会威胁到操作系统的安全。

A 正确 B 错误

1386 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。

A 正确 B 错误

1387 完全备份就是对全部数据库数据进行备份。

A 正确 B 错误

1388 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 C 七 D 八

1389 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

1390 Windows系统安装完后，默认隋况下系统将产生两个帐号，分别是管理员帐号和\_\_\_\_。

A 本地帐号B 域帐号 C 来宾帐号 D 局部帐号

1391 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

1392 —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\_\_\_\_和\_\_\_\_。

A 12 8B 14 10C 12 10 D 14 8

1393 符合复杂性要求的WindowsXP帐号密码的最短长度为\_\_\_\_。

A 4 B 6 C 8D 10

1394 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\_\_\_\_。

A kedaB kedaliu C kedawuj D dawu

1395 某公司的工作时间是上午8点半至12点，下午1点555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\_\_\_\_。

A 上午8点B 中午12点C 下午3点 D 凌晨l点

1396 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\_\_\_\_。

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

1397 在正常情况下，Windows 2000中建议关闭的服务是\_\_\_\_。

A TCP／IP NetBIOS Helper Service B Logical Disk ManagerC Remote Procedure CallD Security Accounts Manager

1398 FTP(文件传输协议，File Transfer Protocol，简称FFP)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\_\_\_\_。

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

1399 下面不是UNIX／Linux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

1400 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

1401 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NFSDaemon 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NFSDaemon，其中安全性能较强的是基于内核的NFSDaemonC UNIX系统中现只有一种NFS服务器，就是基于内核的NFSDaemon，原有的用户空间Daemon已经被淘汰，因为NFSDaemon安全性能较好D UNIX系统中现只有一种NFS服务器，就是基于内核的Daemon，原有的用户空间NFSDaemon已经被淘汰，因为Daemon安全性能较好

1402 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 tarB cpio C umask D backup

1403 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—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

1404 UNIX工具(实用程序，utilities)在新建文件的时候，通常使用\_\_\_\_作为缺省许可位，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 888D 888 999

1405 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／groupC 设置足够强度的帐号密码D 使用shadow密码

1406 UNIX／Linux系统中，下列命令可以将普通帐号变为root帐号的是\_\_\_\_。

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

1407 有编辑／etc／passwd文件能力的攻击者可以通过把UID变为\_\_\_\_就可以成为特权用户。

A -1 B 0 C 1D 2

1408 下面不是保护数据库安全涉及到的任务是\_\_\_\_。

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

1409 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

1410 关于用户角色，下面说法正确的是\_\_\_\_。

A SQL Server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

1411 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D 自主原则

1412 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

1413 有关数据库加密，下面说法不正确的是\_\_\_\_。

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

1414 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

1415 下面不是SQL Server支持的身份认证方式的是\_\_\_\_。

A Windows NT集成认证B SQL Server认证C SQL Server混合认证 D 生物认证

1416 下面\_\_\_\_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RDBMSD 开放源码数据库

1417 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

1418 下面不是Oracle数据库支持的备份形式的是\_\_\_\_。

A 冷备份 B 温备份 C 热备份D 逻辑备份

1419 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

1420 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

1421 根据SahzerJ.H、SchroederM.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

1422 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

1423 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(SecurityAccountManager，简称SAM)模块 B Windows系统的注册(WinLogon)模块 C 本地安全认证(10calSecurityAuthority，简称LSA)模块 D 安全引用监控器模块

1424 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\_\_\_\_。

A DomainAdmins组 B DomainUsers组 C DomainReplicators组 D Domain Guests组

1425 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(ApplicationsLog) D 用户日志(UserLog)

1426 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

1427 UNIX／Linux系统中的密码控制信息保存在／etc／passwd或／ect／shadow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 密码最近的改变时间 D 密码有效的最大天数

1428 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\_\_\_\_。

A 利用HTYP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

1429 数据库访问控制的粒度可能有\_\_\_\_。

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

1430 下面标准可用于评估数据库的安全级别的有\_\_\_\_。

A TCSEC B ITSEC C CC DBMS.PP D GB 17859——1999 E TDI

1431 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 模式对象设计 E 外部对象审计

1432 SQL Server中的预定义服务器角色有\_\_\_\_。

A sysadmin B serveradmin C setupadmin D securityadmin E processadmin

1433 可以有效限制SQL注入攻击的措施有\_\_\_\_。

A 限制DBMS中sysadmin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

1434 事务的特性有\_\_\_\_。

A 原子性(Atomicity) B 一致性(Consistency) C 隔离性(1solation) D 可生存性(Survivability) E 持续性(Durability)

1435 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

1436 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。

A 正确 B 错误

1437 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(DynamicPacketFilter)。

A 正确 B 错误

1438 软件防火墙就是指个人防火墙。

A 正确 B 错误

1439 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。

A 正确 B 错误

1440 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。

A 正确 B 错误

1441 防火墙安全策略一旦设定，就不能在再做任何改变。

A 正确 B 错误

1442 对于防火墙的管理可直接通过Telnet进行。

A 正确 B 错误

1443 防火墙规则集的内容决定了防火墙的真正功能。

A 正确 B 错误

1444 防火墙必须要提供VPN、NAT等功能。

A 正确 B 错误

1445 防火墙对用户只能通过用户名和口令进行认证。

A 正确 B 错误

1446 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。

A 正确 B 错误

1447 只要使用了防火墙，企业的网络安全就有了绝对的保障。

A 正确 B 错误

1448 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。

A 正确 B 错误

1449 iptables可配置具有状态包过滤机制的防火墙。

A 正确 B 错误

1450 可以将外部可访问的服务器放置在内部保护网络中。

A 正确 B 错误

1451 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。

A 正确 B 错误

1452 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。

A 正确 B 错误

1453 主动响应和被动响应是相互对立的，不能同时采用。

A 正确 B 错误

1454 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。

A 正确 B 错误

1455 针对入侵者采取措施是主动响应中最好的响应措施。

A 正确 B 错误

1456 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。

A 正确 B 错误

1457 性能“瓶颈”是当前入侵防御系统面临的一个挑战。

A 正确 B 错误

1458 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。

A 正确 B 错误

1459 与入侵检测系统不同，入侵防御系统采用在线(inline)方式运行。

A 正确 B 错误

1460 蜜罐技术是一种被动响应措施。

A 正确 B 错误

1461 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。

A 正确 B 错误

1462 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。

A 正确 B 错误

1463 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。

A 正确 B 错误

1464 在早期用集线器(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子网。

A 正确 B 错误

1465 可以通过技术手段，一次性弥补所有的安全漏洞。

A 正确 B 错误

1466 漏洞只可能存在于操作系统中，数据库等其他软件系统不会存在漏洞。

A 正确 B 错误

1467 防火墙中不可能存在漏洞。

A 正确 B 错误

1468 基于主机的漏洞扫描不需要有主机的管理员权限。

A 正确 B 错误

1469 半连接扫描也需要完成TCP协议的三次握手过程。

A 正确 B 错误

1470 使用漏洞库匹配的方法进行扫描，可以发现所有的漏洞。

A 正确 B 错误

1471 所有的漏洞都是可以通过打补丁来弥补的。

A 正确 B 错误

1472 通过网络扫描，可以判断目标主机的操作系统类型。

A 正确 B 错误

1473 x-scan能够进行端口扫描。

A 正确 B 错误

1474 隔离网闸采用的是物理隔离技术。

A 正确 B 错误

1475 “安全通道隔离”是一种逻辑隔离。

A 正确 B 错误

1476 隔离网闸两端的网络之间不存在物理连接。

A 正确 B 错误

1477 QQ是与朋友联机聊天的好工具，不必担心病毒。

A 正确 B 错误

1478 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。

A 正确 B 错误

1479 计算机病毒可能在用户打开“txt”文件时被启动。

A 正确 B 错误

1480 在安全模式下木马程序不能启动。

A 正确 B 错误

1481 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。

A 正确 B 错误

1482 家里的计算机没有联网，所以不会感染病毒。

A 正确 B 错误

1483 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。

A 正确 B 错误

1484 校验和技术只能检测已知的计算机病毒。

A 正确 B 错误

1485 采用Rootkit 技术的病毒可以运行在内核模式中。

A 正确 B 错误

1486 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。

A 正确 B 错误

1487 大部分恶意网站所携带的病毒就是脚本病毒。

A 正确 B 错误

1488 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。

A 正确 B 错误

1489 防火墙是\_\_\_\_在网络环境中的应用。

A 字符串匹配 B 访问控制技术 C 入侵检测技术D 防病毒技术

1490 iptables中默认的表名是\_\_\_\_。

A filter B firewallC natD mangle

1491 包过滤防火墙工作在OSI网络参考模型的\_\_\_\_。

A 物理层B 数据链路层 C 网络层 D 应用层

1492 通过添加规则，允许通往192.168.0.2的SSH连接通过防火墙的iptables指令是\_\_\_\_。

A iptables -F INPUT -d 192.168.0.2 -p tcp--dport 22 -j ACCEPTB iptables -A INPUT -d 192.168.0.2 -p tcp--dport 23 -j ACCEPT C iptables -A FORWARD -d 192.168.0.2 -p tcp--dport22 -j ACCEPT D iptables -A FORWARD -d 192.168.0.2 -p tcp--dport 23 -j ACCEPT

1493 防火墙提供的接入模式不包括\_\_\_\_。

A 网关模式B 透明模式C 混合模式 D 旁路接入模式

1494 关于包过滤防火墙说法错误的是\_\_\_\_。

A 包过滤防火墙通常根据数据包源地址、目的地址、端口号和协议类型等标志设置访问控制列表实施对数据包的过滤B 包过滤防火墙不检查OSI网络参考模型中网络层以上的数据，因此可以很快地执行 C 包过滤防火墙可以有效防止利用应用程序漏洞进行的攻击 D 由于要求逻辑的一致性、封堵端口的有效性和规则集的正确性，给过滤规则的制定和配置带来了复杂性，一般操作人员难以胜任管理，容易出现错误

1495 关于应用代理网关防火墙说法正确的是\_\_\_\_。

A 基于软件的应用代理网关工作在OSI网络参考模型的网络层上，它采用应用协议代理服务的工作方式实施安全策略B 一种服务需要一种代理模块，扩展服务较难 C 和包过滤防火墙相比，应用代理网关防火墙的处理速度更快D 不支持对用户身份进行高级认证机制。一般只能依据包头信息，因此很容易受到“地址欺骗型”攻击

1496 关于NAT说法错误的是\_\_\_\_。

A NAT允许一个机构专用Intranet中的主机透明地连接到公共域中的主机，无需内部主机拥有注册的(已经越采越缺乏的)全局互联网地址B 静态NAT是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址C 动态NAT主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态NAT就会分配给用户一个IP地址，当用户断开时，这个IP地址就会被释放而留待以后使用 D 动态NAT又叫做网络地址端口转换NAPT

1497 下面关于防火墙策略说法正确的是\_\_\_\_。

A 在创建防火墙策略以前，不需要对企业那些必不可少的应用软件执行风险分析B 防火墙安全策略一旦设定，就不能在再作任何改变 C 防火墙处理人站通信的缺省策略应该是阻止所有的包和连接，除了被指出的允许通过的通信类型和连接 D 防火墙规则集与防火墙平台体系结构无关

1498 下面关于DMZ区的说法错误的是\_\_\_\_。

A 通常DMZ包含允许来自互联网的通信可进入的设备，如Web服务器、FTP服务器、SMTP服务器和DNS服务器等B 内部网络可以无限制地访问外部网络以及DMZ C DMZ可以访问内部网络 D 有两个DMZ的防火墙环境的典型策略是主防火墙采用NAT方式工作，而内部防火墙采用透明模式工作以减少内部网络结构的复杂程度

1499 在PDRR模型中，\_\_\_\_是静态防护转化为动态的关键，是动态响应的依据。

A 防护 B 检测 C 响应D 恢复

1500 从系统结构上来看，入侵检测系统可以不包括\_\_\_\_。

A 数据源B 分析引擎 C 审计 D 响应

1501 通用入侵检测框架(CIDF)模型中，\_\_\_\_的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

A 事件产生器 B 事件分析器C 事件数据库D 响应单元

1502 基于网络的入侵检测系统的信息源是\_\_\_\_。

A 系统的审计日志B 系统的行为数据C 应用程序的事务日志文件 D 网络中的数据包

1503 误用入侵检测技术的核心问题是\_\_\_\_的建立以及后期的维护和更新。

A 异常模型B 规则集处理引擎 C 网络攻击特征库 D 审计日志

1504 \_\_\_\_是在蜜罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个蜜罐，来构成一个黑客诱捕网络体系架构。

A 蜜网 B 鸟饵C 鸟巢D 玻璃鱼缸

1505 下面关于响应的说法正确的是\_\_\_\_。

A 主动响应和被动响应是相互对立的，不能同时采用B 被动响应是入侵检测系统中的唯一响应方式C 入侵检测系统提供的警报方式只能是显示在屏幕上的警告信息或窗口 D 主动响应的方式可以是自动发送邮件给入侵发起方的系统管理员请求协助以识别问题和处理问题

1506 下面说法错误的是\_\_\_\_。

A 由于基于主机的入侵检测系统可以监视一个主机上发生的全部事件，它们能够检测基于网络的入侵检测系统不能检测的攻击B 基于主机的入侵检测可以运行在交换网络中 C 基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描 D 基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击，因为应用程序日志并不像操作系统审计追踪日志那样被很好地保护

1507 使用漏洞库匹配的扫描方法，能发现\_\_\_\_。

A 未知的漏洞 B 已知的漏洞 C 自行设计的软件中的漏洞D 所有漏洞

1508 下面\_\_\_\_不可能存在于基于网络的漏洞扫描器中。

A 漏洞数据库模块B 扫描引擎模块C 当前活动的扫描知识库模块 D 阻断规则设置模块

1509 网络隔离技术，根据公认的说法，迄今已经发展了\_\_\_\_个阶段。

A 六 B 五 C 四D 三

1510 下面关于隔离网闸的说法，正确的是\_\_\_\_。

A 能够发现已知的数据库漏洞B 可以通过协议代理的方法，穿透网闸的安全控制 C 任何时刻，网闸两端的网络之间不存在物理连接 D 在OSI的二层以上发挥作用

1511 关于网闸的工作原理，下面说法错误的是\_\_\_\_.

A 切断网络之间的通用协议连接B 将数据包进行分解或重组为静态数据；对静态数据进行安全审查，包括网络协议检查和代码扫描等 C 网闸工作在OSI模型的二层以上 D 任何时刻，网闸两端的网络之间不存在物理连接

1512 当您收到您认识的人发来的电子邮件并发现其中有意外附件，您应该\_\_\_\_。

A 打开附件，然后将它保存到硬盘B 打开附件，但是如果它有病毒，立即关闭它 C 用防病毒软件扫描以后再打开附件D 直接删除该邮件

1513 下面病毒出现的时间最晚的类型是\_\_\_\_.

A 携带特洛伊木马的病毒 B 以网络钓鱼为目的的病毒 C 通过网络传播的蠕虫病毒D Office文档携带的宏病毒

1514 某病毒利用RPCDCOM缓冲区溢出漏洞进行传播，病毒运行后，在％System％文件夹下生成自身的拷贝nvchip4.exe，添加注册表项，使得自身能够在系统启动时自动运行。通过以上描述可以判断这种病毒的类型为\_\_\_\_。

A 文件型病毒B 宏病毒 C 网络蠕虫病毒 D 特洛伊木马病毒

1515 采用“进程注入”可以\_\_\_\_。

A 隐藏进程B 隐藏网络端口 C 以其他程序的名义连接网络 D 以上都正确

1516 下列关于启发式病毒扫描技术的描述中错误的是\_\_\_\_。

A 启发式病毒扫描技术是基于人工智能领域的启发式搜索技术B 启发式病毒扫描技术不依赖于特征代码来识别计算机病毒 C 启发式病毒扫描技术不会产生误报，但可能会产生漏报 D 启发式病毒扫描技术能够发现一些应用了已有机制或行为方式的病毒

1517 不能防止计算机感染病毒的措施是\_\_\_\_\_。

A 定时备份重要文件 B 经常更新操作系统C 除非确切知道附件内容，否则不要打开电子邮件附件D 重要部门的计算机尽量专机专用与外界隔绝

1518 企业在选择防病毒产品时不应该考虑的指标为\_\_\_\_。

A 产品能够从一个中央位置进行远程安装、升级B 产品的误报、漏报率较低C 产品提供详细的病毒活动记录 D 产品能够防止企业机密信息通过邮件被传出

1519 防火墙通常阻止的数据包包括\_\_\_\_。

A 来自未授权的源地址且目的地址为防火墙地址的所有入站数据包(除Email传递等特殊用处的端口外) B 源地址是内部网络地址的所有入站数据包 C 所有ICMP类型的入站数据包 D 来自未授权的源地址，包含SNMP的所有入站数据包E 包含源路由的所有入站和出站数据包

1520 目前市场上主流防火墙提供的功能包括\_\_\_\_。

A 数据包状态检测过滤 B 应用代理 C NAT D VPN E 日志分析和流量统计分析

1521 防火墙的局限性包括\_\_\_\_。

A 防火墙不能防御绕过了它的攻击 B 防火墙不能消除来自内部的威胁 C 防火墙不能对用户进行强身份认证 D 防火墙不能阻止病毒感染过的程序和文件进出网络

1522 防火墙的性能的评价方面包括\_\_\_\_。

A 并发会话数 B 吞吐量 C 延时 D 平均无故障时间

1523 下面关于防火墙的维护和策略制定说法正确的是\_\_\_\_。

A 所有防火墙管理功能应该发生在使用了强认证和加密的安全链路上 B Web界面可以通过SSL加密用户名和密码。非Web的图形界面如果既没有内部加密，也没有SSL，可以使用隧道解决方案，如SSH C 对防火墙策略进行验证的最简单的方法是，获得防火墙配置的拷贝，然后把这些拷贝和根据已定义的策略产生的期望配置进行比较 D 对防火墙策略进行验证的另一种方式通过使用软件对防火墙配置进行实际测试 E 渗透分析可以取代传统的审计程序

1524 蜜罐技术的主要优点有\_\_\_\_。

A 蜜罐技术属于被动响应，使用者没有成为刑事诉讼或民事诉讼对象的危险 B 收集数据的真实性，蜜罐不提供任何实际的业务服务，所以搜集到的信息很大可能性都是由于黑客攻击造成的，漏报率和误报率都比较低 C 可以收集新的攻击工具和攻击方法，不像目前的大部分防火墙和入侵检测系统只能根据特征匹配方法来检测已知的攻击 D 不需要强大的资金投入，可以用一些低成本的设备 E 可以及时地阻断网络入侵行为

1525 通用入侵检测框架(CIDF)模型的组件包括\_\_\_\_。

A 事件产生器 B 活动轮廓 C 事件分析器 D 事件数据库 E 响应单元

1526 主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有\_\_\_\_。

A 针对入侵者采取措施 B 修正系统 C 收集更详细的信息 D 入侵追踪

1527 随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器(sniffer)来监听整个子网的办法不再可行。可选择解决的办法有\_\_\_\_。

A 不需要修改，交换网络和以前共享媒质模式的网络没有任何区别 B 使用交换机的核心芯片上的一个调试的端口 C 把入侵检测系统放在交换机内部或防火墙等数据流的关键入口、出口处 D 采用分接器(tap) E 使用以透明网桥模式接入的入侵检测系统

1528 入侵防御技术面临的挑战主要包括\_\_\_\_。

A 不能对入侵活动和攻击性网络通信进行拦截 B 单点故障 C 性能“瓶颈” D 误报和漏报

1529 网络安全扫描能够\_\_\_\_。

A 发现目标主机或网络 B 判断操作系统类型 C 确认开放的端口 D 识别网络的拓扑结构 E 测试系统是否存在安全漏洞

1530 主机型漏洞扫描器可能具备的功能有\_\_\_\_。

A 重要资料锁定：利用安全的校验和机制来监控重要的主机资料或程序的完整性 B 弱口令检查：采用结合系统信息、字典和词汇组合等的规则来检查弱口令 C 系统日志和文本文件分析：针对系统日志档案，如UNIX的syslogs及NT的事件日志(EventLog)，以及其他文本文件的内容做分析 D 动态报警：当遇到违反扫描策略或发现已知安全漏洞时，提供及时的告警。告警可以采取多种方式，可以是声音、弹出窗口、电子邮件甚至手机短信等 E 分析报告：产生分析报告，并告诉管理员如何弥补漏洞

1531 下面对于x-scan扫描器的说法，正确的有\_\_\_\_。

A 可以进行端口扫描 B 含有攻击模块，可以针对识别到的漏洞自动发起攻击 C 对于一些已知的CGI和RPC漏洞，x-scan给出了相应的漏洞描述以及已有的通过此漏洞进行攻击的工具 D 需要网络中每个主机的管理员权限 E 可以多线程扫描

1532 下面软件产品中，\_\_\_\_是漏洞扫描器。

A x-scan B nmap C Internet Scanner D Norton AntiVirusE Snort

1533 隔离网闸的三个组成部分是\_\_\_\_。

A 漏洞扫描单元B 入侵检测单元 C 内网处理单元 D 外网处理单元 E 专用隔离硬件交换单元

1534 网闸可能应用在\_\_\_\_。

A 涉密网与非涉密网之间 B 办公网与业务网之间 C 电子政务的内网与专网之间 D 业务网与互联网之间 E 局域网与互联网之间

1535 下面不是网络端口扫描技术的是\_\_\_\_。

A 全连接扫描B 半连接扫描 C 插件扫描 D 特征匹配扫描 E 源码扫描

1536 按照2000年3月公布的《计算机病毒防治管理办法》对计算机病毒的定义，下列属于计算机病毒的有\_\_\_\_。

A 某Word文档携带的宏代码，当打开此文档时宏代码会搜索并感染计算机上所有的Word文档 B 某用户收到来自朋友的一封电子邮件，当打开邮件附件时，邮件附件将自身发送给该用户地址簿中前五个邮件地址 C 某员工在公司内部使用的系统中加入一个逻辑炸弹，如果该员工在一年内被解雇则逻辑炸弹就会破坏系统D 黑客入侵了某服务器，并在其上安装了一个后门程序 E 某QQ用户打开了朋友发送来的一个链接后，发现每次有好友上线QQ都会自动发送一个携带该链接的消息

1537 病毒传播的途径有\_\_\_\_。

A 移动硬盘 B 内存条 C 电子邮件 D 聊天程序 E 网络浏览

1538 可能和计算机病毒有关的现象有\_\_\_\_。

A 可执行文件大小改变了 B 在向写保护的U盘复制文件时屏幕上出现U盘写保护的提示 C 系统频繁死机 D 内存中有来历不明的进程 E 计算机主板损坏

1539 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。

A 正确 B 错误

1540 反向查询方法可以让接收邮件的互联网服务商确认邮件发送者是否就是如其所言的真实地址。

A 正确 B 错误

1541 SenderlD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。

A 正确 B 错误

1542 DKIM(Domain Keys Identified 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。

A 正确 B 错误

1543 运行防病毒软件可以帮助防止遭受网页仿冒欺诈。

A 正确 B 错误

1544 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。

A 正确 B 错误

1545 网络钓鱼的目标往往是细心选择的一些电子邮件地址。

A 正确 B 错误

1546 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。

A 正确 B 错误

1547 在来自可信站点的电子邮件中输入个人或财务信息是安全的。

A 正确 B 错误

1548 包含收件人个人信息的邮件是可信的。

A 正确 B 错误

1549 可以采用内容过滤技术来过滤垃圾邮件。

A 正确 B 错误

1550 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。

A 正确 B 错误

1551 随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模块成为信息安全领域的一个发展趋势。

A 正确 B 错误

1552 启发式技术通过查找通用的非法内容特征，来尝诩蝴IJ新形式和已知形式的非法内容。

A 正确 B 错误

1553 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。

A 正确 B 错误

1554 实时黑名单是简单黑名单的进—步发展，可以从根本上解决垃圾邮件问题。

A 正确 B 错误

1555 贝叶斯过滤技术具有自适应、自学习的能力，目前已经得到了广泛的应用。

A 正确 B 错误

1556 对网页请求参数进行验证，可以防止SQL注入攻击。

A 正确 B 错误

1557 以下不会帮助减少收到的垃圾邮件数量的是\_\_\_\_。

A 使用垃圾邮件筛选器帮助阻止垃圾邮件B 共享电子邮件地址或即时消息地址时应小心谨慎 C 安装入侵检测软件 D 收到垃圾邮件后向有关部门举报

1558 下列不属于垃圾邮件过滤技术的是\_\_\_\_。

A 软件模拟技术 B 贝叶斯过滤技术C 关键字过滤技术D 黑名单技术

1559 下列技术不支持密码验证的是\_\_\_\_。

A S／MIMEB PGPC AMTP D SMTP

1560 下列行为允许的有\_\_\_\_。

A 未经授权利用他人的计算机系统发送互联网电子邮件B 将采用在线自动收集、字母或者数字任意组合等手段获得的他人的互联网电子邮件地址用于出售、共享、交换或者向通过上述方式获得的电子邮件地址发送互联网电子邮件C 未经互联网电子邮件接收者明确伺意，向其发送包含商业广告内容的互联网电子邮件 D 爱选包含商业广告内容的互联网电子邮件时，在互联网电子邮件标题信息前部注明“广告”或者“AD'’字样

1561 下列技术不能使网页被篡改后能够自动恢复的是\_\_\_\_。

A 限制管理员的权限 B 轮询检测C 事件触发技术D 核心内嵌技术

1562 以下不可以表示电子邮件可能是欺骗性的是\_\_\_\_。

A 它要求您点击电子邮件中的链接并输入您的帐户信息B 传达出一种紧迫感 C 通过姓氏和名字称呼您 D 它要求您验证某些个人信息

1563 如果您认为您已经落入网络钓鱼的圈套，则应采取\_\_\_\_措施。

A 向电子邮件地址或网站被伪造的公司报告该情形B 更改帐户的密码C 立即检查财务报表 D 以上全部都是

1564 内容过滤技术的含义不包括\_\_\_\_。

A 过滤互联网请求从而阻止用户浏览不适当的内容或站点B 过滤流入的内容从而阻止潜在的攻击进入用户的网络系统C 过滤流出的内容从而阻止敏感数据的泄漏 D 过滤用户的输入从而阻止用户传播非法内容

1565 下列内容过滤技术中在我国没有得到广泛应用的是\_\_\_\_。

A 内容分级审查 B 关键字过滤技术C 启发式内容过滤技术D 机器学习技术

1566 会让一个用户的“删除”操作去警告其他许多用户的垃圾邮件过滤技术是\_\_\_\_。

A 黑名单B 白名单C 实时黑名单 D 分布式适应性黑名单

1567 不需要经常维护的垃圾邮件过滤技术是\_\_\_\_。

A 指纹识别技术 B 简单DNS测试 C 黑名单技术D 关键字过滤

1568 下列关于网络钓鱼的描述不正确的是\_\_\_\_。

A 网络钓鱼(Phishing)一词，是“Fishing”和“Phone”的综合体 B 网络钓鱼都是通过欺骗性的电子邮件来进行诈骗活动C 为了消除越来越多的以网络钓鱼和电子曲6件欺骗的形式进行的身份盗窃和欺诈行为，相关行业成立了一个协会——反网络钓鱼工作小组D 网络钓鱼在很多方面和一般垃圾邮件有所不同，理解这些不同点对设计反网络钓鱼技术至关重要

1569 下面技术中不能防止网络钓鱼攻击的是\_\_\_\_。

A 在主页的底部设有一个明显链接，以提醒用户注意有关电子邮件诈骗的问题B 利用数字证书(如 USB KEY)进行登录C 根据互联网内容分级联盟(ICRA)提供的内容分级标准对网站内容进行分级 D 安装杀毒软件和防火墙、及时升级、打补丁、加强员工安全意识

1570 下列邮件为垃圾邮件的有\_\_\_\_。

A 收件人无法拒收的电子邮件 B 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件 C 含有病毒、色情、反动等不良信息或有害信息的邮件 D 隐藏发件人身份、地址、标题等信息的电子邮件 E 含有虚假的信息源、发件人、路由等信息的电子邮件

1571 垃圾邮件带来的危害有\_\_\_\_。

A 垃圾邮件占用很多互联网资源 B 垃圾邮件浪费广大用户的时间和精力 C 垃圾邮件提高了某些公司做广告的效益D 垃圾邮件成为病毒传播的主要途径 E 垃圾邮件迫使企业使用最新的操作系统

1572 网页防篡改技术包括\_\_\_\_。

A 网站采用负载平衡技术 B 防范网站、网页被篡改 C 访问网页时需要输入用户名和口令 D 网页被篡改后能够自动恢复 E 采用HTTPS协议进行网页传输

1573 网络钓鱼常用的手段有\_\_\_\_。

A 利用垃圾邮件 B 利用假冒网上银行、网上证券网站 C 利用虚假的电子商务 D 利用计算机病毒 E 利用社会工程学

1574 内容过滤的目的包括\_\_\_\_。

A 阻止不良信息对人们的侵害 B 规范用户的上网行为，提高工作效率 C 防止敏感数据的泄漏 D 遏制垃圾邮件的蔓延E 减少病毒对网络的侵害

1575 下面技术为基于源的内容过滤技术的是\_\_\_\_。

A 内容分级审查 B DNS过滤 C IP包过滤 D URL过滤 E 关键字过滤技术

1576 内容过滤技术的应用领域包括\_\_\_\_。

A 防病毒 B 网页防篡改 C 防火墙 D 入侵检测 E 反垃圾邮件

1．以下厂商为电子商务提供信息产品硬件的是\_\_\_C\_\_\_\_

A. AOL

B．YAHOO

C．IBM

D．MICROSOFT

2．把明文变成密文的过程，叫作\_\_A\_\_\_\_\_

A.加密

B．密文

C．解密

D．加密算法

3．以下加密法中属于双钥密码体制的是\_\_D\_\_\_\_\_

A．DES

B．AES

C．IDEA

D．ECC

4．MD-4散列算法，输入消息可为任意长，按\_\_\_A\_\_\_\_比特分组。

A．512

B．64

C．32

D．128

5．SHA算法中，输入的消息长度小于264比特，输出压缩值为\_\_\_\_C\_\_\_比特。

A．120

B．140

C．160

D．264

6.计算机病毒最重要的特征是\_\_\_B\_\_\_\_

A．隐蔽性

B．传染性

C．潜伏性

D．表现性

7．主要用于防火墙的VPN系统，与互联网密钥交换IKE有关的框架协议是\_\_A\_\_\_\_\_

A．IPSec

B．L2F

C．PPTP

D．GRE

8．Access VPN又称为\_\_\_A\_\_\_\_

A．VPDN

B．XDSL

C．ISDN

D．SVPN

9．以下不是接入控制的功能的是\_\_\_\_B\_\_\_

A．阻止非法用户进入系统

B．组织非合法人浏览信息

C．允许合法用户人进入系统

D．使合法人按其权限进行各种信息活动

10.在通行字的控制措施中，限制通行字至少为\_\_\_B\_\_\_\_字节以上。

A．3～6

B．6～8

C．3～8

D．4～6

11.用数字办法确认、鉴定、认证网络上参与信息交流者或服务器的身份是指\_\_\_B\_\_\_\_

A．接入控制

B．数字认证

C．数字签名

D．防火墙

12．关于密钥的安全保护下列说法不正确的是\_\_\_\_A\_\_\_

A．私钥送给CA

B．公钥送给CA

C．密钥加密后存人计算机的文件中

D．定期更换密钥

13. \_\_\_D\_\_\_\_在CA体系中提供目录浏览服务。

A．安全服务器

B．CA服务器

C．注册机构RA

D．LDAP服务器

14. Internet上很多软件的签名认证都来自\_\_\_D\_\_\_\_公司。

A．Baltimore

B．Entrust

C．Sun

D．VeriSign

15.目前发展很快的安全电子邮件协议是\_\_\_C\_\_\_\_ ，这是一个允许发送加密和有签名邮件的

协议。\_\_\_\_\_\_\_

A．IPSec

B．SMTP

C．S/MIME

D．TCP/1P

16.实现源的不可否认业务中，第三方既看不到原数据，又节省了通信资源的是\_\_\_C\_\_\_\_

A.源的数字签字

B．可信赖第三方的数字签字

C．可信赖第三方对消息的杂凑值进行签字

D．可信赖第三方的持证

17. SET的含义是\_\_\_B\_\_\_\_

A．安全电子支付协议

B．安全数据交换协议

C．安全电子邮件协议

D．安全套接层协议

18. 对SET软件建立了一套测试的准则。\_\_A\_\_\_\_\_

A．SETCo

B．SSL

C．SET Toolkit

D．电子钱包

19．CFCA认证系统的第二层为\_\_\_B\_\_\_\_

A．根CA

B．政策CA

C．运营CA

D．审批CA

20. SHECA提供了\_\_\_\_A\_\_\_种证书系统。

A．2

B．4

C．5

D．7

1. 信息安全受到的威胁有人为因素的威胁和非人为因素威胁，非人为因素的威胁包括　自然灾害　　　、　　系统故障　　、　技术缺陷　　。

2. 广义的信息安全是指网络系统的　　硬件　　、　软件　　及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，　网络服务　　　不中断，系统中的信息不因偶然的或恶意的原因而遭到　破坏　　　、　　更改　　和　　泄露　　　。

3. 密码学是一门关于　信息加密　　和　　密文破译　　的科学，包括　密码编码学　　　和 密码分析学 两门分支。

4. 信息隐藏技术的4个主要分支是　隐写术　　　、　隐通道　　、　匿名通信　　和　版权标识　　。

1. 信息安全的狭义解释

指信息内容的安全，包括信息的保密性、真实性和完整性。

2. 密码系统

指用于加密和解密的系统。

3. 数字水印

在数字化的信息载体中嵌入不明显的记号隐藏起来，被嵌入的信息包括作品的版权所有者、发行者、购买者、作者的序列号、日期和有特殊意义的文本等。60

4. 消息认证码MAC

MAC就是带密钥的消息摘要函数或称为一种带密钥的数字指纹，它与普通的摘要函数是有本质区别的。

1. 简述数字签名的基本原理?

数字签名包含两个过程：签名过程和验证过程。由于从公开密钥不能推算出私有密钥，因此公开密钥不会损害私有密钥的安全性；公开密钥无需保密，可以公开传播，而私有密钥必须保密。因此若某人用其私有密钥加密消息，并且用其公开密钥正确解密，就可肯定该消息是某人签名的。因为其他人的公开密钥不可能正确解密该加密过的消息，其他人也不可能拥有该人的私有密钥而制造出该加密过的消息，这就是数字签名的原理。

2. 数据备份的种类有哪些？常用的方法有哪些？？

数据备份按照备份时所备份数据的特点可以分为三种：完全备份、增量备份和系统备份。根据数据备份所使用的存储介质种类可以将数据备份方法分成如下若干种：软盘备份、磁带备份、可移动存储备份、可移动硬盘备份、本机多硬盘备份和网络备份。

3. 简述密码策略和帐户策略？

账户策略定义在计算机上，然而却可以影响用户账户与计算机或域交互作用的方式。账户策略在安全区域有如下内容的属性。

（1）密码策略：对于域或本地用户账户，决定密码的设置，如强制性和期限。

（2）账户锁定策略：对于域或本地用户账户，决定系统锁定账户的时间以及锁定哪个账户。

（3）Kerberos策略：对于域用户账户，决定于Kerberos有关的设置，如账户有效期和强制性。

密码策略包含6个策略，及密码必须符合复杂性要求、密码长度最小值、密码最长存留期、密码最短存留期、强制密码历史、为域中所有用户使用可还原的加密来存储密码。

4. 简述Web安全目标及技术？。

Web安全目标是保护Web服务器及其数据的安全、保护Web服务器和用户之间传递信息的安全、保护终端用户计算机及其他人连入Internet的设备的安全。Web安全技术主要包括Web服务器安全技术、Web应用服务安全技术和Web浏览器安全技术。

5. 例举几种常见的攻击实施技术。

社会工程学攻击、口令攻击、漏洞攻击、欺骗攻击、拒绝服务攻击等。

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UPDATE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

X 1.《互联网上网服务营业场所管理条例》规定，可以在居民住宅楼（院）内设立互联网上网服务营业场所。

对 2.未经许可，任何组织和个人不得擅自设立互联网上网服务营业场所和从事互联网上网服务经营活动。

X 3.《互联网上网服务营业场所管理条例》规定，对文化行政部门经审查不符合条件的，或者公安机关经审核不合格的，以口头通知的形式向申请人说明理由。

X 4.《互联网上网服务营业场所管理条例》规定，申请人取得《网络文化经营许可证》后即可开业。

X 5.当互联网上网服务营业场所经营单位终止经营活动时，可以出租、出借或者以其他方式转让《网络文化经营许可证》。

对 6.互联网上网服务营业场所经营单位不的涂改《网络文化经营许可证》。

对 7.互联网上网服务营业场所经营单位变更营业场所地址应当经原审核机关同意。

X 8.互联网上网服务营业场所经营单位对营业场所进行改建、扩建，不用再经原审核机关同意。

X 9.互联网上网服务营业场所经营单位变更计算机数量，不用再经原审核机关同意。

对 10.互联网上网服务营业场所经营单位和上网消费者不得利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用我国法律、法规中所明确禁止的有害信息的内容。

对 11.互联网上网服务营业场所经营单位必须以固定网络地址的方式接入互联网。

对 12.互联网上网服务营业场所经营单位提供上网消费者使用的计算机必须通过局域网的方式接入互联网。

X 13.互联网上网服务营业场所经营单位为了吸引消费者可以经营非网络游戏。

X 14.互联网上网服务营业场所经营单位和上网消费者只可以在场所内通过网络游戏进行赌博或者变相赌博。

对 15.互联网上网服务营业场所经营单位发现上网消费者有违法行为时，应当立即予以制止并向文化行政部门、公安机关举报。

对 16.互联网上网服务营业场所经营单位不得接纳未成年人进入营业场所。

X 17.互联网上网服务营业场所经营单位只有在节假日时才可以接纳未成年人进入营业场所。

X 18.互联网上网服务营业场所经营单位只有在法定监护人的陪同下才能接纳未成年人进入营业场所。

X 19.互联网上网服务营业场所经营单位对上网消费者的登记内容和上网记录备份。在保存期内对不需要的内容可以由经营单位修改或者删除。

对 20.互联网上网服务营业场所经营单位对上网消费者的登记内容和上网记录备份。在文化行政部门、公安机关依法查询时予以提供。

对 21.互联网上网服务营业场所经营单位应当依法履行信息安全职责，不得擅自停止实施安全技术措施。

X 22.文化等有关主管部门的工作人员在不影响工作的前提下，可以从事或者变相从事互联网上网服务经营活动。

X 23.文化等有关主管部门的工作人员在不属于自己管辖的区域内，可以参与或者变相参与互联网上网服务经营活动。

X 24.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，被吊销《网络文化经营许可证》的，其法定代表人或者主要负责人可以在近期重新担任互联网上网服务营业场所经营单位的法定代表人或者主要负责人。

X 25.单位、个人可以擅自挪用、拆除、停用消防设施、器材。

对 26.单位、个人不得埋压、圈占消火栓，不得占用防火间距，不得堵塞消防通道。

对 27.禁止接纳未成年人进入网吧等互联网上网服务营业场所是经营单位的禁止行为之一。

对 28.建立并落实互联网上网服务营业场所信息安全管理制度是信息安全管理的基础和前提，是互联网上网服务营业场所安全管理的保障。

对 29.互联网上网服务营业场所实行上网登记制度对维护国家的信息网络安全、打击计算机犯罪有着重大的意义。

对 30.互联网上网服务营业场所场内巡查与情况报告制度是为维护互联网上网服务营业场所安全、信息网络安全及在巡查中发现违法犯罪行为时及时予以制止和报告而制定的安全管理制度。

对 31.实名登记子系统，是指互联网上网服务营业场所经营单位根据上网消费者出示的有效证件中的相关信息进行如实记录的安全管理系统。

对 32.互联网上网服务营业场所安全管理子系统是以记录并留存计算机信息系统运行日志信息为主，并集过滤封堵非法网站、通知汇报等管理功能于一体的安全管理系统。

对 33.互联网上网服务营业场所作为提供上网服务的公共场所，落实计算机防毒的技术措施是非常必要的。

X 34.互联网上网服务营业场所是作为提供上网服务的营利场所，没必要落实计算机防毒的技术措施。

对 35.行政处罚，是指法定的行政机关或其他主体依法追究公民、法人或者其他组织违反行政管理秩序行为的行政法律责任而实施的法律制裁。

对 36.行政处罚决定程序中的一般程序下列基本步骤：立案、调查取证、提出行政处罚意见、说明理由和告之权利、当事人陈述和申辩、听证、作出处罚决定并制作处罚决定书、送达。

对 37.电信部门负责对互联网上网服务营业场所经营单位的信息网络安全的监督管理。

对 38.火灾预防是消防工作的重点，也是基础。

对 39.消防安全责任由单位的主要负责人对本单位的消防安全工作负责。

X 40.违反治安管理处罚法所引起的责任是一种法律责任。

对 41.18周岁以上属于完全责任年龄时期，需要对自己的行为严格控制。

对 42.公共秩序，是指在社会生活中，由法律、法规和机关、团体、企业、事业单位的规章制度等组成的规范。

对 43.扰乱公共秩序的行为，是指故意扰乱公共秩序，尚不够刑事处罚，依据治安管理处罚法应当给予治安管理处罚的行为。

对 44.公安机关对于不履行治安法规所确定的义务或者危及社会治安秩序，情节轻微，尚不够刑事处罚的行为，依照治安管理法规的规定实施治安行政处罚。

对 45.消防行政处罚是国家特定消防行政机关依法惩戒违反行政管理秩序的个人、组织的一种行政行为。

对 46.消防监督检查人员在进行监督检查时，应当着制式警服，并出示《公安消防监督检查证》。

X 47.学校、图书馆等单位内部附设的为特定对象获取资料、信息提供上网服务的场所属于互联网上网服务营业场所。

对 48.《互联网上网服务营业场所管理条例》规定设立互联网上网服务营业场所经营单位，应当采用企业的组织形式。

2008-07-26 11:08

• 评论(已有0条)

• 阅读全文

•

•

多选

三、多选题

1.公安机关负责对互联网上网服务营业场所经营单位的\_ACD\_的监督管理。

A.网络安全 B.计算机硬件设备安全

C.治安安全 D.消防安全

2.设立互联网上网服务营业场所经营单位，至少要具备下列条件：\_ABCD\_\_。

A.有与其经营活动相关的并符合国家规定的消防安全条件的营业场所。

B.有健全、完善的信息网络安全管理制度和安全技术措施

C.有固定的网络地址和与其经营活动相适应的计算机上等装置及附属设备

D.有与其经营活动相适应并取得从业资格的安全管理人员、经营管理人员、专业技术人员

3.设立互联网上网服务营业场所经营单位，应当向县级以上地方人民政府文化行政部门提出申请，并至少提交下列文件：\_\_ABCD\_\_。

A.名称预先核准通知书和章程 B.法定代表人或者主要负责人的身份证明材料

C.资金信用证明 D.营业场所产权证明或者租赁异香书

4.《互联网上网服务营业场所管理条例》规定，申请人完成筹建后，持同意筹建的批准文件到同级公安机关摄取\_\_B\_\_\_和\_\_D\_\_\_审核。

A.电脑安全 B信息网络安全 C.电力安全 D.消防安全

5.互联网上网服务营业场所经营单位变更名称、住所、法定代表人或者主要负责人、注册资本、网络地址或者终止经营活动的，应当依法到\_ABD\_办理相关手续。

A.工商行政管理部门 B.公安机关

C.通信管理部门 D.文化行政部门

6.互联网上网服务营业场所经营单位和上网消费者不得进行\_BCD\_危害信息网络安全的活动。

A.在BBS上留言或利用QQ聊天

B.故意制作或者传播计算机病毒以及其他破坏性程序

C.非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序

D.进行法律、行政法规禁止的其他活动

7.互联网上网服务营业场所经营单位应当在营业场所的显著位置悬挂\_\_BD\_\_\_。

A.网络游戏许可证 B.工商营业执照

C.计费系统使用证 D.《网络文化经营许可证》

8.《互联网上网服务营业场所管理条例》规定，互联网上网服务营业场所经营单位应当依法履行消防安全职责，并遵守\_ABCD\_规定。

A.禁止明火照明和吸烟并悬挂禁止吸烟标志

B.禁止带入和存放易燃、易爆物品

C.不得安装固定的封闭门窗栅栏

D.营业期间禁止封堵或者锁闭门窗、安全疏散通道和安全出口

9.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，涂改、出租、出借或者以其他方式转让《网络文化经营许可证》，尚不够刑事处罚的，应接受\_BCD\_处罚。

A.没收计算机及各种上网设备

B.吊销《网络文化经营许可证》，没收非法所得

C.违法经营额5000元以上的，并处违法金额2倍以上5倍以下的罚款

D.违法经营额不足5000元的，并处5000元以上10000元以下的罚款

10.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，利用营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用含有《互联网上网服务营业场所管理条例》规定禁止含有的内容的信息，尚不够刑事处罚的，应该受\_\_ABCD\_\_处罚。

A.公安机关给予警告，没收违法所得

B.违法金额1万元以上的，并处违法金额2倍以上5倍以下的罚款

C.违法金额不足1万元的，并处1万元以上2万元以下的罚款

D.情节严重的，责令停业整顿，直至吊销《网络文化经营许可证》

11.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，有下列\_\_ABCD\_\_行为，情节严重的，责令停业整顿，直至吊销《网络文化经营许可证》。

A.接纳未成年人进入营业场所的

B.经营非网络游戏的

C.擅自停止实施经营管理技术措施的

D.未悬挂《网络文化经营许可证》或者未成年人禁入标志的

12.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，有下列\_ACD\_\_行为，情节严重的，责令停业整顿，直至吊销《网络文化经营许可证》。

A.利用明火照明 B.喝酒、打扑克牌

C.发现吸烟不予制止 D.未悬挂禁止吸烟标志

13.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，有下列\_\_ACD\_\_行为，情节严重的，责令停业整顿，直至吊销《网络文化经营许可证》。

A.允许带入或者存放易燃、易爆物品

B.上网游戏或聊天

C.在营业场所安装固定的封闭门窗栅栏

D.营业期间封堵或者锁闭门窗、安全疏散通道或者安全出口

14.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，有下列\_\_ACD\_\_\_行为，由公安机关给予警告，可以并处15000元以下罚款。

A.允许带入或者存放易燃、易爆物品

B.擅自出售QQ帐号

C.在营业场所安装固定的封闭门窗栅栏

D.营业期间封堵或者锁闭门窗、安全疏散通道或者安全出口

15.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》规定，有下列\_\_ACD\_\_\_行为，由公安机关给予警告，可以并处15000元以下罚款。

A.利用明火照明 B.喝酒、打扑克牌

C.发现吸烟不予制止 D.未悬挂禁止吸烟标志

16.对违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处\_CD\_\_。

A.5年以下有期徒刑 B.拘留

C.3年以下有期徒刑 D.拘役

17.多次发送淫秽、侮辱、恐吓或者其他信息，干扰他人正常生活，情节较重的，处\_\_BC\_\_。

A.5日以上15日以下拘留 B.可以并处500元以下罚款

C.5日以上10日以下拘留 D.可以并处1000元以下罚款

18.公然侮辱他人或者捏造事实诽谤他人，情节较重的，处\_AB\_\_。

A.5日以上10日以下拘留 B.可以并处500元以下罚款

C.5日以上15日以下拘留 D.可以并处1000元以下罚款

19.写恐吓信或者以其他方法威胁他人人身安全，情节较重的，处\_AD\_\_。

A.5日以上10日以下拘留 B.可以并处1000元以下罚款

C.10日以上15日以下拘留 D.可以并处500元以下罚款

20.下列\_AD\_行为，情节较重的，可以处5日以上10日以下拘留可以并处500元以下罚款。

A.偷窥、偷拍、窃听、散布他人隐私的

B.未经他人允许向其发送邮件的

C.利用手机向他人发送短信息的

D.捏造事实诬告陷害他人，企图使他人受到刑事追究或者受到治安管理处罚的

21.制作、运输、复制、出售、出租淫秽的书刊、图片、影片、音像制品等淫秽物品或者利用计算机信息网络、电话以及其他通讯工具传播淫秽信息的，处\_CD\_\_。

A.15日以上20日以下拘留 B.可以并处1000元以下罚款

C.10日以上15日以下拘留 D.可以并处3000元以下罚款

22.违反治安管理行为的处罚包含下列三种：\_\_ABD\_\_\_\_。

A.警告 B.罚款 C.劳教 D.行政拘留

23.机关、团体、企业、事业单位应当履行下列\_ABCD\_\_消防安全职责。

A.制定消防安全制度、消防安全操作规程

B.实行防火安全责任制，确定本单位和所属各部门、岗位的消防安全责任人

C.按照国家有关规定配置消防设施和器材、设置消防安全标志，并定期组织检验、维修，确保消防设施和器材完好、有效。

D.保障疏散通道、安全出口畅通，并设置符合国家规定的消防安全疏散标志

24.互联网上网服务营业场所有下列\_\_BCD\_\_行为，责令限期改正；逾期不改正的，责令停产停业，可以并处罚款，并对其直接负责的主管人员和其他直接责任人员处罚款。

A.允许未成年人进入场所的

B.对火灾隐患不及时消除的

C.不按照国家相关规定，配置消防设施和器材的

D.不能保障疏散通道、安全出口畅通的

25.违反消防法的规定，有下列\_ABC\_\_行为，处警告或者罚款。

A.指使或者强令他人违法消防安全规定，冒险作业，尚未造成严重后果的

B.埋压、圈占消火栓或者占用防火间距、堵塞消防通道的，或者损坏和擅自挪用、拆除、停用消防设施、器材的

C.有重大火灾隐患，经公安消防机构通知逾期不改正的

D.其他

26.计算机病毒，是指编制或者在计算机程序中插入的\_B\_或者\_C\_\_，影响计算机上使用，并能自我复制的一组计算机指令或者程序代码。

A.危害操作人员健康 B.破坏计算机功能

C.毁坏数据 D.破坏机房环境安全

27.下列行为中，\_\_ABCD\_\_是《计算机信息网络国际联网安全保护管理办法》所不允许利用国际联网进行的活动。

A.危害国家安全的行为

B.泄露国家秘密的行为

C.侵犯国家的、社会的、集体的利益的行为

D.侵犯公民的合法权益的行为

28.任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：\_\_ABCD\_\_。

A.煽动抗拒、破坏宪法和法律、行政法规实施的；煽动颠覆国家政权，推翻社会主义制度的

B.煽动分裂国家、破坏国家统一的；煽动民族仇恨、民族歧视，破坏民族团结的

C.捏造或者歪曲事实、散布谣言，扰乱社会秩序的；公然侮辱他人或者捏造事实诽谤他人的

D.宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；其他违反宪法和法律、行政法规的

29.下列哪些是互联网提供的功能：\_ABCD\_\_。

A.E-mail B.bbs C.FTP D.www

30.互联网上网服务营业场所存在的主要安全问题是：\_BCD\_。

A.上网消费者过于集中的问题 B.消防安全问题

C.信息网络安全问题 D.治安问题

31.互联网上网服务营业场所的安全管理应该包括以下\_\_ABCD\_\_层次的管理。

A.政府职能部门应依法对互联网上网服务营业场所行使有效的监督、检查和管理

B互联网上网服务营业场所经营单位及从业人员加强法律法规意识，严格守法经营

C.上网消费者必须严格遵守国家的有关法律、法规的规定，文明上网

D.建立广泛的社会监督机制及长效管理体制

32.互联网上网服务营业场所经营单位的禁止行为包括：\_ABCD\_\_。

A.禁止利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播国家法律、法规所禁止的有害信息的行为；禁止利用互联网上网服务营业场所侵犯用户的通信自由、通信秘密等涉及个人隐私的行为

B.禁止擅自停止实施安全技术措施的行为；禁止在互联网上网服务营业场所从事破坏网络安全的各种行为

C.禁止在互联网上网服务营业场所内使用盗版产品等侵犯知识产权的行为；禁止利用互联网上网服务营业场所进行赌博和变相赌博行为

D.禁止接纳未成年人进入互联网上网服务营业场所的行为

33.互联网上网服务营业场所经营单位承担的责任应该包括：\_\_ABCD\_\_\_。

A.维护场所安全的责任 B.维护国家安全的责任

C.维护社会秩序的责任 D.提高自身素质、加强行业自律、宣讲文明上网

34.互联网上网服务营业场所经营单位的责任具体体现在\_ABCD\_\_。

A.接受公安机关的监督、检查和指导；建立并落实各项互联网上网服务营业场所安全管理制度

B.配备相应的网络安全管理技术人员；采取必要的安全技术保护措施

C.正确引导上网消费者的上网行为；发现有网络和其他违法犯罪行为的要及时制止并向主管部门举报

D.禁止接纳未成年人进入互联网上网服务营业场所；法律、法规中对经营单位规定的其他责任

35.互联网上网服务营业场所的安全管理制度，应该包括哪些基本制度：\_ABCD\_\_。

A.审核登记制度 B.场内巡查与情况报告制度

C.上网登记制度 D.信息安全培训制度

36.巡查人员在巡查过程中要做到\_\_ABCD\_\_\_。

A.正确引导上网人员的上网行为，积极鼓励、宣传健康、文明的网络行为

B.给上网人员提供各种相关的技术支持和帮助

C.发现各种违法犯罪行为要给予制止并及时向公安机关举报

D.东西各种安全隐患要及时加以排除，疏导上网人员撤离现场并向公安等有关主管部门报告

37.目前在互联网上网服务营业场所中实施的安全技术措施主要针对的是\_BD\_\_。

A.信息安全管理系统 B.有害信息防治

C.入侵检测 D.计算机病毒防治

38.以下\_\_ABCD\_\_是我国行政处罚规定的行政处罚所包含的种类

A.警告 B.罚款 C.没收违法所得、没收非法财物 D.行政拘留

39.对违反行政管理秩序的公民、法人或者其他组织，将要作出\_\_BCD\_\_的行政处罚之前，行政处罚机关应制作《违法行为处理通知书》，并送达当事人。

A.警告 B.较大数额罚款 C.责令停产停业 D.暂扣或者吊销许可证

40.《互联网上网服务营业场所管理条例》第24条规定，互联网上网服务营业场所经营单位应当依法履行信息网络安全、治安和消防安全职责，并遵守下列规定：ABCDE\_。

A.禁止明火照明和吸烟并悬挂禁止吸烟标志

B.禁止带入和存放易燃、易爆物品

C.不得安装固定的封闭门窗栅栏

D.营业期间禁止封堵或者锁闭门窗、安全疏散通道和安全出口

E.不得擅自停止实施安全技术措施

41.电气线路引起火灾的主要原因是\_ABCD\_\_。

A.超负荷 B.短路或者接触不良

C.断路造成相间电压不平衡 D.电脑、空调、电取暖器自身故障

42.互联网上网服务营业场所经营单位违反《互联网上网服务营业场所管理条例》的规定，有下列\_\_ABCDE\_\_\_行为之一的，由公安机关给予警告，可以并处15000元以下的罚款；情节严重的，责令停业整顿，直至由文化行政部门吊销《网络文化经营许可证》。

A.利用明火照明或者发现吸烟不予制止，或者未悬挂禁止吸烟标志的

B.允许带入和存放易燃、易爆物品的

C.在营业场所安装固定的封闭门窗栅栏的

D.营业期间封堵或者锁闭门窗、安全疏散通道和安全出口的

E.擅自停止实施安全技术措施的

43.互联网上网服务营业场所（网吧）需接受\_ABCE\_\_的监管。

A.公安机关 B.文化行政部门 C.工商行政管理部门

D.交通部门 E.电信部门

44.治安管理处罚法处罚的种类主要分为\_ABCD\_\_\_。

A.警告 B.罚款 C.行政拘留 D.吊销公安机关发放的许可证

45.违反治安管理的行为和处罚主要分为\_ABCD\_\_\_。

A.扰乱公共秩序的行为和处罚 B.妨害公共安全的行为和处罚

C.侵犯人身权利、财产权利的行为和处罚 D.妨害社会管理的行为和处罚

46.营业性场所有下列行为之一的，责令限期改正；逾期不改正的责令停产停业，可以并处罚款，并对其直接负责的主管人员和其他责任人员处罚款：\_ACD\_\_。

A.对火灾隐患不及时消除的

B.未设置业余消防人员

C.不按照国家有关规定、配置消防设施和器材的

D.不能保障疏散通道、安全出口畅通的

47.物质燃烧应具备三个必要条件：\_\_ABD\_。

A.可燃物 B.助燃物 C.空气 D.点火源

48.基本灭火方法有\_ABC\_\_\_。

A.隔离法 B.窒息灭火法 C.冷却灭火法 D.抑制灭火法

49.在治安管理处罚法中规定了以下违反治安管理的行为和罚责：\_ABCD\_\_\_。

A.扰乱公共秩序的行为和罚责 B.妨害公共安全的行为和罚责

C.侵犯人身权利、财产权利的行为和罚责 D.妨害社会管理的行为和罚责

50.根据现行消防法规规定，消防行政处罚主要包括\_ABC\_\_、没收产品和违法所得、吊销许可证、责令停产停业（责令停止施工、责令停止使用）。

A.警告 B.罚款 C.行政拘留 D.训诫

51.互联网上网服务营业场所经营单位，应当履行下列义务：\_ABCD\_\_.

A.落实网络信息安全管理措施；制止、举报利用其营业场所从事法律、行政法规明令禁止的行为

B.在核准的经营范围内提供服务；在营业场所的显著位置悬挂《网络文化经营许可证》和营业执照

C.记录有关上网信息，记录备份保存时间不得少于60日，并在有关部门依法查询时予以提供；不得擅自出租、转让营业场所或者接入线路

D.不得经营含有色情、赌博、暴力、愚昧迷信等不健康内容的电脑游戏；不得接纳未成年人进入营业场所

52.互联网上网服务营业场所经营单位和上网消费者不得进行下列危害信息网络安全的活动：\_ABCD\_。

A.非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序

B.故意制作或者传播计算机病毒以及其他破坏性程序

C.行政法规禁止的其他行为

D.法律禁止的其他行为

53.互联网上网服务营业场所经营单位和上网消费者不得利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用含有下列内容的信息：\_\_ABCD\_\_\_。

A.反对宪法确定的基本原则的；危害国家统一、主权和领土完整的；泄露国家秘密，危害国家安全或者损害国家荣誉和利益的

B.煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的

C.破坏国家宗教政策，宣扬邪教、迷信的；散布谣言，扰乱社会秩序，破坏社会稳定的；宣传淫秽、赌博、暴力或者教唆犯罪的

D.侮辱或者诽谤他人，侵害他人合法权益的；含有法律、行政法规禁止的其他内容的

信息安全试题（1/共3）

单项选择题（每小题2分，共20分）

1．信息安全的基本属性是＿＿＿。

A. 保密性 B.完整性

C. 可用性、可控性、可靠性 D. A，B，C都是

2．假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于＿＿＿。

A. 对称加密技术 B. 分组密码技术

C. 公钥加密技术 D. 单向函数密码技术

3．密码学的目的是＿＿＿。

A. 研究数据加密 B. 研究数据解密

C. 研究数据保密 D. 研究信息安全

4．A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送数字签名M，对信息M加密为：M’= KB公开（KA秘密（M））。B方收到密文的解密方案是＿＿＿。

A. KB公开（KA秘密（M’）） B. KA公开（KA公开（M’））

C. KA公开（KB秘密（M’）） D. KB秘密（KA秘密（M’））

5．数字签名要预先使用单向Hash函数进行处理的原因是＿＿＿。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

6．身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是＿＿。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

7．防火墙用于将Internet和内部网络隔离＿＿＿。

A. 是防止Internet火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

8．PKI支持的服务不包括＿＿＿。

A. 非对称密钥技术及证书管理 B. 目录服务

C. 对称密钥的产生和分发 D. 访问控制服务

9．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0.5，则k约等于＿＿。

A．2128 B．264

C．232 D．2256

10．Bell-LaPadula模型的出发点是维护系统的＿＿＿，而Biba模型与Bell-LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

填空题（每空1分，共20分）

1．ISO 7498-2确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。同时，ISO 7498-2也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。

2．古典密码包括 代替密码和置换密码两种，对称密码体制和非对称密码体制都属于现代密码体制。传统的密码系统主要存在两个缺点：一是 密钥管理与分配问题 ；二是 认证问题 。在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3．根据使用密码体制的不同可将数字签名分为 基于对称密码体制的数字签名 和 基于公钥密码体制的数字签名 ，根据其实现目的的不同，一般又可将其分为 直接数字签名 和 可仲裁数字签名 。

4. DES算法密钥是64位，其中密钥有效位是56位。RSA算法的安全是基于分解两个大素数的积的困难。

5．密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式有两种：一种是由中心集中生成，另一种是由个人分散生成。

6．认证技术包括站点认证、报文认证和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、生理特征识别、零知识证明。

7．NAT的实现方式有三种，分别是静态转换、动态转换、端口多路复用。

8．数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

计算题（每小题8分，共24分）

用置换矩阵Ek=〔〕对明文Now we are having a test加密，并给出其解密矩阵及求出可能的解密矩阵总数。

解：设明文长度L=5，最后一段不足5则加字母x，经过置换后，得到的密文为 Wnewo haaer gvani ttxse

其解密矩阵为

Dk=〔〕

L=5时可能的解密矩阵总数为 5！= 120

DES的密码组件之一是S盒。根据S盒表计算S3(101101)的值,并说明S函数在DES算法中的作用。

解：令101101的第1位和最后1位表示的二进制数为i，则i=(11)2=(3)10

令101101的中间4位表示的二进制数为j，则j=(0110)2=(6)10

查S3盒的第3行第6列的交叉处即为8，从而输出为1000

S函数的作用是将6位的输入变为4位的输出

3．求963和657的最大公约数(963, 657)，并表示成963，657的线性组合。

解：运用广义欧几里得除法，有

963=1\*657+306

657=2\*306+45

306=6\*45+36

45=1\*36+9

36=4\*9+0

（根据给出的最后一个定理）则(963, 657)=9

从广义欧几里得除法逐次消去r(n-1),r(n-2), …,r(3),r(2)，即

9=45-1\*36

=45-（306-6\*45）

=7\*45-306

=7\*（657-2\*306）-306

=7\*657-3\*306

=7\*657-3\*（963-657）

=22\*657-15\*963

所以此线性组合为 9=22\*657-15\*963

问答题（每小题7分，共21分）

1．S拥有所有用户的公开密钥,用户A使用协议

A → S：A || B || Ra

S → A: S || Ss(S || A || Ra || Kb)

其中Ss( )表示S利用私有密钥签名

向S申请B的公开密钥Kb。上述协议存在问题吗？若存在，请说明此问题；若不存在，请给出理由。

答：存在。

由于S没有把公钥和公钥持有人捆绑在一起，A就无法确定它所收到的公钥是不是B的，即B的公钥有可能被伪造。如果攻击者截获A发给S的信息，并将协议改成

A → S：A || C || Ra

S收到消息后，则又会按协议

S → A: S || Ss(S || A || Ra || Kc)

将Kc发送给A，A收到信息后会认为他收到的是Kb ，而实际上收到的是Kc ，但是A会把它当作Kb ，因为他无法确认。

请你利用认证技术设计两套系统，一套用于实现商品的真伪查询，另一套用于防止电脑彩票伪造问题。

答：(1)系统产生一随机数并存储此数，然后对其加密，再将密文贴在商品上。当客户购买到此件商品并拨打电话查询时，系统将客户输入的编码(即密文)解密，并将所得的明文与存储在系统中的明文比较，若匹配则提示客户商品是真货，并从系统中删了此明文；若不匹配则提示客户商品是假货。

(2)首先，系统给彩票编好码，习惯称之为条形码；然后，将条形码通过MD5运算，得到相应的消息摘要；接着，对消息摘要进行加密，得到相应密文；最后，系统将条形码与密文绑定在一起并存储，若需要查询时只要查看条形码与密文是否相关联即可。这样，即可实现电脑彩票防伪，因为伪造者是无法伪造密文的。

3．防火墙的实现技术有哪两类？防火墙存在的局限性又有哪些？

答：防火墙的实现从层次上可以分为两类：数据包过滤和应用层网关，前者工作在网络层，而后者工作在应用层。

防火墙存在的局限性主要有以下七个方面

(1) 网络上有些攻击可以绕过防火墙（如拨号）。

(2) 防火墙不能防范来自内部网络的攻击。

(3) 防火墙不能对被病毒感染的程序和文件的传输提供保护。

(4) 防火墙不能防范全新的网络威胁。

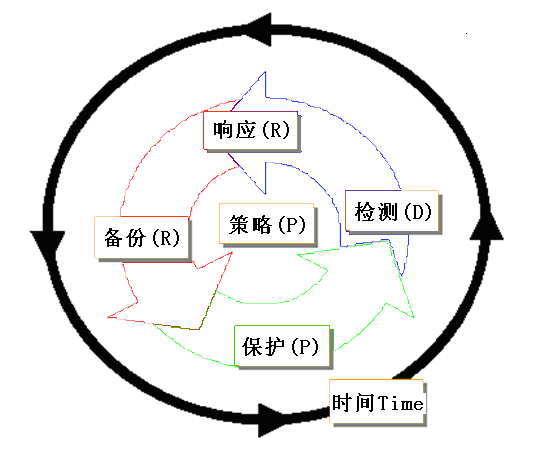
(5) 当使用端到端的加密时，防火墙的作用会受到很大的限制。

(6) 防火墙对用户不完全透明，可能带来传输延迟、瓶颈以及单点失效等问题。

(7) 防火墙不能防止数据驱动式攻击。有些表面无害的数据通过电子邮件或其他方式发送到主机上，一旦被执行就形成攻击（附件）。

分析题（15分）

1．下图表示的是P2DR2动态安全模型，请从信息安全安全角度分析此模型？



答：(主要理解一下黑体字部分，然后按照这个思路自由发挥)

P2DR2动态安全模型研究的是基于企业网对象、依时间及策略特征的（Policy， Protection， Detection，Response，Restore）动态安全模型结构，由策略、防护、检测、响应和恢复等要素构成，是一种基于闭环控制、主动防御的动态安全模型。通过区域网络的路由及安全策略分析与制定，在网络内部及边界建立实时检测、监测和审计机制，采取实时、快速动态响应安全手段，应用多样性系统灾难备份恢复、关键系统冗余设计等方法，构造多层次、全方位和立体的区域网络安全环境。

一个良好的网络安全模型应在充分了解网络系统安全需求的基础上，通过安全模型表达安全体系架构，通常具备以下性质：精确、无歧义；简单和抽象；具有一般性；充分体现安全策略。

P2DR2模型的时间域分析

P2DR2模型可通过数学模型，作进一步理论分析。作为一个防御保护体系，当网络遭遇入侵攻击时，系统每一步的安全分析与举措均需花费时间。设Pt为设置各种保护后的防护时间，Dt为从入侵开始到系统能够检测到入侵所花费的时间，Rt为发现入侵后将系统调整到正常状态的响应时间，则可得到如下安全要求：

Pt >( Dt + Rt)              （1）

由此针对于需要保护的安全目标，如果满足公式（1），即防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前，这种入侵行为就能够被检测到并及时处理。同样，我们假设Et为系统暴露给入侵者的时间，则有

Et=Dt+Rt （如果Pt=0）       （2）

公式（2）成立的前提是假设防护时间为0，这种假设对Web Server这样的系统可以成立。

通过上面两个公式的分析，实际上给出了一个全新的安全定义：及时的检测和响应就是安全，及时的检测和恢复就是安全。不仅于此，这样的定义为解决安全问题给出了明确的提示：提高系统的防护时间Pt、降低检测时间Dt和响应时间Rt，是加强网络安全的有效途径。

图1为P2DR2 安全模型的体系结构。在P2DR2动态安全模型中，采用的加密、访问控制等安全技术都是静态防御技术，这些技术本身也易受攻击或存在问题。那么攻击者可能绕过了静态安全防御技术，进入系统，实施攻击。模型认可风险的存在，绝对安全与绝对可靠的网络系统是不现实的，理想效果是期待网络攻击者穿越防御层的机会逐层递减，穿越第5层的概率趋于零。

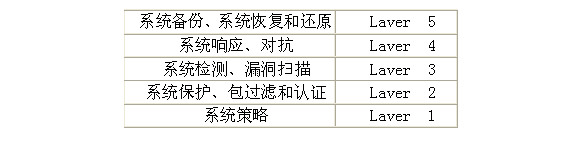


图2 P2DR2 安全模型体系结构

P2DR2模型的策略域分析

网络系统是由参与信息交互的各类实体元素构成，可以是独立计算机、局域网络或大规模分布式网络系统。实体集合可包括网络通信实体集、通信业务类型集和通信交互时间集。

通信实体集的内涵表示发起网络通信的主体，如：进程、任务文件等资源；对于网络系统，表示各类通信设备、服务器以及参与通信的用户。网络的信息交互的业务类型存在多样性，根据数据服务类型、业务类型，可以划分为数据信息、图片业务、声音业务；根据IP数据在安全网关的数据转换服务，业务类型可以划分为普通的分组；根据TCP/IP协议传输协议，业务类型可以划分为 ICMP、TCP、UDP分组。信息安全系统根据不同安全服务需求，使用不同分类法则。通信交互时间集则包含了通信事件发生的时间区域集。

安全策略是信息安全系统的核心。大规模信息系统安全必须依赖统一的安全策略管理、动态维护和管理各类安全服务。安全策略根据各类实体的安全需求，划分信任域，制定各类安全服务的策略。

在信任域内的实体元素，存在两种安全策略属性，即信任域内的实体元素所共同具有的有限安全策略属性集合,实体自身具有的、不违反Sa的特殊安全策略属性Spi 。由此我们不难看出，S=Sa+ΣSpi.

安全策略不仅制定了实体元素的安全等级，而且规定了各类安全服务互动的机制。每个信任域或实体元素根据安全策略分别实现身份验证、访问控制、安全通信、安全分析、安全恢复和响应的机制选择。

信息安全试题（2/共3）

名词解释

信息安全：建立在网络基础上的现代信息系统，其安全定义较为明确，那就是：保护信息系统的硬件软件及其相关数据，使之不因偶然或是恶意侵犯而遭受破坏，更改及泄露，保证信息系统能够连续正常可靠的运行。

VPN：一般是指建筑在因特网上能够自我管理的专用网络，是一条穿过混乱的公共网络的安全稳定的隧道。通过对网络数据的封包和加密传输，在一个公用网络建立一个临时的，安全的连接，从而实现早公共网络上传输私有数据达到私有网络的级别。

数字证书：是指各实体（持卡人、个人、商户、企业、网关、银行等）在网上信息交流及交易活动中的身份证明。

选择题

1.、加密算法分为（对称密码体制和非对称密码体制）

2。、口令破解的最好方法是（B）

A暴力破解 B组合破解 C字典攻击 D生日攻击

3、杂凑码最好的攻击方式是（D）

A 穷举攻击 B中途相遇 C字典攻击 D生日攻击

4、可以被数据完整性机制防止的攻击方式是（D）

A假冒\*\*\* B抵赖\*\*\*\* C数据中途窃取 D数据中途篡改

5、会话侦听与劫持技术属于（B）技术

A密码分析还原 B协议漏洞渗透 C应用漏洞分析与渗透 D DOS攻击

6、PKI的主要组成不包括（B）

A CA B SSL C RA D CR

7，恶意代码是（指没有作用却会带来危险的代码D）

A 病毒\*\*\* B 广告\*\*\* C间谍\*\* D 都是

8，社会工程学常被黑客用于（踩点阶段信息收集A）

A 口令获取 B ARP C TCP D DDOS

9，windows中强制终止进程的命令是（C）

A Tasklist B Netsat C Taskkill D Netshare

10，现代病毒木马融合了（D）新技术

A 进程注入 B注册表隐藏 C漏洞扫描 D都是

11，网络蜜罐技术使用于（.迷惑入侵者，保护服务器诱捕网络罪犯 ）

12，利用三次握手攻击的攻击方式是（DOS\DDOS\DRDOS）

13，溢出攻击的核心是（A）

A 修改堆栈记录中进程的返回地址 B利用Shellcode C 提升用户进程权限 D 捕捉程序漏洞

14，在被屏蔽的主机体系中，堡垒主机位于（A）中，所有的外部连接都经过滤路由器到它上面去。

A 内部网络 B周边网络 C外部网络 D自由连接

15，外部数据包经过过滤路由只能阻止（D）唯一的ip欺骗

A 内部主机伪装成外部主机IP B内部主机伪装成内部主机IP

C外部主机伪装成外部主机IP D外部主机伪装成内部主机IP

17，ICMP数据包的过滤主要基于（D）

A目标端口 B 源端口 C消息源代码 D协议prot

18，网络安全的特征包含保密性，完整性（D）四个方面

A可用性和可靠性 B 可用性和合法性 C可用性和有效性 D可用性和可控性

三，简答题

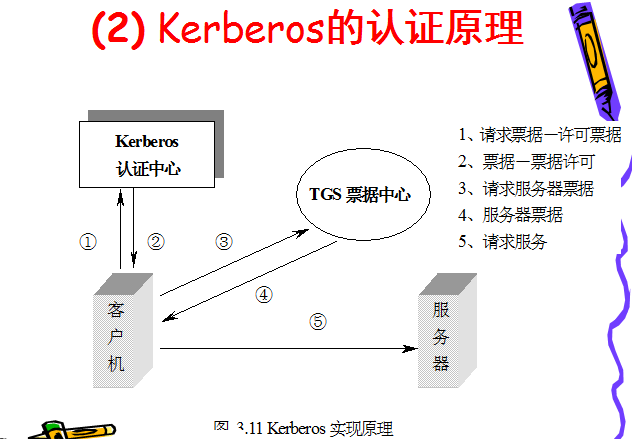
1，信息安全有哪些常见的威胁？信息安全的实现有哪些主要技术措施？

答：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。信息安全的实现可以通过物理安全技术，系统安全技术，网络安全技术，应用安全技术，数据加密技术，认证授权技术，访问控制技术，审计跟踪技术，防病毒技术，灾难恢复和备份技术

2，什么是密码分析，其攻击类型有哪些？DES算法中S盒的作用是什么？

答：密码分析是指研究在不知道密钥的情况下来恢复明文的科学。攻击类型有只有密文的攻击，已知明文的攻击，选择明文的攻击，适应性选择明文攻击，选择密文的攻击，选择密钥的攻击，橡皮管密码攻击。S盒是DES算法的核心。其功能是把6bit数据变为4bit数据。

3，试画图说明kerberos认证原理



4，用户A需要通过计算机网络安全地将一份机密文件传送给用户B，请问如何实现？

如果这份机密文件数据量非常大，B希望A今后对该份机密文件无法抵赖，请问如何实

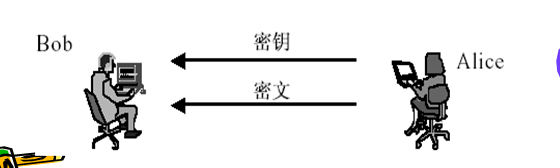
现，试画图说明。

答：（1）假定通信双方分别为Alice和Bob

加密方Alice将商定的密钥秘密地传递给解密方Bob 。

Alice 用商定的密钥加密她的消息，然后传送给Bob。

Bob用Alice传来的密钥解密Alice的消息。



(2)假定通信双方分别为Alice和Bob

Alice和Bob选用一个公开密钥密码系统

Bob将他的公开密钥传送给Alice

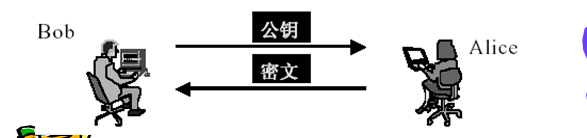
(2)假定通信双方分别为Alice和Bob

Alice和Bob选用一个公开密钥密码系统

Bob将他的公开密钥传送给Alice

Alice用Bob的公开密钥加密她的消息，然后传送给Bob

Bob用他的私人密钥解密Alice的消息。



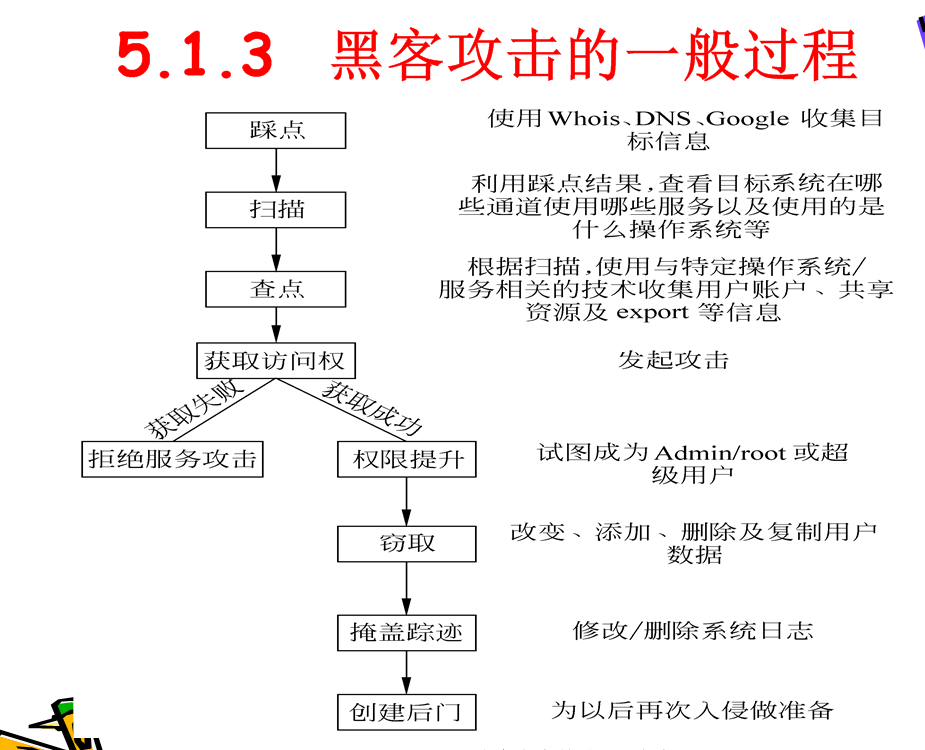
5，防火墙有哪些体系结构？其中堡垒主机的作用是什么？

检测计算机病毒的方法主要有哪些？

答：防火墙的体系结构有屏蔽路由器（Screening Router）和屏蔽主机（Screening Host），双宿主网关（Dual Homed Gateway），堡垒主机（Bastion Host），屏蔽子网（Screened Subnet）防火墙

检测计算机病毒的方法主要有外观检测，特征代码法，系统数据对比法，实时监控法，软件模拟法，检测常规内存数

6，试说明黑客攻击的一般流程及其技术和方法



信息安全试题（3/共3）

1、关于密码学的讨论中，下列（ D ）观点是不正确的。

A、密码学是研究与信息安全相关的方面如机密性、完整性、实体鉴别、抗否认等的综

合技术

B、密码学的两大分支是密码编码学和密码分析学

C、密码并不是提供安全的单一的手段，而是一组技术

D、密码学中存在一次一密的密码体制，它是绝对安全的

2、在以下古典密码体制中，属于置换密码的是（ B）。

A、移位密码 B、倒序密码

C、仿射密码 D、PlayFair密码

3、一个完整的密码体制，不包括以下（ C   ）要素。

A、明文空间 B、密文空间

C、数字签名 D、密钥空间

4、关于DES算法，除了（C ）以外，下列描述DES算法子密钥产生过程是正确的。

A、首先将 DES 算法所接受的输入密钥 K（64 位），去除奇偶校验位，得到56位密钥（即经过PC-1置换，得到56位密钥）

B、在计算第i轮迭代所需的子密钥时，首先进行循环左移，循环左移的位数取决于i的值，这些经过循环移位的值作为下一次循环左移的输入

C、在计算第i轮迭代所需的子密钥时，首先进行循环左移，每轮循环左移的位数都相同，这些经过循环移位的值作为下一次循环左移的输入

D、然后将每轮循环移位后的值经PC-2置换，所得到的置换结果即为第i轮所需的子密钥Ki

5、2000年10月2日，NIST正式宣布将（ B ）候选算法作为高级数据加密标准，该算法是由两位比利时密码学者提出的。

A、MARS B、Rijndael

C、Twofish D、Bluefish

6、根据所依据的数学难题，除了（ A ）以外，公钥密码体制可以分为以下几类。

A、模幂运算问题 B、大整数因子分解问题

C、离散对数问题 D、椭圆曲线离散对数问题

7、密码学中的杂凑函数（Hash函数）按照是否使用密钥分为两大类：带密钥的杂凑函数和不带密钥的杂凑函数，下面（ C ）是带密钥的杂凑函数。

A、MD4 B、SHA-1

C、whirlpool D、MD5

8、完整的数字签名过程（包括从发送方发送消息到接收方安全的接收到消息）包括（C ）和验证过程。

A、加密 B、解密

C、签名 D、保密传输

9、除了（ D ）以外，下列都属于公钥的分配方法。

A、公用目录表 B、公钥管理机构

C、公钥证书 D、秘密传输

10、密码学在信息安全中的应用是多样的，以下（ A ）不属于密码学的具体应用。

A、生成种种网络协议 B、消息认证，确保信息完整性

C、加密技术，保护传输信息 D、进行身份认证

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

二、填空题（每空1分，共20分）

1、信息安全中所面临的威胁攻击是多种多样的，一般将这些攻击分为两大类（主动攻击）和被动攻击。其中被动攻击又分为（消息内容的泄露）和（进行业务流分析）。

2、密码技术的分类有很多种，根据加密和解密所使用的密钥是否相同，可以将加密算法分为：对称密码体制和（非对称密码体制），其中对称密码体制又可分为两类，按字符逐位加密的（序列密码）和按固定数据块大小加密的（分组密码）。

3、密码分析是研究密码体制的破译问题，根据密码分析者所获得的数据资源，可以将密码分析（攻击）分为：（惟密文分析）、已知明文分析（攻击）、（选择明文分析）和选择密文分析（攻击）。

4、古典密码学体制对现代密码学的研究和学习具有十分重要的意义，实现古典密码体制的两种基本方法（代换）和（置换）仍是构造现代对称分组密码的核心方式。

5、（DES）是美国国家标准局公布的第一个数据加密标准，它的分组长度为（64）位，密钥长度为（64（56））位。

6、1976年，美国两位密码学者Diffe和Hellman在该年度的美国计算机会议上提交了一篇论文，提出了（公钥密码体制）的新思想，它为解决传统密码中的诸多难题提出了一种新思路。

7、Elgamal算法的安全性是基于（离散对数问题），它的最大特点就是在加密过程中引入了一个随机数，使得加密结果具有（不确定性），并且它的密文长度是明文长度的（两）倍。该算法的变体常用来进行数据签名。

8、密码系统的安全性取决于用户对于密钥的保护，实际应用中的密钥种类有很多，从密钥管理的角度可以分（初始密钥）、（会话密钥）、密钥加密密钥和（主密钥）。

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

三、简述题（每小题8分，共40分）

古典密码体制中代换密码有哪几种，各有什么特点？

描述说明DES算法的加解密过程（也可以画图说明）。

以DES为例，画出分组密码的密码分组链接（CBC）模式的加密解密示意图，假设加密时明文一个比特错误，对密文造成什么影响，对接收方解密会造成什么影响？

4、简述公钥密码体制的基本思想以及其相对于传统密码体制的优势。

简述数字签名的基本原理及过程。

四、计算题（每题10分，共20分）

计算通过不可约多项式X8+X4+X3+X+1构造的GF（28）上，元素（83）H的乘法逆元。

RSA算法中，选择p=7,q=17,e=13,计算其公钥与私钥，并采用快速模乘（反复平方乘）方法，加密明文m=（19）10。

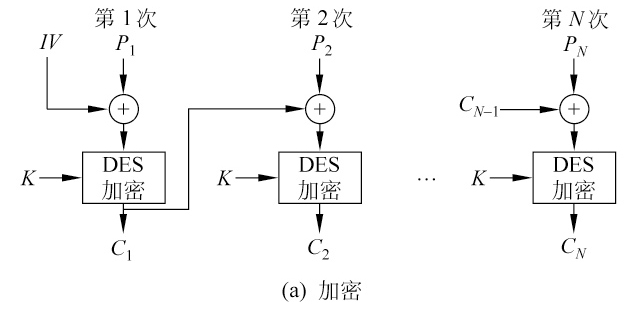
答：在古典密码学中，有四种类型的代替密码：

①简单代替密码（或单表代替密码）（1分），它将明文字母表中的每个字母用密文字母表中的相应字母来代替，明密文表字母存在惟一的一一对应关系，然后通过明密文对照表来进行加解密，容易受到频率统计分析攻击，例如：恺撒密码、仿射密码等（1分）。②多名码代替密码（1分），将明文中的每个字母按一定规律映射到一系列密文字母，这一系列密文字母称为同音字母，它的密文的相关分布会接近于平的，能够较好挫败频率分析，较简单代替密码难破译（1分）。③多字母代替密码（1分），通过一次加密一组字母来使密码分析更加困难，例如Playfair密码（1分）。④多表代替密码（1分），使用从明文字母到密文字母的多个映射，每个映射像简单代替密码中的一一对应，比简单代替密码更安全一些，例如，维吉尼亚密码等（1分）。

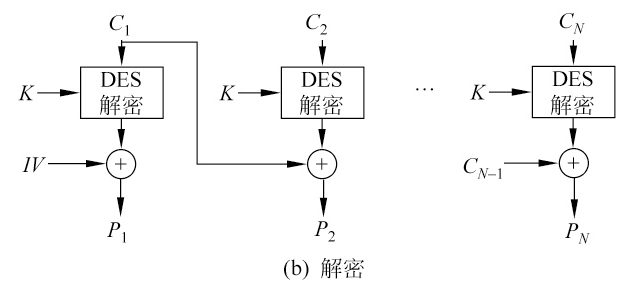
答：DES算法是一个分组加密算法，它以64位分组（0.5分）对数据进行加密，其

初始密钥也是64位，它的加密过程可以描述如下：①64位密钥经子密钥产生算法产生出16个子密钥：K1，K2，…K16，分别供第一次，第二次， …，第十六次加密迭代使用（1分）。②64位明文经初始置换IP（0.5分），将数据打乱重排并分成左右两半。左边为L0，右边为R0： X=L0R0=IP(x)。③16轮（0.5分）轮变换，每轮（第i轮）操作如下：在轮子密钥Ki的控制下，由轮函数f对当前轮输入数据的右半部分Ri-1进行加密：第一步，将Ri-1经过E盒置换扩展成48位（0.5分），第二步，将Ri-1与48位的轮子密钥Ki逐比特异或（0.5分），第三步，对Ri-1进行S盒压缩代换，将其压缩为32位（0.5分），第四步，对Ri-1进行P盒置换（0.5分）。然后，将Ri-1与当前轮输入的左半部分Li-1进行逐比特异或，将该运算结果作为当前轮（第i轮）右半部份的输出Ri=Li-1⊕f(Ri-1,Ki)（0.5分）；将本轮输入的右半部分数据作为本轮输出的左半部分数据：Li=Ri-1（0.5分）。④16轮变换结束后，交换输出数据的左右两部分：X=R16L16（1分）。⑤经过逆初始变换IP-1输出密文（0.5分）。对于DES算法来说，其解密过程与加密过程是同一过程，只不过使用子密钥的顺序相反（1分）。

3、答：因为计算机数据自身的特殊性以及不同场合对于数据加密速度及效率的不同需求，再采用分组对称密码进行数据加密时往往要选择相应的工作模式，密文链接模式（CBC）就是其中的一种。①以DES分组密码为例，CBC模式的加密示意图如下（2分）：



②以DES分组密码为例，CBC模式的解密示意图如下（2分）：



③加密时明文的一个比特错误，会导致该组加密密文发生变化，然后这个错误反馈值会作为下一次DES加密的输入值，再经过DES加密变换。会导致后面的密文都受到影响（2分）。④对于接收方来说，加密明文的一个比特错误，只会影响对应明文块所产生的密文的正常解密，其他数据块可以正常准确地解密（2分）。

4、答：①公钥密码体制的基本思想是把密钥分成两个部分：公开密钥和私有密钥（简称公钥和私钥），公钥可以向外公布，私钥则是保密的（1分）；密钥中的任何一个可以用来加密，另一个可以用来解密（1分）；公钥和私钥必须配对使用，否则不能打开加密文件（1分）；已知密码算法和密钥中的一个，求解另一个在计算上是不可行的（1分）。②相对于传统密码体制来说，公钥密码体制中的公钥可被记录在一个公共数据库里或以某种可信的方式公开发放，而私有密钥由持有者妥善地秘密保存。这样，任何人都可以通过某种公开的途径获得一个用户的公开密要，然后进行保密通信，而解密者只能是知道私钥的密钥持有者（1分），该体制简化了密钥的分配与分发（1分）；同时因为公钥密码体制密钥的非对称性以及私钥只能由持有者一个人私人持有的特性（1分），使得公钥密码体制不仅能像传统密码体制那样用于消息加密，实现秘密通信，还可以广泛应用于数字签名、认证等领域（1分）。

5、答：数字签名与加密不同，它的主要目的是保证数据的完整性和真实性，一般包括两部分：签名算法和验证算法，通常由公钥密码算法和杂凑函数（Hash算法）结合实现。假设发送方A要向接收方B发送一消息M，并对该消息进行数字签名，其具体的原理和过程如下：①发送方A采用杂凑函数生成要发送消息M的消息摘要：Hash（M）（2分）；②发送方A采用自己的私钥Pra对消息M的消息摘要加密，实现签名：EPRa(Hash(M))，并将签名与消息M并联形成最终要发送的消息：M|| EPRa(Hash(M)),然后发送该消息（2分）；③接收方B接收到消息后，采用发送方A的公钥Pua解密签名，恢复原始消息的摘要：Hash(M)=DPUa(EPRa(Hash(M)))（2分）；④接收方B采用杂凑函数，重新计算消息M的消息摘要：H’ash(M)，并与从发送方A接收到的消息摘要进行比较,若相等，则说明消息确实是发送方A发送的，并且消息的内容没有被修改过（2分）。数字签名技术对网络安全通信及各种电子交易系统的成功有重要的作用。

1、解：①将元素（83）H转换为二进制数据为（10000011）2（0.5分）；

②将二进制数据（10000011）2转换为给定有限域上的多项式：X7+X+1（0.5分）；

③利用欧几里得扩展算法求解以上多项式在指定有限域上的逆多项式（每步（行）2分））：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q（X） | A1（X） | A2（X） | A3（X） | B1(X) | B2（X） | B3(X) |
| —— | 1 | 0 | X8+X4+X3+X+1 | 0 | 1 | X7+X+1 |
| X | 0 | 1 | X7+X+1 | 1 | X | X4+X3+X2+1 |
| X3+X2+1 | 1 | X | X4+X3+X2+1 | X3+X2+1 | X4+X3+X+1 | X |
| X3+X2+X | X3+X2+1 | X4+X3+X+1 | X | X6+X2+X+1 | X7 | 1 |

由以上计算可知，在给定有限域中X7+X+1的逆多项式为X7；

④将多项式X7用二进制数据表示为：（10000000）2（0.5分）；

⑤将二进制数据（10000000）2转换为十六进制（80）H（0.5分）；

⑥元素（83）H在给定有限域上的乘法逆元为（80）H。

解：①密钥的生成：

模数n=p×q=7×17=119，φ(n)=（p-1）×（q-1）=6×16=96（0.5分）；

因为加密指数e和私密钥d满足：ed mod φ(n) =1,所以d=e-1 mod φ(n) ,私钥d的计算过程如下（1分）：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| —— | 1 | 0 | 96 | 0 | 1 | 13 |
| 7 | 0 | 1 | 13 | 1 | -7 | 5 |
| 2 | 1 | -7 | 5 | -2 | 15 | 3 |
| 1 | -2 | 15 | 3 | 3 | -22 | 2 |
| 1 | 3 | -22 | 2 | -5 | 37 | 1 |

由以上计算可知私密钥d=37。

公钥为（e,n）=(13,119),私钥为的d=37（0.5分）。

②使用以上密钥对，采用反复平方乘方法加密明文m=（19）10，计算过程如下：

采用RSA算法加密明文，密文c=me mod n=1913 mod 119

将加密指数e=13用二进制表示：（1101）2，则有（每步（计算行）2分）：

|  |  |  |
| --- | --- | --- |
| k | bi | d |
| 3 | 1 | ((12 mod 119) ×19)mod119 = 19 |
| 2 | 1 | ((192 mod 119) ×19) mod 119 = 76 |
| 1 | 0 | (76)2 mod 119 = 64 |
| 0 | 1 | ((64)2 mod 119) ×19) mod 119 = 117 |

由以上计算可知，密文为（117）10。

第一部分　判断题(共65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。

参考答案：对

2、由于传输的不同，电力线可以与网络线同槽铺设。

参考答案：错

3、机房供电线路和电力、照明用电可以用同一线路。

参考答案：错

4、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。

参考答案：对

5、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。

参考答案：对

6、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。

参考答案：错

7、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。

参考答案：错

8、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。

参考答案：对

9、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。

参考答案：对

10、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。

参考答案：对

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

参考答案：错

12、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又是该组成员，则Lois也有此权限。

参考答案：对

13、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。

参考答案：对

14、每个UNIX/Linux系统中都只有一个特权用户，就是root帐号。

参考答案：错

15、SQL注入攻击不会威胁到操作系统的安全。

参考答案：错

16、不需要对数据库应用程序的开发者制定安全策略。

参考答案：错

17、防火墙安全策略一旦设定，就不能再做任何改变。

参考答案：错

18、只要使用了防火墙，企业的网络安全就有了绝对的保障。

参考答案：错

19、半连接扫描也需要完成TCP协议的三次握手过程。

参考答案：错

20、防火墙是设置在内部网络与外部网络（如互联网）之间、或不同内部网络之间，实施访问控制策略的一个或一组系统。

参考答案：对

21、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

参考答案：对

22、与入侵检测系统不同，入侵防御系统采用在线（inline）方式运行。

参考答案：对

23、企业内部只需要在网关和各服务器上安装防病毒软件，客户端不需要安装。

参考答案：错

24、运行防病毒软件可以帮助防止遭受网页仿冒欺诈。

参考答案：对

25、包含收件人个人信息的邮件是可信的。

参考答案：错

26、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。

参考答案：错

27、网络边界保护中主要采用防火墙系统，为了保证其有效发挥作用，应当避免在内网和外网之间存在不经过防火墙控制的其他通信连接。

参考答案：对

28、根据ISO13335标准，信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。

参考答案：错

29、在我国严重的网络犯罪行为也不需要接受刑法的相关处罚。

参考答案：错

30、安全管理的合规性，主要是指在有章可循的基础上，确保信息安全工作符合国家法律、法规、行业标准、机构内部的方针和规定。

参考答案：对

31、从事国际联网经营活动和非经营活动的介入单位在不符合条件时，其国际联网经营许可证由发证机关吊销。

参考答案：错

32、公安部、国家安全部、国家保密局、国务院是计算机信息系统安全保护工作的主管部门。

参考答案：错

33、任何单位和个人不得自行建立或者使用其他信道进行国际联网。

参考答案：对

34、经营国际联网业务的单位，有违法行为的，公安机关可以吊销其经营许可证或者取消其联网资格。

参考答案：错

35、已经联网的用户有对计算机信息信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的权利。

参考答案：错

36、互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织当发现本网络中有危害国家利益的内容的地址、目录时，应当按照规定把它删除。

参考答案：对

37、过滤王控制台必须和同步代理软件安装在同一电脑上

参考答案：对

38、临时卡必须每次刷卡都输入姓名证件号码

参考答案：对

39、过滤王管理中心地址是:221.136.69.81

参考答案：对

40、上网卡密码不可以修改

参考答案：对

第二部分　单项选择题(共118题)

1、下列（ ）行为，情节较重的，处以5日以上10日以下的拘留。

A、未经允许重装系统

B、故意卸载应用程序

C、在互联网上长时间聊天的

D、故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行

参考答案：D

2、公然侮辱他人或者捏造事实诽谤他人的，处（ ）。

A、5日以下拘留或者500元以下罚款

B、10日以上拘留或者500元以下罚款

C、5日以下拘留或者1000元以下罚款

D、10日以上拘留或者1000以下罚款

参考答案：A

3、违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的，处（ ）日以下拘留。

A、5

B、15

C、20

D、30

参考答案：A

4、计算机信息系统，是指由（ ）及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、储存、传输、检索等处理的人机系统。

A、计算机硬件

B、计算机

C、计算机软件

D、计算机网络

参考答案： B

5、过滤王连接公安中心端的地址是（）

A、221.136.69.81

B、221.136.69.82

C、221.136.69.137

D、221.136.69.137

参考答案：A

6、过滤王日志是存放在Winfgate目录下的哪个文件夹下的（）

A、sys

B、log

C、date

D、日志

参考答案： B

7、过滤王用户上网日志是存放在哪个文件夹下的（）

A、access\_log

B、alert\_log

C、sys\_log

D、user\_log

参考答案：A

8、过滤王服务端上网日志需保存（）天以上

A、7

B、15

C、30

D、60

参考答案：D

9、下列哪类证件不得作为有效身份证件登记上网（）

A、驾驶证

B、户口本

C、护照

D、暂住证

参考答案： B

10、下列哪一个日志文件的大小是正常的()

A、1KB

B、20KB

C、7,023KB

D、123,158KB

参考答案：D

11、过滤王上网的用户日志是存放在哪个文件夹下的（）

A、access\_log

B、alert\_log

C、sys\_log

D、user\_log

参考答案：D

12、代表了当灾难发生后，数据的恢复程度的指标是\_\_\_\_\_\_\_。

A、PRO

B、RTO

C、NRO

D、SDO

参考答案：A

13、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、SDO

参考答案： B

14、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\_\_\_\_\_\_\_。

A、磁盘

B、磁带

C、光盘

D、软盘

参考答案： B

15、下列叙述不属于完全备份机制特点描述的是\_\_\_\_\_\_\_。

A、每次备份的数据量较大

B、每次备份所需的时间也就较大

C、不能进行得太频繁

D、需要存储空间小

参考答案：D

16、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

参考答案： B

17、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

参考答案：D

18、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

参考答案：A

19、容灾的目的和实质是\_\_\_\_\_\_\_。

A、数据备份

B、心理安慰

C、保质信息系统的业务持续性

D、系统的有益补充

参考答案：C

20、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

参考答案：A

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

A、-1

B、0

C、1

D、2

参考答案： B

22、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

参考答案： B

23、在正常情况下，Windows 2000中建议关闭的服务是\_\_\_\_\_\_\_。

A、TCP/IP NetBIOS Helper Service

B、Logical Disk Manager

C、Remote Procedure Call

D、Security Accounts Manager

参考答案：A

24、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/group

C、设置足够强度的帐号密码

D、使用shadow密码

参考答案：A

25、下面不是SQL Server支持的身份认证方式的是\_\_\_\_\_\_\_。

A、Windows NT集成认证

B、SQL Server认证

C、SQL Server混合认证

D、生物认证

参考答案：D

26、下面不是Oracle数据库支持的备份形式的是\_\_\_\_\_\_\_。

A、冷备份

B、温备份

C、热备份

D、逻辑备份

参考答案： B

27、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\_\_\_\_\_\_\_。

A、本地帐号

B、域帐号

C、来宾帐号

D、局部帐号

参考答案：C

28、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\_\_\_\_\_\_\_。

A、上午8点

B、中午12点

C、下午3点

D、凌晨1点

参考答案：D

29、下面不是UNIX/Linux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

参考答案：D

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

A、chmod命令

B、/bin/passwd命令

C、chgrp命令

D、/bin/su命令

参考答案：D

31、下面不是保护数据库安全涉及到的任务是\_\_\_\_\_\_\_。

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

参考答案：C

32、有关数据库加密，下面说法不正确的是\_\_\_\_\_\_\_。

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

参考答案：C

33、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

参考答案：A

34、关于NAT说法错误的是\_\_\_\_\_\_\_

A、NAT允许一个机构专用Intranet中的主机透明地连接到公共域中的主机，无需每台内部主机都拥有注册的（已经越来越缺乏的）全局互联网地址

B、静态NAT是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法地址

C、动态NAT主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态NAT就会分配给用户一个IP地址，当用户断开时，这个IP地址就会被释放而留待以后使用

D、动态NAT又叫网络地址端口转换NAPT

参考答案：D

35、通用入侵检测框架(CIDF)模型中,\_\_\_\_\_\_\_的目的是从整个计算环境中获得事件,并向系统的其他部分提供此事件。

A、事件产生器

B、事件分析器

C、事件数据库

D、响应单元

参考答案：A

36、基于网络的入侵检测系统的信息源是\_\_\_\_\_\_\_。

A、系统的审计日志

B、事件分析器

C、应用程序的事务日志文件

D、网络中的数据包

参考答案：D

37、误用入侵检测技术的核心问题是\_\_\_\_\_\_\_的建立以及后期的维护和更新。

A、异常模型

B、规则集处理引擎

C、网络攻击特征库

D、审计日志

参考答案：C

38、下面说法错误的是\_\_\_\_\_\_\_。

A、由于基于主机的入侵检测系统可以监视一个主机上发生的全部事件，它们能够检测基于网络的入侵检测系统不能检测的攻击

B、基于主机的入侵检测系统可以运行在交换网络中

C、基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描

D、基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击，因为应用程序日志并不像操作系统审计追踪日志那样被很好地保护

参考答案：C

39、网络隔离技术，根据公认的说法，迄今已经发展了\_\_\_\_\_\_\_个阶段。

A、六

B、五

C、四

D、三

参考答案： B

40、当您收到您认识的人发来的电子邮件并发现其中有附件，您应该\_\_\_\_\_\_\_。

A、打开附件，然后将它保存到硬盘

B、打开附件，但是如果它有病毒，立即关闭它

C、用防病毒软件扫描以后再打开附件

D、直接删除该邮件

参考答案：C

41、不能防止计算机感染病毒的措施是\_\_\_\_\_\_\_。

A、定时备份重要文件

B、经常更新操作系统

C、除非确切知道附件内容，否则不要打开电子邮件附件

D、重要部门的计算机尽量专机专用，与外界隔绝

参考答案：A

42、下面关于DMZ区的说法错误的是\_\_\_\_\_\_\_

A、通常DMZ包含允许来自互联网的通信可进入的设备，如Web服务器、FTP服务器、SMTP服务器和DNS服务器等

B、内部网络可以无限制地访问外部网络DMZ区

C、DMZ可以访问内部网络

D、有两个DMZ的防火墙环境的典型策略是主防火墙采用NAT方式工作，而内部防火墙采用透明模式工作以减少内部网络结构的复杂程度

参考答案：C

43、使用漏洞库匹配的扫描方法，能发现\_\_\_\_\_\_\_。

A、未知的漏洞

B、已知的漏洞

C、自行设计的软件中的漏洞

D、所有的漏洞

参考答案： B

44、下面关于隔离网闸的说法，正确的是\_\_\_\_\_\_\_

A、能够发现已知的数据库漏洞

B、可以通过协议代理的方法，穿透网闸的安全控制

C、任何时刻，网闸两端的网络之间不存在物理连接

D、在OSI的二层以上发挥作用

参考答案：C

45、某病毒利用RPCDCOM缓冲区溢出漏洞进行传播，病毒运行后，在%System%文件夹下生成自身的拷贝nvchip4.exe，添加注册表项，使得自身能够在系统启动时自动运行。通过以上描述可以判断这种病毒的类型为\_\_\_\_\_\_\_。

A、文件型病毒

B、宏病毒

C、网络蠕虫病毒

D、特洛伊木马病毒

参考答案：C

46、包过滤防火墙工作在OSI网络参考模型的\_\_\_\_\_\_\_

A、物理层

B、数据链路层

C、网络层

D、应用层

参考答案：C

47、防火墙提供的接入模式不包括\_\_\_\_\_\_\_

A、网关模式

B、透明模式

C、混合模式

D、旁路接入模式

参考答案：D

48、下列技术不支持密码验证的是：

A、S/MIME

B、PGP

C、AMTP

D、SMTP

参考答案：D

49、下列不属于垃圾邮件过滤技术的是：

A、软件模拟技术

B、贝叶斯过滤技术

C、关键字过滤技术

D、黑名单技术

参考答案：A

50、下列技术不能使网页被篡改后能够自动恢复的是：

A、限制管理员的权限

B、轮询检测

C、事件触发技术

D、核心内嵌技术

参考答案：A

51、如果您认为您已经落入网络钓鱼的圈套，则应采取（ ）措施。

A、向电子邮件地址或网站被伪造的公司报告该情形

B、更改帐户的密码

C、立即检查财务报表

D、以上全部都是

参考答案：D

52、下面技术中不能防止网络钓鱼攻击的是：

A、在主页的底部设有一个明显链接，以提醒用户注意有关电子邮件诈骗的问题

B、利用数字证书（如USB KEY）进行登录

C、根据互联网内容分级联盟（ICRA）提供的内容分级标准对网站内容进行分级

D、安装杀毒软件和防火墙、及时升级、打补丁、加强员工安全意识

参考答案：C

53、以下不会帮助减少收到的垃圾邮件数量的是：

A、使用垃圾邮件筛选器帮助阻止垃圾邮件

B、共享电子邮件地址或即时消息地址时应小心谨慎

C、安装入侵检测软件

D、收到垃圾邮件后向有关部门举报

参考答案：C

54、内容过滤技术的含义不包括:

A、过滤互联网请求从而阻止用户浏览不适当的内容和站点

B、过滤流入的内容从而阻止潜在的攻击进入用户的网络系统

C、过滤流出的内容从而阻止敏感数据的泄露

D、过滤用户的输入从而阻止用户传播非法内容

参考答案：D

55、下列内容过滤技术中在我国没有得到广泛应用的是:

A、内容分级审查

B、关键字过滤技术

C、启发式内容过滤技术

D、机器学习技术

参考答案：A

56、会让一个用户的“删除”操作去警告其他许多用户的垃圾邮件过滤技术是：

A、黑名单

B、白名单

C、实时黑名单

D、分布式适应性黑名单

参考答案：D

57、不需要经常维护的垃圾邮件过滤技术是：

A、指纹识别技术

B、简单DNS测试

C、黑名单技术

D、关键字过滤

参考答案： B

58、《计算机信息系统安全保护条例》规定，故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品，由公安机关处以警告或者对个人处以( )的罚款、对单位处以（ ）的罚款

A、5000元以下 15000元以下

B、5000元 15000元

C、2000元以下 10000元以下

D、2000元 10000元

参考答案：A

59、PDR模型是第一个从时间关系描述一个信息系统是否安全的模型，PDR模型中的P，D，R代表分别代表（ ）。

A、保护 检测 响应

B、策略 检测 响应

C、策略 检测 恢复

D、保护 检测 恢复

参考答案：A

60、根据权限管理的原则，一个计算机操作员不应当具备访问（ ）的权限。

A、操作指南文档

B、计算机控制台

C、应用程序源代码

D、安全指南

参考答案：C

61、双机热备是一种典型的事先预防和保护措施，用于保证关键设备和服务的（ ）属性。

A、保密性

B、可用性

C、完整性

D、第三方人员

参考答案： B

62、（ ）手段可以有效应对较大范围的安全事件的不良影响，保证关键服务和数据的可用性。

A、定期备份

B、异地备份

C、人工备份

D、本地备份

参考答案： B

63、相对于现有杀毒软件在终端系统中提供保护不同，（ ）在内外边界处提供更加主动和积极的病毒保护。

A、防火墙

B、病毒网关

C、IPS

D、IDS

参考答案： B

64、《信息系统安全等级保护基本要求》中对不同级别的信息系统应具备的基本安全保护能力进行了要求，共划分为（ ）级。

A、4

B、5

C、6

D、7

参考答案：A

65、统计数据表明，网络和信息系统最大的人为安全威胁来自于（ ）

A、恶意竞争对手

B、内部人员

C、互联网黑客

D、第三方人员

参考答案： B

66、1999年，我国发布第一个信息安全等级保护的国家标准GB17859-1999，提出将信息系统的安全等级划分为（ ）个等级。

A、7

B、8

C、4

D、5

参考答案：D

67、互联网服务提供者和联网使用单位落实的记录留存技术措施，应当具有至少保存（ ）天记录备份的功能。

A、10

B、30

C、60

D、90

参考答案：C

68、定期对系统和数据进行备份，在发生灾难时进行恢复。该机制时为了满足信息安全的（ ）属性。

A、真实性

B、完整性

C、不可否认性

D、可用性

参考答案：D

69、公安部网络违法案件举报网站的网址是（ ）

A、www.netpolice.cn

B、www.gongan.cn

C、http://www.cyberpolice.cn

D、www.110.cn

参考答案：C

70、信息安全经历了三个发展阶段，以下（ ）不属于这个阶段。

A、通信保密阶段

B、加密机阶段

C、信息安全阶段

D、安全保障阶段

参考答案： B

71、信息安全在通信保密阶段对信息安全的关注局限在（ ）安全属性。

A、不可否认性

B、可用性

C、保密性

D、完整性

参考答案：C

72、信息安全管理领域权威的标准是（ ）。

A、ISO15408

B、ISO17799/ISO27001

C、ISO9001

D、ISO14001

参考答案： B

73、在PPDRR安全模式中，（ ）是属于安全事件发生后补救措施。

A、保护

B、恢复

C、响应

D、检测

参考答案： B

74、根据风险管理的看法，资产( )价值，( )脆弱性，被安全威胁( )，( )风险。

A、存在 利用 导致 具有

B、具有 存在 利用 导致

C、导致 存在 具有 利用

D、利用 导致 存在 具有

参考答案： B

75、互联网站链接境外新闻网站，登载境外新闻媒体和互联网站发布的新闻，必须另行报（ ）批准。

A、国务院新闻办公室

B、文化部

C、教育部

D、信息产业部

参考答案：A

76、（ ）在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项

A、公安部

B、国家安全部

C、中科院

D、司法部

参考答案：A

77、《中华人民共和国治安管理处罚法》规定，利用计算机信息网络传播淫秽信息的，处（ ）以下拘留，可以并处三千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

A、五日以下

B、五日以上十日以下

C、十日以上十五日

D、十五日

参考答案：C

78、互联单位主管部门对经营性接入单位实行（ ）制度。

A、月检

B、半年检

C、年检

D、周检

参考答案：C

79、计算机信息系统是指由指由（ ）及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理系统。

A、计算机硬件

B、计算机

C、计算机软件

D、计算机网络

参考答案： B

80、我国计算机信息系统实行（ ）保护。

A、责任制

B、主任值班制

C、安全等级

D、专职人员资格

参考答案：C

81、故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，（ ）的，应依法处5年以下有期徒刑或者拘役。

A、后果严重

B、产生危害

C、造成系统失常

D、信息丢失

参考答案：A

82、中华人民共和国进内的计算机信息网络进行国际联网，应当依照（ ）办理。

A、《中华人民共和国计算机信息系统安全保护条例》

B、《中华人民共和国计算机信息网络国际联网暂行规定实施办法》

C、《中华人民共和国计算机互联网国际联网管理办法》

D、《中国互联网络域名注册暂行管理办法》

参考答案： B

83、违反《计算机信息系统安全保护条例》的规定，构成（ ）的，依照《治安管理处罚法》的有关规定处罚。

A、犯罪

B、违反《刑法》

C、违反治安管理行为

D、违反计算机安全行为

参考答案：C

84、涉及国家事务、经济建设、国防建设、尖端科技等重要领域的单位的计算机信息网络与（ ），应当采取相应的安全保护措施。

A、任何单位

B、外单位

C、国内联网

D、国际联网

参考答案：D

85、电子公告服务提供者应当记录在电子公告服务系统中发布的信息内容及其发布时间、互联网地址或者域名。记录备份应当保存（ ）日。

A、90

B、60

C、30

D、10

参考答案： B

86、涉及国家秘密的计算机信息系统，（ ）地与国际互联网或者其他公共信息网络相连，必须实行物理隔离。

A、不得直接或者间接

B、不得直接

C、不得间接

D、不得直接和间接

参考答案：A

87、国际联网采用（ ）制定的技术标准、安全标准、资费政策，以利于提高服务质量和水平。

A、企业统一

B、单位统一

C、国家统一

D、省统一

参考答案：C

88、企业计算机信息网络和其他通过专线进行国际联网的计算机信息网络，只限于（ ）使用。

A、企业

B、外部

C、内部

D、专人

参考答案：C

89、（ ）违反计算机信息系统安全保护条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

A、计算机操作人员

B、计算机管理人员

C、任何组织或者个人

D、除从事国家安全的专业人员以外的任何人

参考答案：C

90、互联单位应当自网络正式联通之日起（ ）内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

A、15

B、30

C、45

D、60

参考答案： B

91、《计算机信息网络国际联网安全保护管理办法》规定，未建立安全保护管理制度的，采取安全技术保护措施，由公安机关（ ），给予（ ），还可（ ）；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可（ ）

A、责令限期改正 警告 没收违法所得 并处罚款

B、通报批评 警告 没收违法所得 并处罚款

C、通报批评 拘留 没收违法所得 并处罚款

D、责令限期改正 警告 没收违法所得 并处拘留

参考答案：A

92、根据《互联网电子公告服务管理规定》规定，（ ）发现电子公告服务系统中出现明显属于该办法第九条所列的禁止信息内容之一的，应当立即删除，保存有关记录，并向国家有关机关报告。

A、电子公告用户

B、电子公告浏览者

C、互联单位

D、电子公告服务提供者

参考答案：D

93、过滤王软件最多监控多少客户端?

A、100

B、200

C、300

D、400

参考答案：C

94、备份过滤王数据是备份哪些内容?

A、过滤控制台目录

B、过滤核心目录

C、核心目录下的ACCERS目录

D、核心目录下的几个目录

参考答案： B

95、安装过滤王核心的逻辑盘要留至少多少空闲空间?

A、1G

B、2G

C、3G

D、15G

参考答案：D

第三部分　多项选择题(共38题)

1、下列（ ）行为，情节较重的，可以处5日以上10日以下拘留，可以并处500元以下罚款。

A、偷窥、偷拍、窃听、散布他人隐私的

B、未经他人允许向其发送邮件的

C、利用手机向他人发送短信息的

D、捏造事实诬告陷害他人，企图使他人受到刑事追究或者受到治安管理处罚的

参考答案：A D

2、下列哪些是互联网提供的功能。（ ）

A、E-mail

B、BBS

C、FTP

D、WWW

参考答案：A B C D

2、对违反行政管理秩序的公民、法人或者其他组织，将要作出（ ）的行政处罚之前，行政处罚机关应制作《违法行为处理通知书》，并送达当事人。

A、警告

B、较大数额罚款

C、责令停产停业

D、暂扣或者吊销许可证

参考答案： B C D

4、系统数据备份包括对象有\_\_\_\_\_\_\_。

A、配置文件

B、日志文件

C、用户文档

D、系统设备文件

参考答案：A B D

5、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

参考答案：A B C D E

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\_\_\_\_\_\_\_。

A、Domain Admins组

B、Domain Users组

C、Domain Replicators组

D、Domain Guests组

参考答案：A B D

7、UNIX/Linux系统中的Apache服务器的主要安全缺陷表现在攻击者可以\_\_\_\_\_\_\_。

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

参考答案：A B C

8、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（Security Account Manager，简称SAM）模块

B、Windows系统的注册（WinLogon）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

参考答案：A B C

9、SQL Server中的预定义服务器角色有\_\_\_\_\_\_\_。

A、sysadmin

B、serveradmin

C、setupadmin

D、securityadmin

E、processadmin

参考答案：A B C D E

10、可以有效限制SQL注入攻击的措施有\_\_\_\_\_\_\_。

A、限制DBMS中sysadmin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

参考答案： B C D E

11、防火墙的局限性包括\_\_\_\_\_\_\_

A、防火墙不能防御绕过了它的攻击

B、防火墙不能消除来自内部的威胁

C、防火墙不能对用户进行强身份认证

D、防火墙不能阻止病毒感染过的程序和文件进出网络

参考答案：A B D

12、网络安全扫描能够\_\_\_\_\_\_\_

A、发现目标主机或网络

B、判断操作系统类型

C、确认开放的端口

D、识别网络的拓扑结构

E、测试系统是否存在安全漏洞

参考答案：A B C D E

13、入侵防御技术面临的挑战主要包括\_\_\_\_\_\_\_

A、不能对入侵活动和攻击性网络通信进行拦截

B、单点故障

C、性能“瓶颈”

D、误报和漏报

参考答案： B C D

14、病毒传播的途径有\_\_\_\_\_\_\_

A、移动硬盘

B、内存条

C、电子邮件

D、聊天程序

E、网络浏览

参考答案：A C D E

15、下列邮件为垃圾邮件的有：

A、收件人无法拒收的电子邮件

B、收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件

C、含有病毒、色情、反动等不良信息或有害信息的电子邮件

D、隐藏发件人身份、地址、标题等信息的电子邮件

E、含有虚假的信息源、发件人、路由等信息的电子邮件

参考答案：A C D E

16、内容过滤的目的包括：

A、阻止不良信息对人们的侵害

B、规范用户的上网行为，提高工作效率

C、防止敏感数据的泄露

D、遏制垃圾邮件的蔓延

E、减少病毒对网络的侵害

参考答案：A B C D E

17、所有进入网络和信息系统工作的人员，必须签订保密协议，具体协议保密协议的人员范围包括：（ ）

A、网络使用者

B、正式雇员

C、离职雇员

D、第三方人员

参考答案： B C D

18、我国信息网络重点单位一共分为12类，下列属于信息网络重点单位包括（ ）

A、党政机关

B、金融机构、邮电、广电部门、能源单位、交通运输单位

C、所有工程建设单位、互联网管理中心和重要网站

D、尖端科研单位、社会应急服务部门、重要物资储备单位

参考答案：A B C D

19、信息系统安全等级保护的核心是对信息系统分等级、按标准进行建设、管理和监督。信息系统安全等级保护实施过程中应遵循以下基本原则有（ ）

A、自主保护原则

B、重点保护原则

C、同步建设原则

D、动态调整原则

参考答案：A B C D

20、计算机病毒具有以下特点（ ）

A、传染性

B、隐蔽性

C、潜伏性

D、可预见性

E、破坏性

参考答案：A B C E

21、公安机关对计算机信息系统安全保护工作行使下列监督职权：（ ）

A、监督、检查、指导计算机信息系统安全保护工作

B、查处危害计算机信息系统安全的违法犯罪案件

C、履行计算机信息系统安全保护工作的其他监督职责

D、就涉及计算机信息系统安全的特定事项发布专项通令

参考答案：A B C D

22、违反《计算机信息系统安全保护条例》的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：（ ）

A、违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的

B、违反计算机信息系统国际联网备案制度的

C、按照规定时间报告计算机信息系统中发生的案件的

D、接到公安机关要求改进安全状况的通知后，在限期内拒不改进的

参考答案：A B D

23、任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款，情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚法的规定处罚；构成犯罪的，依法追究刑事责任： （ ）

A、捏造或者歪曲事实，散布谣言，扰乱社会秩序的

B、煽动抗拒、破坏宪法和法律、行政法规实施的

C、公然侮辱他人或者捏造事实诽谤他人的

D、表示对国家机关不满的

参考答案：A B C

24、任何人不得在电子公告服务系统中发布含有下列内容之一的信息： （ ）

A、反对宪法所确定的基本原则的、危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的

B、损害国家荣誉和利益的；煽动民族仇恨、民族歧视，破坏民族团结的

C、破坏国家宗教政策，宣扬邪教和封建迷信的

D、散布谣言、淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的

参考答案：A B C D

25、互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责 （ ）

A、负责本网络的安全保护管理工作，建立健全落实安全保护管理制度

B、负责对本网络用户的安全教育和培训

C、对委托发布信息的单位和个人进行登记，并对所提供的信息内容进行审核

D、发现计算机案件应当保留有关原始记录，并在二十四小时内向当地公安机关报告

参考答案：A B C D

26、为了保障互联网的运行安全，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：（ ）

A、侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统

B、故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害

C、违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行

D、非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密

参考答案：A B C D

27、安装过滤王核心需要哪些数据

A、网吧代码

B、管理中心地址

C、序列号

D、计算机名

参考答案：A B C

28、目前使用的过滤王核心的版本是多少?

A、5.0.00.141

B、5.0.00.142

C、5.0.00.143

D、5.0.00.146

参考答案：A B C D

29、过滤王可以过滤哪些类型的网站

A、赌博

B、邪教

C、暴力

D、色情

参考答案：A B C D

第四部分　填空题(共25题)

1、对发现人员身份信息录入有误的会员卡要及时\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，重新做新卡。

参考答案：注销

2、发行会员卡时必须严格核对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_后正确录入保存

参考答案：上网人员身份信息

3、与安装过滤王核心电脑相连接的交换机上，必须具有\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

参考答案：镜像端口

4、物理安全是指物理介质层次上对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_的网络信息的安全保护，是网络信息安全的最基本保障。

参考答案：存储和传输

5、容灾就是减少灾难事件发生的可能性以及限制灾难对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_所造成的影响的一整套行为。

参考答案：关键业务流程

6、数据备份是目的是为了\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_在崩溃时能够快速地恢复数据。

参考答案：系统数据

7、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是PKI系统安全的核心。

参考答案：CA

8、公钥密码体制有两种基本模型：一种是加密模型；另一种是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_模型。

参考答案：认证

9、著名的DES数据加密标准是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_加密系统

参考答案：对称

10、数据库恢复技术中，建立冗余数据最常用的技术有两种：第一种是数据备份，第二种是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

参考答案：日志文件

11、数据库访问控制的粒度可分为4个层次，分别是数据库级、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_、记录级（行级）和属性级（字段级）。

参考答案：表级

12、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是在密罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个密罐，来构成一个黑客诱捕网络体系架构。

参考答案：密网

13、在PDRR模型中，\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是静态防护转化为动态的关键，是动态相应的依据。

参考答案：检测

14、ISO 17799/ISO 27001最初是由\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_提出的国家标准。

参考答案：英国

15、凡是违反国家法律、危害计算机信息系统安全以及利用计算机信息系统实施的违法犯罪活动，统称计算机案件，计算机案件主要分为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_两类。

参考答案：刑事案件和行政案件

16、一个完整的信息安全保障体系，应当包括\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_五个主要环节，这就是PPDRR模型的内容。

参考答案：安全策略、保护、检测、响应、恢复

17、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是国家授权对信息安全和网络安全进行监控和管理的职能机构，各单位、组织都应当密切配合。

参考答案：公安部

18、GB 17859-1999的全称是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是建立计算机信息系统安全等级保护制度，实施安全等级管理的基础性标准。

参考答案：计算机信息系统安全保护等级划分准则

19、从事国际联网业务的单位和个人应当接受\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

参考答案：公安机关

20、任何单位发现有违反规定的有害信息的，应当保留原始纪录后及时删除，并在\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_小时内向当地公安机关报告；发现计算机犯罪案件，应立即向公安网监部门报案，并保护好现场。

参考答案：24

21、违反国家规定，对计算机信息系统功能进行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

参考答案：删除、修改、增加、干扰

22、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

参考答案：任何单位和个人

23、《计算机信息网络国际联网安全保护管理办法》规定了备案制度与罚则，\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_均为备案对象。

参考答案：接入服务单位、数据中心、信息服务单位、联网单位

24、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,是指互联网上一切可能对现存法律秩序和其他公序良俗造成破坏或者威胁的数据、新闻和知识等信息。

参考答案：互联网上的有害信息

25、过滤王自动保存最近\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_天的上网记录

参考答案：60

1.通常为保证信息处理对象的认证性采用的手段是\_\_\_C\_\_\_\_\_\_\_

A.信息加密和解密 B.信息隐匿

C.数字签名和身份认证技术 D.数字水印

2.关于Diffie-Hellman算法描述正确的是\_\_\_\_B\_\_\_\_\_\_

A.它是一个安全的接入控制协议 B.它是一个安全的密钥分配协议

C.中间人看不到任何交换的信息 D.它是由第三方来保证安全的

3.以下哪一项不在证书数据的组成中? \_\_\_\_\_D\_\_\_\_\_

A.版本信息 B.有效使用期限

C.签名算法 D.版权信息

4．关于双联签名描述正确的是\_\_\_\_D\_\_\_\_\_\_

A．一个用户对同一消息做两次签名 B．两个用户分别对同一消息签名

C．对两个有联系的消息分别签名 D．对两个有联系的消息同时签名

5．Kerberos中最重要的问题是它严重依赖于\_\_\_\_C\_\_\_\_\_\_

A．服务器 B．口令

C．时钟 D．密钥

6．网络安全的最后一道防线是\_\_\_\_A\_\_\_\_\_\_

A．数据加密 B．访问控制

C．接入控制 D．身份识别

7．关于加密桥技术实现的描述正确的是\_\_\_\_A\_\_\_\_\_\_

A．与密码设备无关，与密码算法无关 B．与密码设备有关，与密码算法无关

C．与密码设备无关，与密码算法有关 D．与密码设备有关，与密码算法有关

8．身份认证中的证书由\_\_\_\_A\_\_\_\_\_\_

A．政府机构发行 B．银行发行

C．企业团体或行业协会发行 D．认证授权机构发行

9．称为访问控制保护级别的是\_\_\_\_C\_\_\_\_\_\_

A．C1 B．B1

C．C2 D．B2

10．DES的解密和加密使用相同的算法，只是将什么的使用次序反过来? \_\_\_\_C\_\_\_\_\_\_

A．密码 B．密文

C．子密钥 D．密钥

11．PKI的性能中，信息通信安全通信的关键是\_\_\_\_\_C\_\_\_\_\_

A．透明性 B．易用性

C．互操作性 D．跨平台性

12．下列属于良性病毒的是\_\_\_\_D\_\_\_\_\_

A．黑色星期五病毒 B．火炬病毒

C．米开朗基罗病毒 D．扬基病毒

13．目前发展很快的基于PKI的安全电子邮件协议是\_\_\_\_A\_\_\_\_\_\_

A．S／MIME B．POP

C．SMTP D．IMAP

14．建立计算机及其网络设备的物理环境，必须要满足《建筑与建筑群综合布线系统工程设计规范》的要求，计算机机房的室温应保持在\_\_\_A\_\_\_\_\_\_\_

A．10℃至25℃之间 B．15℃至30℃之间

C．8℃至20℃之间 D．10℃至28℃之间

15．SSL握手协议的主要步骤有\_\_\_\_B\_\_\_\_\_\_

A．三个 B．四个

C．五个 D．六个

16．SET安全协议要达到的目标主要有\_\_\_\_C\_\_\_\_\_\_

A．三个 B．四个

C．五个 D．六个

17．下面不属于SET交易成员的是\_\_\_\_\_B\_\_\_\_\_

A．持卡人 B．电子钱包

C．支付网关 D．发卡银行

18．使用加密软件加密数据时，往往使用数据库系统自带的加密方法加密数据，实施

\_\_\_\_\_A\_\_\_\_\_

A．DAC B．DCA

C．MAC D．CAM

19．CTCA指的是\_\_\_\_B\_\_\_\_\_\_

A．中国金融认证中心 B．中国电信认证中心

C．中国技术认证中心 D．中国移动认证中心

20．下列选项中不属于SHECA证书管理器的操作范围的是\_\_\_\_\_C\_\_\_\_\_

A．对根证书的操作 B．对个人证书的操作

C．对服务器证书的操作 D．对他人证书的操作

1. Windows系统安全模型由 登录流程 、 本地安全授权　、　安全账号管理器和　安全引用监视器　组合而成。  
2. 注册表是按照　　子树　、　项　、子项和　值　　组成的分层结构。实际上注册表只有两个子树: 　 HKEY\_LOCAL\_MACHINE　　和　HKEY\_USERS　　，但为了便于检索，用注册表编辑器打开注册表时，展现为五个子树，这些子树的总体组成了Windows中所有的系统配置。

3. 在Windows 2000 网络中有两种主要的帐号类型:　　域用户账号　　和　　本地用户账号　　。

5. E-mail系统主要由　　邮件分发代理　、邮件传输代理、邮件用户代理及　邮件工作站　　组成。

6. 电子邮件安全技术主要包括　　身份证认证技术、　加密签名技术、　协议过滤技术、　防火墙技术和　　邮件病毒过滤技术　。

1. 信息安全的狭义解释

信息安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，信息安全就是指信息处理和传输的安全。它包括硬件系统的安全可靠运行、操作系统和应用软件的安全、数据库系统的安全、电磁信息泄露的防护等。狭义的信息安全，就是指信息内容的安全，包括信息的保密性、真实性和完整性。P5

2. 密码系统

密码系统指用于加密和解密的系统。加密时，系统输入明文和加密密钥，加密变换后，输出密文；解密时，系统输入密文和解密密钥，解密变换后，输出明文。一个密码系统由信源、加密变换、解密变换、信宿和攻击者组成。密码系统强调密码方案的实际应用，通常应当是一个包含软、硬件的系统。P19

3. 数字水印

数字水印类似于信息隐藏，是在数字化的信息载体中嵌入不明显的记号隐藏起来，被嵌入的信息包括作品的版权所有者、发行者、购买者、作者的序列号、日期和有特殊意义的文本等，但目的不是为了隐藏或传递这些信息，而是在发现盗版或发生知识产权纠纷时，用来证明数字作品的来源、版本、原作者、拥有者、发行人以及合法使用人等。数字水印是数字化的多媒体作品版权保护的关键技术之一，也是信息隐藏的重要分支。P60

4. 消息认证码MAC

通常表示为MAC=Ck(M)，其中：M是长度可变的消息；K是收、发双方共享的密钥；函数值Ck(M)是定长的认证码，也称为密码校验和。MAC是带密钥的消息摘要函数，即一种带密钥的数字指纹，它与不带密钥的数字指纹是又本质区别的。P73

1. 常见的网络踩点方法有哪些？常见的网络扫描技术有哪些?

P335-1

方法：域名相关信息的查询、公司性质的了解、对主页进行分析、对目标IP地址范围进行查询和网络勘察等。

技术：端口扫描、共享目录扫描、系统用户扫描和漏洞扫描。

2. 简述欺骗攻击的种类及其原理？？

P336-5

DNS欺骗：域名解析过程中，假设当提交给某个域名服务器的域名解析请求的数据包截获，然后按截获者的意图将一个虚假的IP地址作为应答信息返回给请求者。

Web欺骗：攻击者通过伪造某个WWW站点的影像拷贝，使改影像Web的入口进入攻击者的Web服务器，并经过攻击者计算机的过滤作用，从而达到攻击者监控受攻击者的任何活动以获取有用的信息为目的。

IP欺骗：在服务器不存在任何漏洞的情况下，通过利用TCP/IP协议本身存在的一些缺陷进行攻击的方法。

电子邮件欺骗：攻击者佯称自己为系统管理员，给用户发送邮件要求用户修改口令或在貌似正常的附件中加载病毒或其他木马程序。

ARP欺骗：利用主机从网上接收到的任何ARP应答都会更新自己的地址映射表，而不管是否是真实的缺陷实施的攻击形式。

3. 简述拒绝服务攻击的原理和种类？。

P336-3

拒绝服务攻击广义上可以指任何导致用户的服务器不能正常提供服务的攻击。DoS攻击具有各种各样的攻击模式，是分别针对各种不同的服务而产生的。它对目标系统进行的攻击可以分为以下三类：消耗稀少的、有限的并且无法再生的系统资源；破坏或者更改系统的配置信息；对网络部件和设施进行物理破坏和修改。

4. 例举几种常见的攻击实施技术。

P335-2

社会工程学攻击、口令攻击、漏洞攻击、欺骗攻击、拒绝服务攻击等。

5. 简述TCP/IP协议的封装过程？

P131 图9-1-2

试述RAID 0、RAID 1、RAID 3、RAID 5方案。

（1）RAID0：无冗余、无校验的磁盘阵列。RAID0至少使用两个磁盘驱动器，并将数据分成从512字节到数兆节的若干块（数据条带），这些数据块被交替写到磁盘中。RAID0不适用于对可靠性要求高的关键任务环境，但却非常适合于对性能要求较高的视频或图像编辑。

（2）RAID1：镜像磁盘阵列。每一个磁盘驱动器都有一个镜像磁盘驱动器，镜像磁盘驱动器随时保持与原磁盘驱动器的内容一致。RAID1具有较高的安全性，但只有一半的磁盘空间被用来存储数据。为了实时保护镜像磁盘数据的一致性，RAID1磁盘控制器的负载相当大，在此性能上没有提高。RAID1主要用于在对数据安全性要求很高，而且要求能够快速恢复损坏的数据的场合。

（3）RAID3：带奇偶校验码的并行传送。RAID3使用一个专门的磁盘存放所有的校验数据，而在剩余的磁盘中创建带区集分散数据的读写操作。RAID3适合用于数据密集型环境或单一用户环境，尤其有益于要访问较长的连续记录，例如数据库和Web服务器等。

（4）RAID5：无独立校验盘的奇偶校验磁盘阵列。RAID5把校验块分散到所有的数据盘中。RAID5使用了一种特殊的算法，可以计算出任何一个带区校验块的存放位置，这样就可以确保任何对校验块进行的读写操作都会在所有的RAID磁盘中进行均衡，从而消除了产生瓶颈的可能。RAID5能提供较完美的性能，因而也是被广泛应用的一种磁盘阵列方案。它适合于I/O密集、高读/写比率的应用程序，如事务处理等。为了具有RAID5级的冗余度，我们至少需要三个磁盘组成的磁盘阵列。RAID5可以通过磁盘阵列控制器硬件实现，也可以通过某些网络操作系统软件实现。P108

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. 在重要场所的迸出口安装监视器，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 Service B. 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。×

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。√

29. 在早期用集线器 (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，一样可以用来监昕整个子网。×

30. 可以通过技术手段，一次性弥补所有的安全漏洞。×

31. 漏洞只可能存在于操作系统中，数据库等其他软件系统不会存在漏洞。×

32. 防火墙中不可能存在漏洞。×

33. 基于主机的漏洞扫描不需要有主机的管理员权限。×

34. 半连接扫描也需要完成 TCP 协议的三次握手过程。×

35. 使用漏洞库匹配的方法进行扫描，可以发现所有的漏洞。×

36. 所有的漏洞都是可以通过打补丁来弥补的。×

37. 通过网络扫描，可以判断目标主机的操作系统类型。√

38.x-scan 能够进行端口扫描。√

39. 隔离网闸采用的是物理隔离技术。√

40." 安全通道隔离 " 是一种逻辑隔离。×

41. 隔离网闸两端的网络之间不存在物理连接。√

42.QQ 是与朋友联机聊天的好工具，不必担心病毒。×

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。×

44. 计算机病毒可能在用户打开 "txt" 文件时被启动。√

45. 在安全模式下木马程序不能启动。×

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。√

47. 家里的计算机没有联网，所以不会感染病毒。×

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。×

49. 校验和技术只能检测已知的计算机病毒。×

50. 采用 Rootkit 技术的病毒可以运行在内核模式中。√

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×

52. 大部分恶意网站所携带的病毒就是脚本病毒。√

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。√

二、单选题

1. 防火墙是在网络环境中的应用。

A. 字符串匹配 B. 访问控制技术 C. 入侵检测技术 D. 防病毒技术

2.iptables中默认的表名是一一一。

A.filter B.firewall C.nat D.mangle

3. 包过滤防火墙工作在 OSI 网络参考模型的

A. 物理层 B. 数据链路层

C. 网络层 D. 应用层

4. 通过添加规则，允许通往 192.168.0.2 的 SSH 连接通过防火墙的 iptables 指令是一一一。

A.iptables -F INPUTE –d 192.168.0.2 -p tcp -- dport 22 -j ACCEPT

B.iptables -A INPUT -d 192.168.0.2 -p tcp –dport 23-j ACCEPT

C.iptables -A FORWARD –d 192.168.0.2 -p tcp—dport 22 -j ACCEPT

D.iptables -A FORWARD –d 192.168.0.2 -p tcp—dport 23 -j ACCEPT

5. 防火墙提供的接入模式不包括一一一。

A. 网关模式 B.透明模式 C. 混合模式 D.旁路接入模式

6. 关于包过滤防火墙说法错误的是

A. 包过滤防火墙通常根据数据包源地址、

访问控制列表实施对数据包的过滤

B. 包过滤防火墙不检查 OSI 网络参考模型中网络层以上的数据，因此可以很快地执行

C. 包过滤防火墙可以有效防止利用应用程序漏洞进行的攻击

D. 由于要求逻辑的一致性、封堵端口的有效性和规则集的正确性，给过滤规则的制

定和配置带来了复杂性，一般操作人员难以胜任管理，容易出现错误

7. 关于应用代理网关防火墙说法正确的是

A. 基于软件的应用代理网关工作在θ SI 网络参考模型的网络层上，它采用应用协议

代理服务的工作方式实施安全策略

B. 一种服务需要一种代理模块，扩展服务较难

C. 和包过滤防火墙相比，应用代理网关防火墙的处理速度更快

D. 不支持对用户身份进行高级认证机制 O 一般只能依据包头信息，因此很容易受到" 地址欺骗型 " 攻击

8. 关于 NAT 说法错误的是

A.NAT 允许一个机构专用 Intramt 中的主机透明地连接到公共域中的主机，元需内 部主机拥有注册的 ( 已经越来越缺乏的 ) 全局互联网地址

B. 静态 NAT 是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址

C. 动态 NKT 主要应用于拨号和频繁的远程连接、当远程用户连接上之后，动态 NAT 就会分配给用户一个 IP 地址，当用户断开时，这个 IP 地址就会被释放而留待以后使用

D. 动态 NAT 又叫做网络地址端口转换 NAPT

9. 下面关于防火墙策略说法正确的是

A. 在创建防火墙策略以前，不需要对企业那些必不可少的应用软件执行风险分析 B. 防火墙安全策略一旦设定，就不能在再作任何改变

C. 防火墙处理入站通信的缺省策略应该是阻止所有的包和连接，除了被指出的允许 通过的通信类型和连接

D. 防火墙规则集与防火墙平台体系结构无关

10. 下面关于 DMZ 区的说法错误的是

A. 通常 DMZ 包含允许来自互联网的通信可进入的设备，如 Web 服务器、 FTP 服务器、 SMTP 服务器和 DNS 服务器等

B. 内部网络可以无限制地访问外部网络以及 DMZ

C.DMZ 可以访问内部网络

D. 有两个 DMZ 的防火墙环境的典型策略是主防火墙采用 NAT 方式工作，而内部防 火墙采用透明模式工作以减少内部网络结构的复杂程度

11. 在 PDRR 模型中，一一一一是静态防护转化为动态的关键，是动态响应的依据。

A. 防护 B. 检测 C. 响应 D. 恢复

12. 从系统结构上来看，入侵检测系统可以不包括

A. 数据源 B. 分析引擎 C. 审计 D. 响应

13. 通用入侵检测框架 (CIDF) 模型中，一一一的目的是从整个计算环境中获得事件 ,并向系统的其他部分提供此事件。

A. 事件产生器 B.事件分析器 C. 事件数据库 D.响应单元

14. 基于网络的入侵检测系统的信息源是

A. 系统的审计日志 B. 系统的行为数据

C. 应用程序的事务日志文件 D. 网络中的数据包

15. 误用入侵检测技术的核心问题是一一一的建立以及后期的维护和更新。

A. 异常模型 B. 规则集处理引擎去

C. 网络攻击特征库 D. 审计日志

16. 一一一是在蜜罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个蜜罐，来构成一个黑客诱捕网络体系架构。

A. 蜜网 B. 鸟饵 C.鸟巢 D.玻璃鱼缸

17. 下面关于响应的说法正确的是

A. 主动响应和被动响应是相互对立的，不能同时采用

B. 被动响应是入侵检测系统中的唯一响应方式

C. 入侵检测系统提供的警报方式只能是显示在屏幕上的警告信息或窗口

D. 主动响应的方式可以是自动发送邮件给入侵发起方的系统管理员请求协助以识别问题和处理问题

18. 下面说法错误的是

A. 由于基于主机的入侵检测系统可以监视一个主机上发生的全部事件，它们能够检

测基于网络的入侵检测系统不能检测的攻击

B. 基于主机的入侵检测可以运行在交换网络中

C. 基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描

D. 基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击，因为应 用程序日志并不像操作系统审计追踪日志那样被很好地保护

19. 使用漏洞库匹配的扫描方法，能发现

A. 未知的漏洞 B. 已知的漏洞

C. 自行设计的软件中的漏洞 D. 所有漏洞

20. 下面不可能存在于基于网络的漏洞扫描器中。

A. 漏洞数据库模块 B. 扫描引擎模块

C. 当前活功的扫描知识库模块 D. 阻断规则设置模块

21. 网络隔离技术，根据公认的说法，迄今已经发展了个阶段。

A. 六 B. 五 C. 四 D.三

22. 下面关于隔离网闸的说法，正确的是

A. 能够发现已知的数据库漏洞

B. 可以通过协议代理的方法，穿透网闸的安全控制

C. 任何时刻，网闸两端的网络之间不存在物理连接

D. 在 OSI 的二层以上发挥作用

23. 关于网闸的工作原理，下面说法错误的是

A. 切断网络之间的通用协议连接

B. 将数据包进行分解或重组为静态数据 ; 对静态数据进行安全审查，包括网络协议检查和代码扫描等

C. 网闸工作在 OSI 模型的二层以上

D. 任何时刻，网闸两端的网络之间不存在物理连接品

24. 当您收到您认识的人发来的电子邮件并发现其中有意外附件，您应该

A. 打开附件，然后将它保存到硬盘

B. 打开附件，但是如果它有病毒，立即关闭它

C. 用防病毒软件扫描以后再打开附件

D. 直接删除该邮件

25. 下面病毒出现的时间最晚的类型是

A. 携带特洛伊术马的病毒 B. 以网络钓鱼为目的的病毒

C. 通过网络传播的蠕虫病毒 D.OEice 文档携带的宏病毒

26. 某病毒利用 RPCDCOM 缓冲区溢出漏洞选行传播，病毒运行后，在 %System% 文件 夹下生成自身的拷贝 nvcl 呻牛 .exe, 添加注册表项，使得自身能够在系统启动时自动运行。通 过以上描述可以判断这种病毒的类型为 O S

A. 文件型病毒 B. 宏病毒

C. 网络蠕虫病毒 D. 特洛伊木马病毒

27. 采用 " 进程注入 "; 可以

A. 隐藏进程 B. 隐藏网络端口

C. 以其他程序的名义连接网络 D. 以上都正确

28. 下列关于启发式病毒扫描技术的描述中错误的是

A. 启发式病毒扫描技术是基于人工智能领域的启发式搜索技术

B. 启发式病毒扫描技术不依赖于特征代码来识别计算机病毒

C. 启发式病毒扫描技术不会产生误报，但可能会产生漏报

D. 启发式病毒扫描技术能够发现一些应用了已有机制或行为方式的病毒

29. 不能防止计算飞机感染病毒的措施是 u

A. 定时备份重要文件

B. 经常更新操作系统

C. 除非确切知道附件内容，否则不要打开电子邮件附件

D. 重要部门的计算机尽量专机专用与外界隔绝

30. 企业在选择防病毒产品时不应该考虑的指标为 I

A. 产品能够从一个中央位置进行远程安装、升级 '

B. 产品的误报、漏报率较低

C. 产品提供详细的病毒活动记录

D. 产品能够防止企业机密信息通过邮件被传出

三、多选题

1. 防火墙通常阻止的数据包包括

A. 来自未授权的源地址且目的地址为防火墙地址的所有入站数据包 { 除 Email 传递等特殊用处的端口外 )

B. 源地址是内部网络地址的所有人站数据包

C. 所有 ICMP 类型的入站数据包如

D. 来自未授权的源地址，包含 SNMP 的所有入站数据包

E. 包含源路由的所有入站和出站数据包

2. 目前市场上主流防火墙提供的功能包括

A. 数据包状态检测过滤 B. 应用代理

C.NAT D.VPN E. 日志分析和流量统计分析

3. 防火墙的局限性包括

A. 防火墙不能防御绕过了它的攻击

B. 防火墙不能消除来自内部的威胁

C. 防火墙不能对用户进行强身份认证

D. 防火墙不能阻止病毒感染过的程序和文件迸出网络

4. 防火墙的性能的评价方面包括

A. 并发会话数 B. 吞吐量

C. 延时 D. 平均无故障时间

5. 下面关于防火墙的维护和策略制定说法正确的是

A. 所有防火墙管理功能应该发生在使用了强认证和加密的安全链路上

B.Web 界面可以通过 SSL 加密用户名和密码。非 Web 的图形界面如果既没有内部加

密，也没有 SSL, 可以使用隧道解决方案，如 SSH

C. 对防火墙策略进行验证的最简单的方法是，获得防火墙配置的拷贝，然后把这些

拷贝和根据已定义的策略产生的期望配置进行比较

D. 对防火墙策略进行验证的另一种方式通过使用软件对防火墙配置进行实际测试

E. 渗墙分析可以取代传统的审计程序

6. 蜜罐技术的主要优点有一一一

A. 蜜罐技术属于被动响应，使用者没有成为刑事诉讼或民事诉讼对象的危险

B. 收集数据的真实性，蜜罐不提供任何实际的业务服务，所以搜集到的信息很大可

能性都是由于黑客攻击造成的，漏报率和误报率都比较低

c. 可以收集新的攻击工具和攻击方法，不像目前的大部分防火墙和入授检测系统只

能根据特征匹配方法来检测已知的攻击

D. 不需要强大的资金投入，可以用一些低成本的设备

E. 可以及时地阻断网络入侵行为

7. 通用入侵检测框架 (CIDF) 模型的组件包括

A. 事件产生器 B. 活动轮廓

C. 事件分析器 D. 事件数据库

E. 响应单元

8. 主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择

的措施可以归入的类别有

A. 针对入侵者采取措施 B. 修正系统

C. 收集更详细的信息 D. 入侵追踪

9. 随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由 于交换机不支持共享媒质的模式，传统的采用一个嗅探器 (snibr) 来监听整个子网的办法 不再可行。可选择解决的办法有

A. 不需要修改，交换网络和以前共享媒质模式的网络没有任何区别

B. 使用交换机的核心芯片上的一个调试的端口

C. 把入侵检测系统放在交换机内部或防火墙等数据流的关键入口、出口处

D. 采用分接器 (tap)

E. 使用以透明网桥模式接入的入侵检测系统

10. 入侵防御技术面临的挑战主要包括一一一

A. 不能对入侵活动和攻击性网络通信进行拦截 B.单点故障

C. 性能 " 瓶颈 " D.误报和漏报

11. 网络安全扫描能够一一一。

A. 发现目标主机或网络 B.判断操作系统类型

C. 确认开放的端口 D.识别网络和拓扑结构

E. 测试系统是否存在安全漏洞

12. 主机型漏洞扫描器可能具备的功能有一一一。

A. 重要资料锁定 : 利用安全的校验和机制来监控重要的主机资料或程序的完整性

B. 弱口令检查 : 采用结合系统信息、字典和词汇组合等的规则来检查弱口令

C. 系统日志和文本文件分析 : 针对系统日志档案，如 UNIX 的 syslogs 及 NT 的事件 日志 (Event Log), 以及其他文本文件的内容做分析

D. 动态报警 : 当遇到违反扫描策略或发现已知安全漏洞时，提供及时的告警。告警 可以采取多种方式，可以是声音、弹出窗口、电子邮件甚至手机短信等

E. 分析报告 : 产生分析报告，并告诉管理员如何弥补漏洞

13. 下面对于 x-scan 扫描器的说法，正确的有一一 -O

A. 可以进行端目扫描

B. 含有攻击模块，可以针对识别到的漏洞自动发起攻击

C. 对于一些已知的 CGI 和 RPC 漏洞 ,x-scan 给出了相应的漏洞描述以及已有的通过此漏洞进行攻击的工具

D. 需要网络中每个主机的管理员权限也

E. 可以多线程扫描

14. 下面软件产品中，一一一是漏洞扫描器。

A.X-scan B.nmap C.Internet Scanner D.norton AntiVirus E.Snort

15. 隔离网闸的三个组成部分是一一一。

A. 漏洞扫描单元 B.入侵检测单元

C. 内网处理单元 D.外网处理单元

E. 专用隔离硬件交换单元

16. 网闸可能应用在一一一 -

A. 涉密网与非涉密网之间 B.办公网与业务网之间

C. 电子政务的内网与专网之间 D.业务网与互联网之间

E. 局域网与互联网之间

17. 下面不是网络端口扫描技术的是

A. 全连接扫描 B.半连接扫描

C. 插件扫描 D.特征匹配扫描

E. 源码扫描

18. 按照 2000 年 3 月公布的《计算机病毒防治管理办法》对计算机病毒的定义，下列属于计算机病毒的有

A. 某 Word 文档携带的宏代码，当打开此文档时宏代码会搜索并感染计算机上所有 的 Word 文档

B. 某用户收到来自朋友的一封电子邮件，当打开邮件附件时，邮件附件将自身发送 给该用户地址簿中前五个邮件地址

C. 某员工在公司内部使用的系统中加入一个逻辑炸弹，如果该员工在一年内被解雇 则逻辑炸弹就会破坏系统

D. 黑客人侵了某服务器，并在其上安装了一个后门程序

E. 某 QQ 用户打开了朋友发送来的一个链接后，发现每次有好友上线 QQ 都会自动 发送一个携带该链接的消息

19. 病毒传播的途径有

A. 移动硬盘 B. 内存条

C. 电子邮件 D. 聊天程序

E 网络浏览

20. 可能和计算机病毒有关的现象有

A. 可执行文件大小改变了

B. 在向写保护的 U 盘复制文件时屏幕上出现 U 盘写保护的提示

C. 系统频繁死机

D. 内存中有来历不明的进程

E. 计算机主板损坏

四、问答题

1. 简述防火墙策略的创建步骤。

2. 简述内部网络、外部网络和 DMZ 之间的关系。

3. 简述防火墙环境构建准则。

4. 入侵检测技术可分为哪两类 ? 各自的优缺点分别是什么 ?

5. 基于网络的入侵检测系统在网络中的部署位置有哪些 ? 各自的优点是什么 ? 6. 简述 IDS 和 IPS 的关系。

7. 简述基于网络的漏洞扫描器原理。

8. 简述基于网络的漏洞扫描器的不足之处。

9. 简述网络隔离技术原理。

10. 计算机病毒有哪些特征 ?

11. 简述文件型病毒和网络蠕虫病毒的区别。

271

12. 请比较计算机病毒扫描技术中的特征代码技术和校验和技术。

第七章

应用安全

一、判断题

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。√

2. 反向查询方法可以让接收邮件的互联网服务商确认邮件发送者是否就是如其所言的真实地址。√

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。√

4.DKIM(Domainkeys Identified 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 J 性。√

5. 运行防病毒软件可以帮助防止遭受网页仿冒欺诈。√

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。√

7. 网络钓鱼的目标往往是细心选择的一些电子邮件地址。√

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。×

9. 在来自可信站点的电子邮件中输入个人或财务信息是安全的。×

10. 包含收件人个人信息的邮件是可信的。

11. 可以采用内容过滤技术来过滤垃圾邮件。√

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。√

13. 随着应用环境的复杂化和传统安全技术的成熟，整合各种安全模块成为信息安全领域的一个发展趋势√

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才肤内容。√

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。√

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。×

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

18. 对网页请求参数进行验证，可以防止 SQL 注入攻击。√

二、单选题

1. 以下不会帮助减少收到的垃圾邮件数量的是一一一。

A. 使用垃圾邮件筛选器帮助阻止垃圾邮件 .

B. 共享电子邮件地址或即时消息地址时应小心谨慎

C. 安装入侵检测软件

D. 收到垃圾邮件后向有关部门举报

2. 下列不属于垃圾邮件过滤技术的是

A. 软件模拟技术 B.贝叶斯过滤技术

C. 关键字过滤技术 D.黑名单技术

3. 下列技术不支持密码验证的是

A.S/MIME B.PGP

C.AMTP D.SMTP

4. 下列行为允许的有

A. 未经授权利用他人的计算机系统发送互联网电子邮件

B. 将采用在线自动收集、字母或者数字任意组合等手段获得的他人的互联网电子邮 件地址用于出售、共享、交换或者向通过上述方式获得的电子邮件地址发送互联 网电子邮件

C. 未经互联网电子邮件接收者明确同意，向其发送包含商业广告内容的互联网电子 邮件

D. 发送包含商业广告内容的互联网电子邮件时，在互联网电子邮件标题信息前部注 明 " 广告 " 或者 "AD" 字样

5. 下列技术不能使网页被篡改后能够自动恢复的是

A. 限制管理员的权限 B. 轮询检测

C. 事件触发技术 D. 核心内嵌技术

6. 以下不可以表示电子邮件可能是欺骗性的是

A. 它要求您点击电子邮件中的链接并输入您的帐户信息

B. 传达出一种紧迫感

C. 通过姓氏和名字称呼您

D. 它要求您验证某些个人信息

7. 如果您认为您已经落入网络钓鱼的圈套，则应采取措施。

A. 向电子邮件地址或网站被伪造的公司报告该情形

B. 更改帐户的密码

C. 立即检查财务报表

D. 以上全部都是

8. 内容过滤技术的含义不包括

A. 过滤互联网请求从而阻止用户浏览不适当的内容或站点

B. 过滤流入的内容从而阻止潜在的攻击进入用户的网络系统

C. 过滤流出的内容从而阻止敏感数据的泄漏

D. 过滤用户的输入从而阻止用户传播非法内容

9. 下列内容过滤技术中在我国没有得到广泛应用的是

A. 内容分级审查 B. 关键字过滤技术

C. 启发式内容过滤技术 D. 机器学习技术

10. 会让一个用户的 " 删除 " 操作去警告其他许多用户的垃圾邮件过滤技术是一一一。

A. 黑名单 B. 白名单

C. 实时黑名单 D. 分布式适应性黑名单

11. 不需要经常维护的垃圾邮件过滤技术是一一一一。

A. 指纹识别技术 B. 简单 DNS 测试

C. 黑名单技术 D. 关键字过滤

12. 下列关于网络钓鱼的描述不正确的是一一一。

A. 网络钓鱼 (Phishing) 一词，是 "Fishing" 和 "Phone" 的综合体

B. 网络钓鱼都是通过欺骗性的电子邮件来进行诈骗活动

C. 为了消除越来越多的以网络钓鱼和电子邮件欺骗的形式进行的身份盗窃和欺诈行

为，相关行业成立了一个协会一一反网络钓鱼工作小组

D. 网络钓鱼在很多方面和一般垃圾邮件有所不同，理解这些不同点对设计反网络钓 鱼技术至关重要

13. 下面技术中不能防止网络钓鱼攻击的是一一 -J

A. 在主页的底部设有一个明显链接，以提醒用户注意有关电子邮件诈骗的问题

B. 利用数字证书 ( 如 USB KEY) 进行登录

C. 根据互联网内容分级联盟 (ICRA) 提供的内容分级标准对网站内容进行分级

D. 安装杀毒软件和防火墙、及时升级、打补丁、加强员工安全意识

三、多选题

1. 下列邮件为垃圾邮件的有

A. 收件人无法拒收的电子邮件

B. 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件 C. 含有病毒、色情、反动等不良信息或有害信息的邮件

D. 隐藏发件人身份、地址、标题等信息的电子邮件

E. 含有虚假的信息源、发件人、路由等信息的电子邮件

2. 垃圾邮件带来的危害有

A. 垃圾邮件占用很多互联网资源

B. 垃圾邮件浪费广大用户的时间和精力

C. 垃圾邮件提高了某些公司做广告的效益

D. 垃圾邮件成为病毒传播的主要途径

E. 垃圾邮件迫使企业使用最新的操作系统

3. 网页防篡改技术包括

A. 网站采用负载平衡技术 B. 防范网站、网页被篡改

C. 访问网页时需要输入用户名和口令 D. 网页被篡改后能够自动恢复

E 采用 HITPS 协议进行网页传输主

4. 网络钓鱼常用的手段有

A. 利用垃圾邮件 B. 利用假冒网上银行、网上证券网站

C. 利用虚假的电子商务 D. 利用计算机病毒

E. 利用社会工程学

5. 内容过滤的目的包括

A. 阻止不良信息对人们的侵害

B. 规范用户的上网行为，提高工作效率

C. 防止敏感数据的泄漏

D. 遏制垃圾邮件的蔓延

E. 减少病毒对网络的侵害

6. 下面技术为基于源的内容过滤技术的是

A. 内容分级审查 B.DNS 过滤

C.IP 包过滤 D.URL 过滤

E. 关键字过滤技术

7. 内容过滤技术的应用领域包括

A. 防病毒 B.网页防篡改 C. 防火墙 D.入侵检测 E. 反垃圾邮件

四、问答题

1. 什么是垃圾邮件 ?

2. 简述网络钓鱼攻击和一般垃圾邮件之间的区别。 3. 什么是内容过滤技术 ?

一、选择题

1. 计算机网络是地理上分散的多台（C）遵循约定的通信协议，通过软硬件互联的系统。

A. 计算机 B. 主从计算机

C. 自主计算机 D. 数字设备

2. 密码学的目的是（C）。

A. 研究数据加密 B. 研究数据解密

C. 研究数据保密 D. 研究信息安全

3. 假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（A）。

A. 对称加密技术 B. 分组密码技术

C. 公钥加密技术 D. 单向函数密码技术

4. 网络安全最终是一个折衷的方案，即安全强度和安全操作代价的折衷，除增加安全设施投资外，还应考虑（D）。

A. 用户的方便性 B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持

D. 上面3项都是

5．A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送

数字签名M，对信息M加密为：M’= KB公开（KA秘密（M））。B方收到密文的解密方案是

（C）。

A. KB公开（KA秘密（M’）） B. KA公开（KA公开（M’））

C. KA公开（KB秘密（M’）） D. KB秘密（KA秘密（M’））

6. “公开密钥密码体制”的含义是（C）。

A. 将所有密钥公开 B. 将私有密钥公开，公开密钥保密

C. 将公开密钥公开，私有密钥保密 D. 两个密钥相同

二、填空题

密码系统包括以下4个方面：明文空间、密文空间、密钥空间和密码算法。

解密算法D是加密算法E的 逆运算 。

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

如果加密密钥和解密密钥 相同 ，这种密码体制称为对称密码体制。

DES算法密钥是 64 位，其中密钥有效位是 56 位。

RSA算法的安全是基于 分解两个大素数的积 的困难。

公开密钥加密算法的用途主要包括两个方面：密钥分配、数字签名。

消息认证是 验证信息的完整性 ，即验证数据在传送和存储过程中是否被篡改、重放或延迟等。

MAC函数类似于加密，它于加密的区别是MAC函数 不 可逆。

10．Hash函数是可接受 变长 数据输入，并生成 定长 数据输出的函数。

三、问答题

1．简述主动攻击与被动攻击的特点，并列举主动攻击与被动攻击现象。

主动攻击是攻击者通过网络线路将虚假信息或计算机病毒传入信息系统内部，破坏信息的真实性、完整性及系统服务的可用性，即通过中断、伪造、篡改和重排信息内容造成信息破坏，使系统无法正常运行。被动攻击是攻击者非常截获、窃取通信线路中的信息，使信息保密性遭到破坏，信息泄露而无法察觉，给用户带来巨大的损失。

2．简述对称密钥密码体制的原理和特点。

对称密钥密码体制，对于大多数算法，解密算法是加密算法的逆运算，加密密钥和解密密钥相同，同属一类的加密体制。它保密强度高但开放性差，要求发送者和接收者在安全通信之前，需要有可靠的密钥信道传递密钥，而此密钥也必须妥善保管。

3．具有N个节点的网络如果使用公开密钥密码算法，每个节点的密钥有多少？网络中的密钥共有多少？

每个节点的密钥是2个，网络中的密钥共有2N个。

对称密码算法存在哪些问题？

适用于封闭系统，其中的用户是彼此相关并相互信任的，所要防范的是系统外攻击。随

着开放网络环境的安全问题日益突出，而传统的对称密码遇到很多困难：密钥使用一段时间后需要更换，而密钥传送需要可靠的通道；在通信网络中，若所有用户使用相同密钥，则失去保密意义；若使用不同密钥N个人之间就需要N(N-1)/2个密钥，密钥管理困难。无法满足不相识的人之间私人谈话的保密性要求。对称密钥至少是两人共享，不带有个人的特征，因此不能进行数字签名。

IDEA是对称加密算法还是非对称加密算法？加密密钥是多少位？

IDEA是一种对称密钥算法，加密密钥是128位。

什么是序列密码和分组密码？

序列密码是一种对明文中的单个位（有时对字节）运算的算法。分组密码是把明文信息

分割成块结构，逐块予以加密和解密。块的长度由算法设计者预先确定。

简述公开密钥密码机制的原理和特点？

公开密钥密码体制是使用具有两个密钥的编码解码算法，加密和解密的能力是分开的；

这两个密钥一个保密，另一个公开。根据应用的需要，发送方可以使用接收方的公开密钥加密消息，或使用发送方的私有密钥签名消息，或两个都使用，以完成某种类型的密码编码解码功能。

什么是MD5？

MD消息摘要算法是由Rivest提出，是当前最为普遍的Hash算法，MD5是第5个版本，

该算法以一个任意长度的消息作为输入，生成128位的消息摘要作为输出，输入消息是按512位的分组处理的。

安全问题概述

一、选择题

1. 信息安全的基本属性是（D）。

A. 机密性 B. 可用性

C. 完整性 D. 上面3项都是

2. “会话侦听和劫持技术”是属于（B）的技术。

A. 密码分析还原 B. 协议漏洞渗透

C. 应用漏洞分析与渗透 D. DOS攻击

3. 对攻击可能性的分析在很大程度上带有（B）。

A. 客观性 B. 主观性

C. 盲目性 D. 上面3项都不是

4. 从安全属性对各种网络攻击进行分类，阻断攻击是针对（B）的攻击。

A. 机密性 B. 可用性 C. 完整性 D. 真实性

5. 从安全属性对各种网络攻击进行分类，截获攻击是针对（A）的攻击。

A. 机密性 B. 可用性 C. 完整性 D. 真实性

6. 从攻击方式区分攻击类型，可分为被动攻击和主动攻击。被动攻击难以（C），然而（C）这些攻击是可行的；主动攻击难以（C），然而（C）这些攻击是可行的。

A. 阻止,检测,阻止,检测 B. 检测,阻止,检测,阻止

C. 检测,阻止,阻止,检测 D. 上面3项都不是

7. 窃听是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接收站之间。截获是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接受站之间。

A. 被动,无须,主动,必须 B. 主动,必须,被动,无须

C. 主动,无须,被动,必须 D. 被动,必须,主动,无须

8. 拒绝服务攻击的后果是（E）。

A. 信息不可用 B. 应用程序不可用

C. 系统宕机 D. 阻止通信 E. 上面几项都是

9. 机密性服务提供信息的保密，机密性服务包括（D）。

A. 文件机密性 B. 信息传输机密性

C. 通信流的机密性 D. 以上3项都是

10．最新的研究和统计表明，安全攻击主要来自（B）。

A. 接入网 B. 企业内部网 C. 公用IP网 D. 个人网

11．攻击者用传输数据来冲击网络接口，使服务器过于繁忙以至于不能应答请求的攻击方

式是（A）。

A. 拒绝服务攻击 B. 地址欺骗攻击

C. 会话劫持 D. 信号包探测程序攻击

12．攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息

重新发往B称为（D）。

A. 中间人攻击 B. 口令猜测器和字典攻击

C. 强力攻击 D. 回放攻击

二、问答题

请解释5种“窃取机密攻击”方式的含义。

1）网络踩点（Footprinting）

攻击者事先汇集目标的信息，通常采用Whois、Finger、Nslookup、Ping等工具获得目标的一些信息，如域名、IP地址、网络拓扑结构、相关的用户信息等，这往往是黑客入侵所做的第一步工作。

2）扫描攻击（Scanning）

这里的扫描主要指端口扫描，通常采用Nmap等各种端口扫描工具，可以获得目标计算

机的一些有用信息，比如机器上打开了哪些端口，这样就知道开设了哪些网络服务。黑客

就可以利用这些服务的漏洞，进行进一步的入侵。这往往是黑客入侵所做的第二步工作。

3）协议栈指纹（Stack Fingerprinting）鉴别（也称操作系统探测）

黑客对目标主机发出探测包，由于不同OS厂商的IP协议栈实现之间存在许多细微差别，

因此每种OS都有其独特的响应方法，黑客经常能够确定目标主机所运行的OS。这往往也可

以看作是扫描阶段的一部分工作。

4）信息流嗅探（Sniffering）

通过在共享局域网中将某主机网卡设置成混杂（Promiscuous）模式，或在各种局域网

中某主机使用ARP欺骗，该主机就会接收所有经过的数据包。基于这样的原理，黑客可以

使用一个嗅探器（软件或硬件）对网络信息流进行监视，从而收集到帐号和口令等信息。

这是黑客入侵的第三步工作。

5）会话劫持（Session Hijacking）

所谓会话劫持，就是在一次正常的通信过程中，黑客作为第三方参与到其中，或者是

在数据流里注射额外的信息，或者是将双方的通信模式暗中改变，即从直接联系变成交由

黑客中转。这种攻击方式可认为是黑客入侵的第四步工作——真正的攻击中的一种。

请解释5种“非法访问”攻击方式的含义。

1）口令破解

攻击者可以通过获取口令文件然后运用口令破解工具进行字典攻击或暴力攻击来获得

口令，也可通过猜测或窃听等方式获取口令，从而进入系统进行非法访问，选择安全的口

令非常重要。这也是黑客入侵中真正攻击方式的一种。

2) IP欺骗

攻击者可通过伪装成被信任源IP地址等方式来骗取目标主机的信任，这主要针对Linux

UNIX下建立起IP地址信任关系的主机实施欺骗。这也是黑客入侵中真正攻击方式的一种。

3) DNS欺骗

当DNS服务器向另一个DNS服务器发送某个解析请求（由域名解析出IP地址）时，因

为不进行身份验证，这样黑客就可以冒充被请求方，向请求方返回一个被篡改了的应答（IP

地址），将用户引向黑客设定的主机。这也是黑客入侵中真正攻击方式的一种。

4) 重放（Replay）攻击

在消息没有时间戳的情况下，攻击者利用身份认证机制中的漏洞先把别人有用的消息

记录下来，过一段时间后再发送出去。

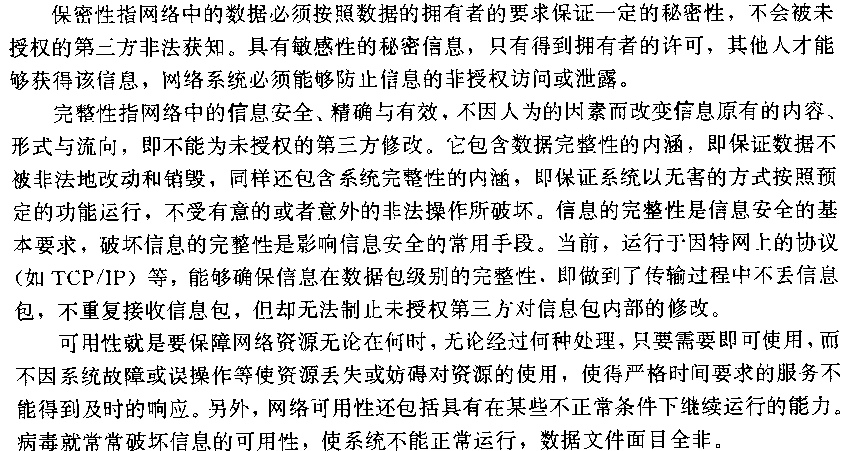
5) 特洛伊木马（Trojan Horse）

把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中，而一

旦用户触发正常程序，黑客代码同时被激活，这些代码往往能完成黑客早已指定的任务（如

监听某个不常用端口，假冒登录界面获取帐号和口令等）。

请解释下列网络信息安全的要素：

保密性、完整性、可用性、可存活性

安全体系结构与模型

一、选择题

1. 网络安全是在分布网络环境中对（D）提供安全保护。

A. 信息载体 B. 信息的处理、传输

C. 信息的存储、访问 D. 上面3项都是

2. ISO 7498-2从体系结构观点描述了5种安全服务，以下不属于这5种安全服务的是（B）。

A. 身份鉴别 B. 数据报过滤

C. 授权控制 D. 数据完整性

3. ISO 7498-2描述了8种特定的安全机制，以下不属于这8种安全机制的是（A）。

A. 安全标记机制 B. 加密机制

C. 数字签名机制 D. 访问控制机制

4. 用于实现身份鉴别的安全机制是（A）。

A. 加密机制和数字签名机制

B. 加密机制和访问控制机制

C. 数字签名机制和路由控制机制

D. 访问控制机制和路由控制机制

5. 在ISO/OSI定义的安全体系结构中，没有规定（E）。

A. 对象认证服务 B.数据保密性安全服务

C. 访问控制安全服务 D. 数据完整性安全服务

E. 数据可用性安全服务

6. ISO定义的安全体系结构中包含（B）种安全服务。

A. 4 B. 5 C. 6 D. 7

7. （D）不属于ISO/OSI安全体系结构的安全机制。

A. 通信业务填充机制 B. 访问控制机制

C. 数字签名机制 D. 审计机制 E. 公证机制

8. ISO安全体系结构中的对象认证服务，使用（B）完成。

A. 加密机制 B. 数字签名机制

C. 访问控制机制 D. 数据完整性机制

9. CA属于ISO安全体系结构中定义的（D）。

A. 认证交换机制 B. 通信业务填充机制

C. 路由控制机制 D. 公证机制

10. 数据保密性安全服务的基础是（D）。

A. 数据完整性机制 B. 数字签名机制

C. 访问控制机制 D. 加密机制

11. 可以被数据完整性机制防止的攻击方式是（D）。

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏

二、填空题

GB/T 9387.2-1995定义了5大类 安全服务 ，提供这些服务的8种 安全机制 以及相应的开放系统互连的安全管理，并可根据具体系统适当地配置于OSI模型的七层协议中。

P2DR的含义是：策略、保护、探测、反应。

三、问答题

列举并解释ISO/OSI中定义的5种标准的安全服务。

（1）鉴别

用于鉴别实体的身份和对身份的证实，包括对等实体鉴别和数据原发鉴别两种。

（2）访问控制

提供对越权使用资源的防御措施。

（3）数据机密性

针对信息泄露而采取的防御措施。分为连接机密性、无连接机密性、选择字段机密性、通信业务流机密性四种。

（4）数据完整性

防止非法篡改信息，如修改、复制、插入和删除等。分为带恢复的连接完整性、无恢复的连接完整性、选择字段的连接完整性、无连接完整性、选择字段无连接完整性五种。

（5）抗否认

是针对对方否认的防范措施，用来证实发生过的操作。包括有数据原发证明的抗否认和有交付证明的抗否认两种。

8．TCP/IP协议的网络安全体系结构的基础框架是什么？

由于OSI参考模型与TCP/IP参考模型之间存在对应关系，因此可根据GB/T 9387.2-1995的安全体系框架，将各种安全机制和安全服务映射到TCP/IP的协议集中，从而形成一个基于TCP/IP协议层次的网络安全体系结构。

密钥分配与管理

一、填空题

1．密钥管理的主要内容包括密钥的 生成、分配、使用、存储、备份、恢复和销毁。

2. 密钥生成形式有两种：一种是由 中心集中 生成，另一种是由 个人分散 生成。

密钥的分配是指产生并使使用者获得 密钥 的过程。

密钥分配中心的英文缩写是 KDC 。

二、问答题

1. 常规加密密钥的分配有几种方案，请对比一下它们的优缺点。

1. 集中式密钥分配方案

由一个中心节点或者由一组节点组成层次结构负责密钥的产生并分配给通信的双方，在这种方式下，用户不需要保存大量的会话密钥，只需要保存同中心节点的加密密钥，用于安全传送由中心节点产生的即将用于与第三方通信的会话密钥。这种方式缺点是通信量大，同时需要较好的鉴别功能以鉴别中心节点和通信方。目前这方面主流技术是密钥分配中心KDC技术。我们假定每个通信方与密钥分配中心KDC之间都共享一个惟一的主密钥，并且这个惟一的主密钥是通过其他安全的途径传递。

2. 分散式密钥分配方案

使用密钥分配中心进行密钥的分配要求密钥分配中心是可信任的并且应该保护它免于被破坏。如果密钥分配中心被第三方破坏，那么所有依靠该密钥分配中心分配会话密钥进行通信的所有通信方将不能进行正常的安全通信。如果密钥分配中心被第三方控制，那么所有依靠该密钥分配中心分配会话密钥进行进信的所有通信方之间的通信信息将被第三方窃听到

4. 密钥的产生需要注意哪些问题?

算法的安全性依赖于密钥，如果用一个弱的密钥产生方法，那么整个系统都将是弱的。DES有56位的密钥，正常情况下任何一个56位的数据串都能成为密钥，所以共有256种可能的密钥。在某些实现中，仅允许用ASCII码的密钥，并强制每一字节的最高位为零。有的实现甚至将大写字母转换成小写字母。这些密钥产生程序都使得DES的攻击难度比正常情况下低几千倍。因此，对于任何一种加密方法，其密钥产生方法都不容忽视。

大部分密钥生成算法采用随机过程或者伪随机过程来生成密钥。随机过程一般采用一个随机数发生器，它的输出是一个不确定的值。伪随机过程一般采用噪声源技术，通过噪声源的功能产生二进制的随机序列或与之对应的随机数。

5．KDC在密钥分配过程中充当何种角色？

KDC在密钥分配过程中充当可信任的第三方。KDC保存有每个用户和KDC之间共享的唯一密钥，以便进行分配。在密钥分配过程中，KDC按照需要生成各对端用户之间的会话密钥，并由用户和KDC共享的密钥进行加密，通过安全协议将会话密钥安全地传送给需要进行通信的双方。

数字签名与鉴别协议

一、选择题

1. 数字签名要预先使用单向Hash函数进行处理的原因是（C）。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

二、填空题

数字签名 是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、问答题

1. 数字签名有什么作用？

当通信双方发生了下列情况时，数字签名技术必须能够解决引发的争端：

否认，发送方不承认自己发送过某一报文。

伪造，接收方自己伪造一份报文，并声称它来自发送方。

冒充，网络上的某个用户冒充另一个用户接收或发送报文。

篡改，接收方对收到的信息进行篡改。

2. 请说明数字签名的主要流程。

数字签名通过如下的流程进行：

(1) 采用散列算法对原始报文进行运算，得到一个固定长度的数字串，称为报文摘要(Message Digest)，不同的报文所得到的报文摘要各异，但对相同的报文它的报文摘要却是惟一的。在数学上保证，只要改动报文中任何一位，重新计算出的报文摘要值就会与原先的值不相符，这样就保证了报文的不可更改性。

(2) 发送方用目己的私有密钥对摘要进行加密来形成数字签名。

(3) 这个数字签名将作为报文的附件和报文一起发送给接收方。

(4) 接收方首先对接收到的原始报文用同样的算法计算出新的报文摘要，再用发送方的公开密钥对报文附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的，否则就认为收到的报文是伪造的或者中途被篡改。

3. 数字证书的原理是什么？

数字证书采用公开密钥体制（例如RSA）。每个用户设定一仅为本人所知的私有密钥，用它进行解密和签名；同时设定一公开密钥，为一组用户所共享，用于加密和验证签名。

采用数字证书，能够确认以下两点：

(1) 保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。

(2) 保证信息自签发后到收到为止未曾做过任何修改，签发的信息是真实信息。

身份认证

一、选择题

1. Kerberos的设计目标不包括（B）。

A. 认证 B.授权 C.记账 D.审计

2. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（B）。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

3. 基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（C）。

A. 公钥认证 B. 零知识认证

C. 共享密钥认证 D. 口令认证

5．（C）是一个对称DES加密系统，它使用一个集中式的专钥密码功能，系统的核心是KDC。

A. TACACS B. RADIUS C. Kerberos D. PKI

二、填空题

身份认证是 验证信息发送者是真的 ，而不是冒充的，包括信源、信宿等的认证和识别。

三、问答题

解释身份认证的基本概念。

身份认证是指用户必须提供他是谁的证明，这种证实客户的真实身份与其所声称的身份是否相符的过程是为了限制非法用户访问网络资源，它是其他安全机制的基础。

身份认证是安全系统中的第一道关卡，识别身份后，由访问监视器根据用户的身份和授权数据库决定是否能够访问某个资源。一旦身份认证系统被攻破，系统的所有安全措施将形同虚设，黑客攻击的目标往往就是身份认证系统。

2. 单机状态下验证用户身份的三种因素是什么？

（1）用户所知道的东西：如口令、密码。

（2）用户所拥有的东西：如智能卡、身份证。

（3）用户所具有的生物特征：如指纹、声音、视网膜扫描、DNA等。

3. 有哪两种主要的存储口令的方式，各是如何实现口令验证的？

1. 直接明文存储口令

有很大风险，只要得到了存储口令的数据库，就可以得到全体人员的口令。比如攻击者可以设法得到一个低优先级的帐号和口令，进入系统后得到明文存储口令的文件，这样他就可以得到全体人员的口令。

2. Hash散列存储口令

散列函数的目的是为文件、报文或其他分组数据产生“指纹”。对于每一个用户，系统存储帐号和散列值对在一个口令文件中，当用户登录时，用户输入口令x，系统计算F(x)，然后与口令文件中相应的散列值进行比对，成功即允许登录。

5. 使用口令进行身份认证的优缺点？

优点在于黑客即使得到了口令文件，通过散列值想要计算出原始口令在计算上也是不可能的，这就相对增加了安全性。

严重的安全问题（单因素的认证），安全性仅依赖于口令，而且用户往往选择容易记忆、

容易被猜测的口令（安全系统最薄弱的突破口），口令文件也可被进行离线的字典式攻击。

6. 利用智能卡进行的双因素的认证方式的原理是什么？

智能卡具有硬件加密功能，有较高的安全性。每个用户持有一张智能卡，智能卡存储用户个性化的秘密信息，同时在验证服务器中也存放该秘密信息。进行认证时，用户输入PIN（个人身份识别码），智能卡认证PIN，成功后，即可读出智能卡中的秘密信息，进而利用该秘密信息与主机之间进行认证。

双因素的认证方式（PIN+智能卡），即使PIN或智能卡被窃取，用户仍不会被冒充。智能卡提供硬件保护措施和加密算法，可以利用这些功能加强安全性能。

7. 有哪些生物特征可以作为身份认证的依据，这种认证的过程是怎样的？

以人体唯一的、可靠的、稳定的生物特征（如指纹、虹膜、脸部、掌纹等）为依据，采用计算机强大的计算功能和网络技术进行图象处理和模式识别。该技术具有很好的安全性、可靠性和有效性。

所有的工作有4个步骤：抓图、抽取特征、比较和匹配。生物捕捉系统捕捉到生物特征的样品，唯一的特征将会被提取并且被转化成数字符号，这些符号被存成那个人的特征摸板，人们同识别系统交互进行身份认证，以确定匹配或不匹配

授权与访问控制

一、选择题

1. 访问控制是指确定（A）以及实施访问权限的过程。

A. 用户权限 B. 可给予哪些主体访问权利

C. 可被用户访问的资源 D. 系统是否遭受入侵

2. 下列对访问控制影响不大的是（D）。

A. 主体身份 B. 客体身份

C. 访问类型 D. 主体与客体的类型

3. 为了简化管理，通常对访问者（A），以避免访问控制表过于庞大。

A. 分类组织成组 B. 严格限制数量

C. 按访问时间排序，删除长期没有访问的用户

D. 不作任何限制

二、填空题

访问控制 的目的是为了限制访问主体对访问客体的访问权限。

三、问答题

解释访问控制的基本概念。

访问控制是建立在身份认证基础上的，通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

访问控制的目的：限制主体对访问客体的访问权限（安全访问策略），从而使计算机系统在合法范围内使用。

2. 访问控制有几种常用的实现方法？它们各有什么特点？

1 访问控制矩阵

行表示客体（各种资源），列表示主体（通常为用户），行和列的交叉点表示某个主体对某个客体的访问权限。通常一个文件的Own权限表示可以授予（Authorize）或撤消（Revoke）其他用户对该文件的访问控制权限。

2 访问能力表

实际的系统中虽然可能有很多的主体与客体，但两者之间的权限关系可能并不多。为了减轻系统的开销与浪费，我们可以从主体（行）出发，表达矩阵某一行的信息，这就是访问能力表（Capabilities）。

只有当一个主体对某个客体拥有访问的能力时，它才能访问这个客体。但是要从访问能力表获得对某一特定客体有特定权限的所有主体就比较困难。在一个安全系统中，正是客体本身需要得到可靠的保护，访问控制服务也应该能够控制可访问某一客体的主体集合，于是出现了以客体为出发点的实现方式——ACL。

3 访问控制表

也可以从客体（列）出发，表达矩阵某一列的信息，这就是访问控制表（Access Control

List）。它可以对某一特定资源指定任意一个用户的访问权限，还可以将有相同权限的用户分组，并授予组的访问权。

4 授权关系表

授权关系表（Authorization Relations）的每一行表示了主体和客体的一个授权关系。对表按客体进行排序，可以得到访问控制表的优势；对表按主体进行排序，可以得到访问能力表的优势。适合采用关系数据库来实现。

3. 访问控制表ACL有什么优缺点？

ACL的优点：表述直观、易于理解，比较容易查出对某一特定资源拥有访问权限的所有用户，有效地实施授权管理。

ACL应用到规模大的企业内部网时，有问题：

（1）网络资源很多，ACL需要设定大量的表项，而且修改起来比较困难，实现整个组织

范围内一致的控制政策也比较困难。

（2）单纯使用ACL，不易实现最小权限原则及复杂的安全政策。

4. 有哪几种访问控制策略？

三种不同的访问控制策略：自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC），前两种属于传统的访问控制策略，而RBAC是90年代后期出现的，有很大的优势，所以发展很快。

每种策略并非是绝对互斥的，我们可以把几种策略综合起来应用从而获得更好、更安全的系统保护——多重的访问控制策略。

PKI技术

一、选择题

1. PKI支持的服务不包括（D）。

A. 非对称密钥技术及证书管理 B. 目录服务

C. 对称密钥的产生和分发 D. 访问控制服务

2. PKI的主要组成不包括（B）。

A. 证书授权CA B. SSL

C. 注册授权RA D. 证书存储库CR

3. PKI管理对象不包括（A）。

A. ID和口令 B. 证书

C. 密钥 D. 证书撤消

4. 下面不属于PKI组成部分的是（D）。

A. 证书主体 B. 使用证书的应用和系统

C. 证书权威机构 D. AS

PKI能够执行的功能是（A）和（C）。

A. 鉴别计算机消息的始发者 B. 确认计算机的物理位置

C. 保守消息的机密 D. 确认用户具有的安全性特权

二、问答题

1. 为什么说在PKI中采用公钥技术的关键是如何确认某个人真正的公钥？如何确认？

信息的可认证性是信息安全的一个重要方面。认证的目的有两个：一个是验证信息发送者的真实性，确认他没有被冒充；另一个是验证信息的完整性，确认被验证的信息在传递或存储过程中没有被篡改、重组或延迟。

在认证体制中，通常存在一个可信的第三方，用于仲裁、颁发证书和管理某些机密信息。公钥密码技术可以提供网络中信息安全的全面解决方案。采用公钥技术的关键是如何确认某个人真正的公钥。在PKI中，为了确保用户及他所持有密钥的正确性，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心(CA)，来确认声称拥有公开密钥的人的真正身份。

要确认一个公共密钥，CA首先制作一张“数字证书”，它包含用户身份的部分信息及用户所持有的公开密钥，然后CA利用本身的私钥为数字证书加上数字签名。

任何想发放自己公钥的用户，可以去认证中心(CA)申请自己的证书。CA中心在认证该人的真实身份后，颁发包含用户公钥的数字证书，它包含用户的真实身份、并证实用户公钥的有效期和作用范围(用于交换密钥还是数字签名)。其他用户只要能验证证书是真实的，并且信任颁发证书的CA，就可以确认用户的公钥。

2. 什么是数字证书？现有的数字证书由谁颁发，遵循什么标准，有什么特点？

数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心(CA)作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。认证中心颁发的数字证书均遵循X.509 V3标准。X.509标准在编排公共密钥密码格式方面已被广为接受。X.509证书已应用于许多网络安全，其中包括IPSec(IP安全)、SSL、SET、S/MIME。

3. X.509规范中是如何定义实体A信任实体B的？在PKI中信任又是什么具体含义？

X.509规范中给出了适用于我们目标的定义：

当实体A假定实体B严格地按A所期望的那样行动，则A信任B。在PKI中，我们可以把这个定

义具体化为：如果一个用户假定CA可以把任一公钥绑定到某个实体上，则他信任该CA。

5. 简述认证机构的严格层次结构模型的性质？

层次结构中的所有实体都信任惟一的根CA。在认证机构的严格层次结构中，每个实体(包括中介CA和终端实体)都必须拥有根CA的公钥，该公钥的安装是在这个模型中为随后进行的所有通信进行证书处理的基础，因此，它必须通过一种安全（带外）的方式来完成。

值得注意的是，在一个多层的严格层次结构中．终端实体直接被其上层的CA认证(也就是颁发证书)，但是它们的信任锚是另一个不同的CA (根CA)。

6. Web信任模型有哪些安全隐患？

Web模型在方便性和简单互操作性方面有明显的优势，但是也存在许多安全隐患。例如，因为浏览器的用户自动地信任预安装的所有公钥，所以即使这些根CA中有一个是“坏的”(例如，该CA从没有认真核实被认证的实体)，安全性将被完全破坏。

另外一个潜在的安全隐患是没有实用的机制来撤消嵌入到浏览器中的根密钥。如果发现一个根密钥是“坏的”(就像前而所讨论的那样)或者与根的公钥相应的私钥被泄密了，要使全世界数百万个浏览器都自动地废止该密钥的使用是不可能的。

7. 以用户为中心的信任模型是怎样实现信任关系的？哪个实际系统是使用这种模型的？

PGP最能说明以用户为中心的信任模型，在PGP中，一个用户通过担当CA（签署其他实体的公钥）并使其公钥被其他人所认证来建立（或参加）所谓的信任网（Web of Trust）。

例如，当A1ice收到一个据称属于Bob的证书时，她将发现这个证书是由她不认识的David签署的，但是David的证书是由她认识并且信任的Catherine签署的。在这种情况下，Alice可以决定信任Bob的密钥（即信任从Catherine到David再到Bob的密钥链），也可以决定不信任Bob的密钥（认为“未知的”Bob与“已知的”Catherine之间的“距离大远”）。

因为要依赖于用户自身的行为和决策能力，因此以用户为中心的模型在技术水平较高和利害关系高度一致的群体中是可行的，但是在一般的群体（它的许多用户有极少或者没有安全及PKI的概念）中是不现实的。

10. 构造证书库的最佳方法是什么？

证书库是证书的集中存放地，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。构造证书库的最佳方法是采用支持LDAP协议的目录系统，用户或相关的应用通过LDAP来访问证书库。系统必须确保证书库的完整性，防止伪造、篡改证书。

11. 掌握证书管理有哪3个阶段组成，每个阶段包括哪些具体内容？

1 证书管理

（1）初始化阶段

1. 终端实体注册

终端实体注册是单个用户或进程的身份被建立和验证的过程。注册过程能够通过不同的方法来实现，图示说明了一个实体初始化包括一个RA和一个CA的可能的方案（注意RA部件根本不存在的其他可能方案也是可用的）。终端实体注册是在线执行的，是用注册表格的交换来说明的。注册过程一般要求包括将一个或更多的共享秘密赋给终端实体以便后来在初始化过程中CA确认那个个体。

2. 密钥对产生

密钥资料可以在终端实体注册过程之前或直接响应终端实体注册过程时产生。在RA中或在CA中产生密钥资料是可能的。每个终端实体多个密钥可以被用做支持分离的和截然不同的服务。例如，一个密钥对可以被用作支持不可否认性服务而另一个密钥对可以被用作支持机密性或密钥管理功能（双密钥对模型）。

3. 证书创建和密钥/证书分发

无论密钥在哪里产生，证书创建的职责都将单独地落在被授权的CA上。如果公钥是被终端实体而不是CA所产生的，那么该公钥必须被安全地传送到CA以便其能够被放入证书。

一旦密钥资料和相关的证书已经被产生，它们必须被适当分发。请求证书和从可信实体（即CA）取回证书（以及相关的密钥，如果适用的话）的必要条件是要求一个安全协议机制。

4. 证书分发

如果私钥和相应的公钥证书已经被分发，那么有一种或多种传送给另一个实体的方法：

• 带外分发；

• 在一个公众的资料库或数据库中公布，以使查询和在线检索简便；

• 带内协议分发，例如，包括带有安全E-mail报文的适用的验证证书。

被用做数字签名目的的证书可以仅需要分发给它们的所有者，被用做机密性目的的证书对于发信方必须是容易获得的。

5. 密钥备份和托管

一定比例的加密密钥将因为许多原因（忘记密码、磁盘被破坏、失常的智能卡或雇员被解雇）使这些密钥的所有者无法访问，这就需要事先进行密钥备份。

密钥托管是指把一个秘密的密钥或私钥交由第三方保管，这样做的问题是哪些密钥应委托保管以及谁是可以信任的第三方（政府？）。

（2）颁布阶段

1. 证书检索

证书检索与访问一个终端实体证书的能力有关。检索一个终端实体证书的需求可能被两个不同的使用要求所驱动。

• 加密发给其他实体的数据的需求；

• 验证一个从另一个实体收到的数字签名的需求。

2. 证书验证

证书验证与评估一个给定证书的合法性和证书颁发者的可信赖性有关。证书验证是在基于那个证书被准许加密操作之前进行的。

3. 密钥恢复

密钥管理生命周期包括从远程备份设施（如可信密钥恢复中心或CA）中恢复私有加密密钥的能力。 密钥的恢复能使PKI管理员和终端用户的负担减至最小，这个过程必须尽可能最大程度自动化。

4. 密钥更新

当证书被颁发时，其被赋与一个固定的生存期。当证书“接近”过期时，必须颁发一个新的公/私钥和相关证书，这被称为密钥更新。应该允许一个合理的转变时间使依托方取得新证书，从而避免与过期证书所有有关的服务中断。这个过程是自动的，并对终端用户完全透明。

（3）取消阶段

1. 证书过期

证书在颁布时被赋与一个固定的生存期，在其被建立的有效期结束后，证书将会过期。当一个证书过期后，与该证书有关的终端实体可能发生三件事：

• 没有活动：终端实体不在参加PKI；

• 证书恢复：相同的公钥被加入新有效期的新证书（当与最初证书的颁布有关的环境没有变化时使用，并且它仍然认为是可靠的）；

• 证书更新：一个新的公/私钥对被产生，并且一个新的证书被颁发。

2. 证书撤消

在证书自然过期之前对给定证书的即时取消（可疑的密钥损害、作业状态的变化或者雇佣终止等）。

一个终端用户个人可以亲自初始化自己的证书撤消（例如由于相应私有密钥的可疑损害）。RA可以代表终端用户被用做初始化证书撤消。经授权的管理者也可以有能力撤消终端实体的证书。

3. 密钥历史

由于机密性加密密钥最后要过期，因此可靠安全地存储用做解密的私有密钥是必须的，这被称作密钥历史，否则无法恢复。

4. 密钥档案

可靠地保存已经过期的用于验证数字签名的公钥，以便对历史文档的数字签名进行验证。

12. 什么是X.500目录服务？

X.500是一种CCITT针对已经被ISO接受的目录服务系统的建议，它定义了一个机构如何在一个企业的全局范围内共享名字和与它们相关的对象。

一个完整的X.500系统称为一个“目录”，X.500是层次性的，其中的管理性域(机构、分支、部门和工作组)可以提供这些域内的用户和资源的信息。它被认为是实现一个目录服务的最好途径。

X.500目录服务是一种用于开发一个单位内部人员目录的标准方法，这个目录可以成为全球目录的一部分，任何人都可以查询这个单位中人员的信息。这个目录有一个树型结构：国家，单位(或组织)，部门和个人。一个知名和最大的X.500目录是用于管理域名注册的InterNIC。

X.500目录服务可以向需要访问网络任何地方资源的电子函件系统和应用，或需要知道在网络上的实体名字和地点的管理系统提供信息。这个目录是一个目录信息数据库(DIB)。

13. 什么是X.509方案，它是如何实现数字签名的？

X.509是一种行业标准或者行业解决方案——X.509公共密钥证书，在X.509方案中，默认的加密体制是公钥密码体制。

为进行身份认证，X.509标准及公共密钥加密系统提供了数字签名的方案。用户可生成一段信息及其摘要(指纹)。用户用专用密钥对摘要加密以形成签名，接收者用发送者的公共密钥对签名解密，并将之与收到的信息“指纹”进行比较，以确定其真实性。

15. X.500和LDAP有什么联系和区别？

LDAP协议基于X.500标准，但是比较简单，并且可以根据需要定制，LDAP支持TCP/IP。在企业范围内实现LDAP可以让运行在几乎所有计算机平台上的所有的应用程序从LDAP目录中获取信息（电子邮件地址、邮件路由信息、人力资源数据、公用密钥、联系人列表）。

16. 实施PKI的过程中产生了哪些问题，如何解决？

首先是实施的问题，PKI定义了严格的操作协议和信任层次关系。任何向CA申请数字证书的人必须经过线下(offline)的身份验证(通常由RA完成)，这种身份验证工作很难扩展到整个Internet范围，因此，现今构建的PKI系统都局限在一定范围内，这造成了PKI系统扩展问题。

由于不同PKI系统都定义了各自的信任策略，在进行互相认证的时候，为了避免由于信任策略不同而产生的问题，普遍的做法是忽略信任策略。这样，本质上是管理Internet上的信任关系的PKI就仅仅起到身份验证的作用了。

提出用PMI解决。

17．什么是证书链？根CA证书由谁签发？

由于一个公钥用户拥有的可信证书管理中心数量有限，要与大量不同管理域的用户建立安全通信需要CA建立信任关系，这样就要构造一个证书链。证书链是最常用的用于验证实体它的公钥之间的绑定的方法。一个证书链一般是从根CA证书开始，前一个证书主体是后一个证书的签发者。也就是说，该主题对后一个证书进行了签名。而根CA证书是由根自己签发的。

18．叙述基于X.509数字证书在PKI中的作用。

X.509数字证书是各实体在网络中的身份证明，它证书了实体所声明的身份与其公钥的匹配关系。从公钥管理的机制讲，数字证书是非对称密码体制中密钥管理的媒介。即在非对称密码体制中，公钥的分发、传送是通过数字证书来实现的。通过数字证书，可以提供身份的认证与识别，完整性、保密性和不可否认等安全服务。

电子邮件的安全

一、问答题

1. 电子邮件存在哪些安全性问题？

1）垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷，影响网络传输速度，占用邮件服务器的空间。

2）诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜，发信人能迅速让大量受害者上当。

3）邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为，信箱不能承受时就会崩溃。

4）通过电子邮件传播的病毒通常用VBScript编写，且大多数采用附件的形式夹带在电子邮件中。当收信人打开附件后，病毒会查询他的通讯簿，给其上所有或部分人发信，并将自身放入附件中，以此方式继续传播扩散。

端到端的安全电子邮件技术，能够保证邮件从发出到接收的整个过程中的哪三种安全性？

端到端的安全电子邮件技术，保证邮件从被发出到被接收的整个过程中，内容保密、无法修改、并且不可否认。目前的Internet上，有两套成型的端到端安全电子邮件标准：PGP和S/MIME。它一般只对信体进行加密和签名， 而信头则由于邮件传输中寻址和路由的需要，必须保证原封不动。

为什么PGP在加密明文之前先压缩它？

PGP内核使用Pkzip算法来压缩加密前的明文。一方面对电子邮件而言，压缩后加密再经过7位编码密文有可能比明文更短，这就节省了网络传输的时间。另一方面，经过压缩的明文，实际上相当于多经过了一次变换，信息更加杂乱无章，能更强地抵御攻击。

在服务器端和用户端各有哪些方式防范垃圾邮件？

在服务器端，应该设置发信人身份认证，以防止自己的邮件服务器被选做垃圾邮件的传递者。现在包括不少国内知名电子邮件提供者在内的诸多邮件服务器被国外的拒绝垃圾邮件组织列为垃圾邮件来源。结果是：所有来自该服务器的邮件全部被拒收!

在用户端，防范垃圾邮件有如下方式：

1）不随便公开自己的电子邮件地址，防止其被收入垃圾邮件的发送地址列表。因为有很多软件可以自动收集这些新闻组文章或者论坛中出现过的电子邮件地址。一旦被收入这些

垃圾邮件的地址列表中，一些不怀好意的收集者将出售这些电子邮件地址牟利，然后，很不幸地，这个地址将可能源源不断地收到各种垃圾邮件。

2）尽量采用转发的方式收信，避免直接使用ISP提供的信箱。申请一个转发信箱地址，结合垃圾邮件过滤，然后再转发到自己的真实信箱。实践证明，这的确是一个非常有效的方法。只有结合使用地址过滤和字符串特征过滤才能取得最好的过滤效果。

不要回复垃圾邮件，这是一个诱人进一步上当的花招。

Web与电子商务的安全

一、选择题

1. SSL产生会话密钥的方式是（C）。

A. 从密钥管理数据库中请求获得

B. 每一台客户机分配一个密钥的方式

C. 随机由客户机产生并加密后通知服务器

D. 由服务器产生并分配给客户机

2. （C）属于Web中使用的安全协议。

A. PEM、SSL B. S-HTTP、S/MIME

C. SSL、S-HTTP D. S/MIME、SSL

3. 传输层保护的网络采用的主要技术是建立在（A）基础上的（A）。

A. 可靠的传输服务，安全套接字层SSL协议

B. 不可靠的传输服务，S-HTTP协议

C. 可靠的传输服务， S-HTTP协议

D. 不可靠的传输服务，安全套接字层SSL协议

二、问答题

9、什么是SET电子钱包？

SET交易发生的先决条件是，每个持卡人(客户)必须拥有一个惟一的电子(数字)证书，且由客户确定口令，并用这个口令对数字证书、私钥、信用卡号码及其他信息进行加密存储，这些与符合SET协议的软件一起组成了一个SET电子钱包。

10、简述一个成功的SET交易的标准流程。

(1) 客户在网上商店选中商品并决定使用电子钱包付款，商家服务器上的POS软件发报文给客户的浏览器要求电子钱包付款。

(2) 电子钱包提示客户输入口令后与商家服务器交换“握手”消息，确认客户、商家均为合法，初始化支付请求和支付响应。

(3) 客户的电子钱包形成一个包含购买订单、支付命令(内含加密了的客户信用卡号码)的报文发送给商家。

(4) 商家POS软件生成授权请求报文(内含客户的支付命令)，发给收单银行的支付网关。

(5) 支付网关在确认客户信用卡没有超过透支额度的情况下，向商家发送一个授权响应报文。

(6) 商家向客户的电子钱包发送一个购买响应报文，交易结束，客户等待商家送货上

防火墙技术

一、选择题

1. 一般而言，Internet防火墙建立在一个网络的（C）。

A. 内部子网之间传送信息的中枢

B. 每个子网的内部

C. 内部网络与外部网络的交叉点

D. 部分内部网络与外部网络的结合处

2. 包过滤型防火墙原理上是基于（C）进行分析的技术。

A. 物理层 B. 数据链路层

C. 网络层 D. 应用层

3. 为了降低风险，不建议使用的Internet服务是（D）。

A. Web服务 B. 外部访问内部系统

C. 内部访问Internet D. FTP服务

4. 对非军事DMZ而言，正确的解释是（D）。

A. DMZ是一个真正可信的网络部分

B. DMZ网络访问控制策略决定允许或禁止进入DMZ通信

C. 允许外部用户访问DMZ系统上合适的服务

D. 以上3项都是

5. 对动态网络地址交换（NAT），不正确的说法是（B）。

A. 将很多内部地址映射到单个真实地址

B. 外部网络地址和内部地址一对一的映射

C. 最多可有64000个同时的动态NAT连接

D. 每个连接使用一个端口

以下（D）不是包过滤防火墙主要过滤的信息？

A. 源IP地址 B. 目的IP地址 C. TCP源端口和目的端口 D. 时间

防火墙用于将Internet和内部网络隔离，（B）。

A. 是防止Internet火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

二、填空题

防火墙是位于两个 网络之间 ，一端是 内部网络 ，另一端是 外部网络 。

防火墙系统的体系结构分为 双宿主机体系结构 、屏蔽主机体系结构 、屏蔽子网体系结构。

三、问答题

1. 什么是防火墙，为什么需要有防火墙？

防火墙是一种装置，它是由软件/硬件设备组合而成，通常处于企业的内部局域网与Internet之间，限制Internet用户对内部网络的访问以及管理内部用户访问Internet的权限。换言之，一个防火墙在一个被认为是安全和可信的内部网络和一个被认为是不那么安全和可信的外部网络(通常是Internet)之间提供一个封锁工具。

如果没有防火墙，则整个内部网络的安全性完全依赖于每个主机，因此，所有的主机都必须达到一致的高度安全水平，这在实际操作时非常困难。而防火墙被设计为只运行专用的访问控制软件的设备，没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞，这就使得安全管理变得更为方便，易于控制，也会使内部网络更加安全。

防火墙所遵循的原则是在保证网络畅通的情况下，尽可能保证内部网络的安全。它是一种被动的技术，是一种静态安全部件。

2. 防火墙应满足的基本条件是什么？

作为网络间实施网间访问控制的一组组件的集合，防火墙应满足的基本条件如下：

(1) 内部网络和外部网络之间的所有数据流必须经过防火墙。

(2) 只有符合安全策略的数据流才能通过防火墙。

(3) 防火墙自身具有高可靠性，应对渗透(Penetration)免疫，即它本身是不可被侵入的。

3. 列举防火墙的几个基本功能？

(1) 隔离不同的网络，限制安全问题的扩散，对安全集中管理，简化了安全管理的复杂程度。

(2) 防火墙可以方便地记录网络上的各种非法活动，监视网络的安全性，遇到紧急情况报警。

(3) 防火墙可以作为部署NAT的地点，利用NAT技术，将有限的IP地址动态或静态地与内部的IP地址对应起来，用来缓解地址空间短缺的问题或者隐藏内部网络的结构。

(4) 防火墙是审计和记录Internet使用费用的一个最佳地点。

(5) 防火墙也可以作为IPSec的平台。

(6) 内容控制功能。根据数据内容进行控制，比如防火墙可以从电子邮件中过滤掉垃圾邮件，可以过滤掉内部用户访问外部服务的图片信息。只有代理服务器和先进的过滤才能实现。

防火墙有哪些局限性？

(1) 网络上有些攻击可以绕过防火墙（如拨号）。

(2) 防火墙不能防范来自内部网络的攻击。

(3) 防火墙不能对被病毒感染的程序和文件的传输提供保护。

(4) 防火墙不能防范全新的网络威胁。

(5) 当使用端到端的加密时，防火墙的作用会受到很大的限制。

(6) 防火墙对用户不完全透明，可能带来传输延迟、瓶颈以及单点失效等问题。

(7) 防火墙不能防止数据驱动式攻击。有些表面无害的数据通过电子邮件或其他方式发送到主机上，一旦被执行就形成攻击（附件）。

包过滤防火墙的过滤原理是什么？

包过滤防火墙也称分组过滤路由器，又叫网络层防火墙，因为它是工作在网络层。路由器便是一个网络层防火墙，因为包过滤是路由器的固有属性。它一般是通过检查单个包的地址、协议、端口等信息来决定是否允许此数据包通过，有静态和动态两种过滤方式。

这种防火墙可以提供内部信息以说明所通过的连接状态和一些数据流的内容，把判断的信息同规则表进行比较，在规则表中定义了各种规则来表明是否同意或拒绝包的通过。包过滤防火墙检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则能符合，防火墙就会使用默认规则（丢弃该包）。在制定数据包过滤规则时，一定要注意数据包是双向的。

状态检测防火墙的原理是什么，相对包过滤防火墙有什么优点？

状态检测又称动态包过滤，所以状态检测防火墙又称动态防火墙，最早由CheckPoint提出。

状态检测是一种相当于4、5层的过滤技术，既提供了比包过滤防火墙更高的安全性和更灵活的处理，也避免了应用层网关的速度降低问题。要实现状态检测防火墙，最重要的是实现连接的跟踪功能，并且根据需要可动态地在过滤规则中增加或更新条目。防火墙应当包含关于包最近已经通过它的“状态信息”，以决定是否让来自Internet的包通过或丢弃。

应用层网关的工作过程是什么？它有什么优缺点？

主要工作在应用层，又称为应用层防火墙。它检查进出的数据包，通过自身复制传递数据，防止在受信主机与非受信主机间直接建立联系。应用层网关能够理解应用层上的协议，能够做复杂的访问控制，并做精细的注册和审核。

基本工作过程是：当客户机需要使用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后再由代理服务器将数据传输给客户机。

常用的应用层网关已有相应的代理服务软件，如HTTP、SMTP、FTP、Telnet等，但是对于新开发的应用，尚没有相应的代理服务，它们将通过网络层防火墙和一般的代理服务。

应用层网关有较好的访问控制能力，是目前最安全的防火墙技术。能够提供内容过滤、用户认证、页面缓存和NAT等功能。但实现麻烦，有的应用层网关缺乏“透明度”。应用层网关每一种协议需要相应的代理软件，使用时工作量大，效率明显不如网络层防火墙。

代理服务器有什么优缺点？

代理服务技术的优点是：隐蔽内部网络拓扑信息；网关理解应用协议，可以实施更细粒度的访问控制；较强的数据流监控和报告功能。（主机认证和用户认证）缺点是对每一类应用都需要一个专门的代理，灵活性不够；每一种网络应用服务的安全问题各不相同，分析困难，因此实现困难。速度慢。

静态包过滤和动态包过滤有什么不同？

静态包过滤在遇到利用动态端口的协议时会发生困难，如FTP，防火墙事先无法知道哪些端口需要打开，就需要将所有可能用到的端口打开，会给安全带来不必要的隐患。

而状态检测通过检查应用程序信息(如FTP的PORT和PASV命令)，来判断此端口是否需要临时打开，而当传输结束时，端口又马上恢复为关闭状态。

VPN技术

一、选择题

1. 通常所说的移动VPN是指（A）。

A. Access VPN B. Intranet VPN

C. Extranet VPN D. 以上皆不是

2. 属于第二层的VPN隧道协议有（B）。

A. IPSec B. PPTP C.GRE D. 以上皆不是

3. GRE协议的乘客协议是（D）。

A. IP B. IPX C. AppleTalk D. 上述皆可

4. VPN的加密手段为（C）。

A. 具有加密功能的防火墙

B. 具有加密功能的路由器

C. VPN内的各台主机对各自的信息进行相应的加密

D. 单独的加密设备

6. 将公司与外部供应商、客户及其他利益相关群体相连接的是（B）。

A. 内联网VPN B. 外联网VPN C. 远程接入VPN D. 无线VPN

7. PPTP、L2TP和L2F隧道协议属于（B）协议。

A. 第一层隧道 B. 第二层隧道 C. 第三层隧道 D. 第四层隧道

8．不属于隧道协议的是（C）。

A. PPTP B. L2TP C. TCP/IP D. IPSec

不属于VPN的核心技术是（C）。

A. 隧道技术 B. 身份认证 C. 日志记录 D. 访问控制

10．目前，VPN使用了（A）技术保证了通信的安全性。

隧道协议、身份认证和数据加密

身份认证、数据加密

隧道协议、身份认证

隧道协议、数据加密

（A）通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部

网的远程访问。

A. Access VPN B. Intranet VPN C. Extranet VPN D. Internet VPN

13．L2TP隧道在两端的VPN服务器之间采用（A）来验证对方的身份。

A. 口令握手协议CHAP B. SSL

C. Kerberos D. 数字证书

二、问答题

1. 解释VPN的基本概念。

VPN是Virtual Private Network的缩写，是将物理分布在不同地点的网络通过公用骨干网，尤其是Internet连接而成的逻辑上的虚拟子网。

Virtual是针对传统的企业“专用网络”而言的。VPN则是利用公共网络资源和设备建立一个逻辑上的专用通道，尽管没有自己的专用线路，但它却可以提供和专用网络同样的功能。

Private表示VPN是被特定企业或用户私有的，公共网络上只有经过授权的用户才可以使用。在该通道内传输的数据经过了加密和认证，保证了传输内容的完整性和机密性。

2．简述VPN使用了哪些主要技术。

1）隧道（封装）技术是目前实现不同VPN用户业务区分的基本方式。一个VPN可抽象为一个没有自环的连通图，每个顶点代表一个VPN端点（用户数据进入或离开VPN的设备端口），相邻顶点之间的边表示连结这两对应端点的逻辑通道，即隧道。

隧道以叠加在IP主干网上的方式运行。需安全传输的数据分组经一定的封装处理，从信源的一个VPN端点进入VPN，经相关隧道穿越VPN（物理上穿越不安全的互联网），到达信宿的另一个VPN端点，再经过相应解封装处理，便得到原始数据。（不仅指定传送的路径，在中转节点也不会解析原始数据）

2）当用户数据需要跨越多个运营商的网络时，在连接两个独立网络的节点该用户的数据分组需要被解封装和再次封装，可能会造成数据泄露，这就需要用到加密技术和密钥管理技术。目前主要的密钥交换和管理标准有SKIP和ISAKMP（安全联盟和密钥管理协议）。

3）对于支持远程接入或动态建立隧道的VPN，在隧道建立之前需要确认访问者身份，是否可以建立要求的隧道，若可以，系统还需根据访问者身份实施资源访问控制。这需要访问者与设备的身份认证技术和访问控制技术。

安全扫描技术

一、问答题

1. 简述常见的黑客攻击过程。

1 目标探测和信息攫取

先确定攻击日标并收集目标系统的相关信息。一般先大量收集网上主机的信息，然后根据各系统的安全性强弱确定最后的目标。

1) 踩点（Footprinting）

黑客必须尽可能收集目标系统安全状况的各种信息。Whois数据库查询可以获得很多关于目标系统的注册信息，DNS查询(用Windows/UNIX上提供的nslookup命令客户端)也可令黑客获得关于目标系统域名、IP地址、DNS务器、邮件服务器等有用信息。此外还可以用traceroute工具获得一些网络拓扑和路由信息。

2) 扫描（Scanning）

在扫描阶段，我们将使用各种工具和技巧(如Ping扫射、端口扫描以及操作系统检测等)确定哪些系统存活着、它们在监听哪些端口(以此来判断它们在提供哪些服务)，甚至更进一步地获知它们运行的是什么操作系统。

3) 查点（Enumeration）

从系统中抽取有效账号或导出资源名的过程称为查点，这些信息很可能成为目标系统的祸根。比如说，一旦查点查出一个有效用户名或共享资源，攻击者猜出对应的密码或利用与资源共享协议关联的某些脆弱点通常就只是一个时间问题了。查点技巧差不多都是特定于操作系统的，因此要求使用前面步骤汇集的信息。

2 获得访问权（Gaining Access）

通过密码窃听、共享文件的野蛮攻击、攫取密码文件并破解或缓冲区溢出攻击等来获得系统的访问权限。

3 特权提升（Escalating Privilege）

在获得一般账户后，黑客经常会试图获得更高的权限，比如获得系统管理员权限。通常可以采用密码破解(如用L0phtcrack破解NT的SAM文件)、利用已知的漏洞或脆弱点等技术。

4 窃取（Stealing）

对敏感数据进行篡改、添加、删除及复制（如Windows系统的注册表、UNIX的rhost文件等）。

5 掩盖踪迹（Covering Tracks）

此时最重要就隐藏自己踪迹，以防被管理员发觉，比如清除日志记录、使用rootkits等工具。

6 创建后门（Creating Bookdoor）

在系统的不同部分布置陷阱和后门，以便入侵者在以后仍能从容获得特权访问。

入侵检测与安全审计

一、填空题

1．IDS的物理实现不同，按检测的监控位置划分，入侵检测系统可分为基于 主机的入侵检测系统、基于 网络的入侵检测系统 和 分布式入侵检测系统。

二、问答题

1. 什么是IDS，它有哪些基本功能？

入侵检测系统IDS，它从计算机网络系统中的若干关键点收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门。

1）监测并分析用户和系统的活动，查找非法用户和合法用户的越权操作；

2）核查系统配置和漏洞并提示管理员修补漏洞；

3）评估系统关键资源和数据文件的完整性；

4）识别已知的攻击行为，统计分析异常行为；

5）操作系统日志管理，并识别违反安全策略的用户活动等。

网络病毒防范

一、选择题

1. 计算机病毒是计算机系统中一类隐藏在（C）上蓄意破坏的捣乱程序。

A. 内存 B. 软盘 C. 存储介质 D. 网络

二、填空题

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

2．恶意代码的基本形式还有 后门、逻辑炸弹、特洛伊木马、蠕虫、细菌。

蠕虫是通过 网络 进行传播的。

4．计算机病毒的工作机制有潜伏机制、传染机制、表现机制。

三、问答题

了解基本的计算机病毒防范措施。

计算机病毒防范，是指通过建立合理的计算机病毒防范体系和制度，及时发现计算机病毒侵入，并采取有效的手段阻止计算机病毒的传播和破坏，恢复受影响的计算机系统和数据。

计算机病毒利用读写文件能进行感染，利用驻留内存、截取中断向量等方式能进行传染和破坏。预防计算机病毒就是要监视、跟踪系统内类似的操作，提供对系统的保护，最大限度地避免各种计算机病毒的传染破坏。

9．什么是病毒的特征代码？它有什么作用？

病毒的特征代码是病毒程序编制者用来识别自己编写程序的唯一代码串。因此检测病毒程序可利用病毒的特征代码来检测病毒，以防止病毒程序感染。

10．什么是网络蠕虫？它的传播途径是什么？

网络蠕虫是一种可以通过网络（永久连接网络或拨号网络）进行自身复制的病毒程序。一旦在系统中激活，蠕虫可以表现得象计算机病毒或细菌。可以向系统注入特洛伊木马程序，或者进行任何次数的破坏或毁灭行动。普通计算机病毒需要在计算机的硬件或文件系统中繁殖，而典型的蠕虫程序会在内存中维持一个活动副本。蠕虫是一个独立运行的程序，自身不改变其他的程序，但可以携带一个改变其他程序功能的病毒。

综合习题

一、选择题

1. 计算机网络是地理上分散的多台（C）遵循约定的通信协议，通过软硬件互联的系统。

A. 计算机 B. 主从计算机

C. 自主计算机 D. 数字设备

2. 密码学的目的是（C）。

A. 研究数据加密 B. 研究数据解密

C. 研究数据保密 D. 研究信息安全

3. 假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（A）。

A. 对称加密技术 B. 分组密码技术

C. 公钥加密技术 D. 单向函数密码技术

4. 网络安全最终是一个折衷的方案，即安全强度和安全操作代价的折衷，除增加安全设施投资外，还应考虑（D）。

A. 用户的方便性 B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持

D. 上面3项都是

5．A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送

数字签名M，对信息M加密为：M’= KB公开（KA秘密（M））。B方收到密文的解密方案是

（C）。

A. KB公开（KA秘密（M’）） B. KA公开（KA公开（M’））

C. KA公开（KB秘密（M’）） D. KB秘密（KA秘密（M’））

6. “公开密钥密码体制”的含义是（C）。

A. 将所有密钥公开 B. 将私有密钥公开，公开密钥保密

C. 将公开密钥公开，私有密钥保密 D. 两个密钥相同

二、填空题

密码系统包括以下4个方面：明文空间、密文空间、密钥空间和密码算法。

解密算法D是加密算法E的 逆运算 。

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

如果加密密钥和解密密钥 相同 ，这种密码体制称为对称密码体制。

DES算法密钥是 64 位，其中密钥有效位是 56 位。

RSA算法的安全是基于 分解两个大素数的积 的困难。

公开密钥加密算法的用途主要包括两个方面：密钥分配、数字签名。

消息认证是 验证信息的完整性 ，即验证数据在传送和存储过程中是否被篡改、重放或延迟等。

MAC函数类似于加密，它于加密的区别是MAC函数 不 可逆。

10．Hash函数是可接受 变长 数据输入，并生成 定长 数据输出的函数。

三、问答题

1．简述主动攻击与被动攻击的特点，并列举主动攻击与被动攻击现象。

主动攻击是攻击者通过网络线路将虚假信息或计算机病毒传入信息系统内部，破坏信息的真实性、完整性及系统服务的可用性，即通过中断、伪造、篡改和重排信息内容造成信息破坏，使系统无法正常运行。被动攻击是攻击者非常截获、窃取通信线路中的信息，使信息保密性遭到破坏，信息泄露而无法察觉，给用户带来巨大的损失。

2．简述对称密钥密码体制的原理和特点。

对称密钥密码体制，对于大多数算法，解密算法是加密算法的逆运算，加密密钥和解密密钥相同，同属一类的加密体制。它保密强度高但开放性差，要求发送者和接收者在安全通信之前，需要有可靠的密钥信道传递密钥，而此密钥也必须妥善保管。

3．具有N个节点的网络如果使用公开密钥密码算法，每个节点的密钥有多少？网络中的密钥共有多少？

每个节点的密钥是2个，网络中的密钥共有2N个。

对称密码算法存在哪些问题？

适用于封闭系统，其中的用户是彼此相关并相互信任的，所要防范的是系统外攻击。随

着开放网络环境的安全问题日益突出，而传统的对称密码遇到很多困难：密钥使用一段时间后需要更换，而密钥传送需要可靠的通道；在通信网络中，若所有用户使用相同密钥，则失去保密意义；若使用不同密钥N个人之间就需要N(N-1)/2个密钥，密钥管理困难。无法满足不相识的人之间私人谈话的保密性要求。对称密钥至少是两人共享，不带有个人的特征，因此不能进行数字签名。

IDEA是对称加密算法还是非对称加密算法？加密密钥是多少位？

IDEA是一种对称密钥算法，加密密钥是128位。

什么是序列密码和分组密码？

序列密码是一种对明文中的单个位（有时对字节）运算的算法。分组密码是把明文信息

分割成块结构，逐块予以加密和解密。块的长度由算法设计者预先确定。

简述公开密钥密码机制的原理和特点？

公开密钥密码体制是使用具有两个密钥的编码解码算法，加密和解密的能力是分开的；

这两个密钥一个保密，另一个公开。根据应用的需要，发送方可以使用接收方的公开密钥加密消息，或使用发送方的私有密钥签名消息，或两个都使用，以完成某种类型的密码编码解码功能。

什么是MD5？

MD消息摘要算法是由Rivest提出，是当前最为普遍的Hash算法，MD5是第5个版本，

该算法以一个任意长度的消息作为输入，生成128位的消息摘要作为输出，输入消息是按512位的分组处理的。

安全问题概述

一、选择题

1. 信息安全的基本属性是（D）。

A. 机密性 B. 可用性

C. 完整性 D. 上面3项都是

2. “会话侦听和劫持技术”是属于（B）的技术。

A. 密码分析还原 B. 协议漏洞渗透

C. 应用漏洞分析与渗透 D. DOS攻击

3. 对攻击可能性的分析在很大程度上带有（B）。

A. 客观性 B. 主观性

C. 盲目性 D. 上面3项都不是

4. 从安全属性对各种网络攻击进行分类，阻断攻击是针对（B）的攻击。

A. 机密性 B. 可用性 C. 完整性 D. 真实性

5. 从安全属性对各种网络攻击进行分类，截获攻击是针对（A）的攻击。

A. 机密性 B. 可用性 C. 完整性 D. 真实性

6. 从攻击方式区分攻击类型，可分为被动攻击和主动攻击。被动攻击难以（C），然而（C）这些攻击是可行的；主动攻击难以（C），然而（C）这些攻击是可行的。

A. 阻止,检测,阻止,检测 B. 检测,阻止,检测,阻止

C. 检测,阻止,阻止,检测 D. 上面3项都不是

7. 窃听是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接收站之间。截获是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接受站之间。

A. 被动,无须,主动,必须 B. 主动,必须,被动,无须

C. 主动,无须,被动,必须 D. 被动,必须,主动,无须

8. 拒绝服务攻击的后果是（E）。

A. 信息不可用 B. 应用程序不可用

C. 系统宕机 D. 阻止通信 E. 上面几项都是

9. 机密性服务提供信息的保密，机密性服务包括（D）。

A. 文件机密性 B. 信息传输机密性

C. 通信流的机密性 D. 以上3项都是

10．最新的研究和统计表明，安全攻击主要来自（B）。

A. 接入网 B. 企业内部网 C. 公用IP网 D. 个人网

11．攻击者用传输数据来冲击网络接口，使服务器过于繁忙以至于不能应答请求的攻击方

式是（A）。

A. 拒绝服务攻击 B. 地址欺骗攻击

C. 会话劫持 D. 信号包探测程序攻击

12．攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息

重新发往B称为（D）。

A. 中间人攻击 B. 口令猜测器和字典攻击

C. 强力攻击 D. 回放攻击

二、问答题

请解释5种“窃取机密攻击”方式的含义。

1）网络踩点（Footprinting）

攻击者事先汇集目标的信息，通常采用Whois、Finger、Nslookup、Ping等工具获得目标的一些信息，如域名、IP地址、网络拓扑结构、相关的用户信息等，这往往是黑客入侵所做的第一步工作。

2）扫描攻击（Scanning）

这里的扫描主要指端口扫描，通常采用Nmap等各种端口扫描工具，可以获得目标计算

机的一些有用信息，比如机器上打开了哪些端口，这样就知道开设了哪些网络服务。黑客

就可以利用这些服务的漏洞，进行进一步的入侵。这往往是黑客入侵所做的第二步工作。

3）协议栈指纹（Stack Fingerprinting）鉴别（也称操作系统探测）

黑客对目标主机发出探测包，由于不同OS厂商的IP协议栈实现之间存在许多细微差别，

因此每种OS都有其独特的响应方法，黑客经常能够确定目标主机所运行的OS。这往往也可

以看作是扫描阶段的一部分工作。

4）信息流嗅探（Sniffering）

通过在共享局域网中将某主机网卡设置成混杂（Promiscuous）模式，或在各种局域网

中某主机使用ARP欺骗，该主机就会接收所有经过的数据包。基于这样的原理，黑客可以

使用一个嗅探器（软件或硬件）对网络信息流进行监视，从而收集到帐号和口令等信息。

这是黑客入侵的第三步工作。

5）会话劫持（Session Hijacking）

所谓会话劫持，就是在一次正常的通信过程中，黑客作为第三方参与到其中，或者是

在数据流里注射额外的信息，或者是将双方的通信模式暗中改变，即从直接联系变成交由

黑客中转。这种攻击方式可认为是黑客入侵的第四步工作——真正的攻击中的一种。

请解释5种“非法访问”攻击方式的含义。

1）口令破解

攻击者可以通过获取口令文件然后运用口令破解工具进行字典攻击或暴力攻击来获得

口令，也可通过猜测或窃听等方式获取口令，从而进入系统进行非法访问，选择安全的口

令非常重要。这也是黑客入侵中真正攻击方式的一种。

2) IP欺骗

攻击者可通过伪装成被信任源IP地址等方式来骗取目标主机的信任，这主要针对Linux

UNIX下建立起IP地址信任关系的主机实施欺骗。这也是黑客入侵中真正攻击方式的一种。

3) DNS欺骗

当DNS服务器向另一个DNS服务器发送某个解析请求（由域名解析出IP地址）时，因

为不进行身份验证，这样黑客就可以冒充被请求方，向请求方返回一个被篡改了的应答（IP

地址），将用户引向黑客设定的主机。这也是黑客入侵中真正攻击方式的一种。

4) 重放（Replay）攻击

在消息没有时间戳的情况下，攻击者利用身份认证机制中的漏洞先把别人有用的消息

记录下来，过一段时间后再发送出去。

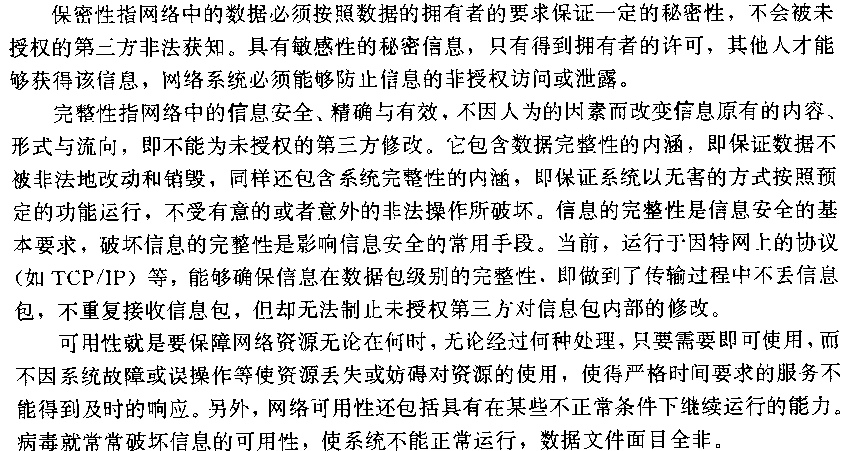
5) 特洛伊木马（Trojan Horse）

把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中，而一

旦用户触发正常程序，黑客代码同时被激活，这些代码往往能完成黑客早已指定的任务（如

监听某个不常用端口，假冒登录界面获取帐号和口令等）。

请解释下列网络信息安全的要素：

保密性、完整性、可用性、可存活性

安全体系结构与模型

一、选择题

1. 网络安全是在分布网络环境中对（D）提供安全保护。

A. 信息载体 B. 信息的处理、传输

C. 信息的存储、访问 D. 上面3项都是

2. ISO 7498-2从体系结构观点描述了5种安全服务，以下不属于这5种安全服务的是（B）。

A. 身份鉴别 B. 数据报过滤

C. 授权控制 D. 数据完整性

3. ISO 7498-2描述了8种特定的安全机制，以下不属于这8种安全机制的是（A）。

A. 安全标记机制 B. 加密机制

C. 数字签名机制 D. 访问控制机制

4. 用于实现身份鉴别的安全机制是（A）。

A. 加密机制和数字签名机制

B. 加密机制和访问控制机制

C. 数字签名机制和路由控制机制

D. 访问控制机制和路由控制机制

5. 在ISO/OSI定义的安全体系结构中，没有规定（E）。

A. 对象认证服务 B.数据保密性安全服务

C. 访问控制安全服务 D. 数据完整性安全服务

E. 数据可用性安全服务

6. ISO定义的安全体系结构中包含（B）种安全服务。

A. 4 B. 5 C. 6 D. 7

7. （D）不属于ISO/OSI安全体系结构的安全机制。

A. 通信业务填充机制 B. 访问控制机制

C. 数字签名机制 D. 审计机制 E. 公证机制

8. ISO安全体系结构中的对象认证服务，使用（B）完成。

A. 加密机制 B. 数字签名机制

C. 访问控制机制 D. 数据完整性机制

9. CA属于ISO安全体系结构中定义的（D）。

A. 认证交换机制 B. 通信业务填充机制

C. 路由控制机制 D. 公证机制

10. 数据保密性安全服务的基础是（D）。

A. 数据完整性机制 B. 数字签名机制

C. 访问控制机制 D. 加密机制

11. 可以被数据完整性机制防止的攻击方式是（D）。

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏

二、填空题

GB/T 9387.2-1995定义了5大类 安全服务 ，提供这些服务的8种 安全机制 以及相应的开放系统互连的安全管理，并可根据具体系统适当地配置于OSI模型的七层协议中。

P2DR的含义是：策略、保护、探测、反应。

三、问答题

列举并解释ISO/OSI中定义的5种标准的安全服务。

（1）鉴别

用于鉴别实体的身份和对身份的证实，包括对等实体鉴别和数据原发鉴别两种。

（2）访问控制

提供对越权使用资源的防御措施。

（3）数据机密性

针对信息泄露而采取的防御措施。分为连接机密性、无连接机密性、选择字段机密性、通信业务流机密性四种。

（4）数据完整性

防止非法篡改信息，如修改、复制、插入和删除等。分为带恢复的连接完整性、无恢复的连接完整性、选择字段的连接完整性、无连接完整性、选择字段无连接完整性五种。

（5）抗否认

是针对对方否认的防范措施，用来证实发生过的操作。包括有数据原发证明的抗否认和有交付证明的抗否认两种。

8．TCP/IP协议的网络安全体系结构的基础框架是什么？

由于OSI参考模型与TCP/IP参考模型之间存在对应关系，因此可根据GB/T 9387.2-1995的安全体系框架，将各种安全机制和安全服务映射到TCP/IP的协议集中，从而形成一个基于TCP/IP协议层次的网络安全体系结构。

密钥分配与管理

一、填空题

1．密钥管理的主要内容包括密钥的 生成、分配、使用、存储、备份、恢复和销毁。

2. 密钥生成形式有两种：一种是由 中心集中 生成，另一种是由 个人分散 生成。

密钥的分配是指产生并使使用者获得 密钥 的过程。

密钥分配中心的英文缩写是 KDC 。

二、问答题

1. 常规加密密钥的分配有几种方案，请对比一下它们的优缺点。

1. 集中式密钥分配方案

由一个中心节点或者由一组节点组成层次结构负责密钥的产生并分配给通信的双方，在这种方式下，用户不需要保存大量的会话密钥，只需要保存同中心节点的加密密钥，用于安全传送由中心节点产生的即将用于与第三方通信的会话密钥。这种方式缺点是通信量大，同时需要较好的鉴别功能以鉴别中心节点和通信方。目前这方面主流技术是密钥分配中心KDC技术。我们假定每个通信方与密钥分配中心KDC之间都共享一个惟一的主密钥，并且这个惟一的主密钥是通过其他安全的途径传递。

2. 分散式密钥分配方案

使用密钥分配中心进行密钥的分配要求密钥分配中心是可信任的并且应该保护它免于被破坏。如果密钥分配中心被第三方破坏，那么所有依靠该密钥分配中心分配会话密钥进行通信的所有通信方将不能进行正常的安全通信。如果密钥分配中心被第三方控制，那么所有依靠该密钥分配中心分配会话密钥进行进信的所有通信方之间的通信信息将被第三方窃听到

4. 密钥的产生需要注意哪些问题?

算法的安全性依赖于密钥，如果用一个弱的密钥产生方法，那么整个系统都将是弱的。DES有56位的密钥，正常情况下任何一个56位的数据串都能成为密钥，所以共有256种可能的密钥。在某些实现中，仅允许用ASCII码的密钥，并强制每一字节的最高位为零。有的实现甚至将大写字母转换成小写字母。这些密钥产生程序都使得DES的攻击难度比正常情况下低几千倍。因此，对于任何一种加密方法，其密钥产生方法都不容忽视。

大部分密钥生成算法采用随机过程或者伪随机过程来生成密钥。随机过程一般采用一个随机数发生器，它的输出是一个不确定的值。伪随机过程一般采用噪声源技术，通过噪声源的功能产生二进制的随机序列或与之对应的随机数。

5．KDC在密钥分配过程中充当何种角色？

KDC在密钥分配过程中充当可信任的第三方。KDC保存有每个用户和KDC之间共享的唯一密钥，以便进行分配。在密钥分配过程中，KDC按照需要生成各对端用户之间的会话密钥，并由用户和KDC共享的密钥进行加密，通过安全协议将会话密钥安全地传送给需要进行通信的双方。

数字签名与鉴别协议

一、选择题

1. 数字签名要预先使用单向Hash函数进行处理的原因是（C）。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

二、填空题

数字签名 是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、问答题

1. 数字签名有什么作用？

当通信双方发生了下列情况时，数字签名技术必须能够解决引发的争端：

否认，发送方不承认自己发送过某一报文。

伪造，接收方自己伪造一份报文，并声称它来自发送方。

冒充，网络上的某个用户冒充另一个用户接收或发送报文。

篡改，接收方对收到的信息进行篡改。

2. 请说明数字签名的主要流程。

数字签名通过如下的流程进行：

(1) 采用散列算法对原始报文进行运算，得到一个固定长度的数字串，称为报文摘要(Message Digest)，不同的报文所得到的报文摘要各异，但对相同的报文它的报文摘要却是惟一的。在数学上保证，只要改动报文中任何一位，重新计算出的报文摘要值就会与原先的值不相符，这样就保证了报文的不可更改性。

(2) 发送方用目己的私有密钥对摘要进行加密来形成数字签名。

(3) 这个数字签名将作为报文的附件和报文一起发送给接收方。

(4) 接收方首先对接收到的原始报文用同样的算法计算出新的报文摘要，再用发送方的公开密钥对报文附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的，否则就认为收到的报文是伪造的或者中途被篡改。

3. 数字证书的原理是什么？

数字证书采用公开密钥体制（例如RSA）。每个用户设定一仅为本人所知的私有密钥，用它进行解密和签名；同时设定一公开密钥，为一组用户所共享，用于加密和验证签名。

采用数字证书，能够确认以下两点：

(1) 保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。

(2) 保证信息自签发后到收到为止未曾做过任何修改，签发的信息是真实信息。

身份认证

一、选择题

1. Kerberos的设计目标不包括（B）。

A. 认证 B.授权 C.记账 D.审计

2. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（B）。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

3. 基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（C）。

A. 公钥认证 B. 零知识认证

C. 共享密钥认证 D. 口令认证

5．（C）是一个对称DES加密系统，它使用一个集中式的专钥密码功能，系统的核心是KDC。

A. TACACS B. RADIUS C. Kerberos D. PKI

二、填空题

身份认证是 验证信息发送者是真的 ，而不是冒充的，包括信源、信宿等的认证和识别。

三、问答题

解释身份认证的基本概念。

身份认证是指用户必须提供他是谁的证明，这种证实客户的真实身份与其所声称的身份是否相符的过程是为了限制非法用户访问网络资源，它是其他安全机制的基础。

身份认证是安全系统中的第一道关卡，识别身份后，由访问监视器根据用户的身份和授权数据库决定是否能够访问某个资源。一旦身份认证系统被攻破，系统的所有安全措施将形同虚设，黑客攻击的目标往往就是身份认证系统。

2. 单机状态下验证用户身份的三种因素是什么？

（1）用户所知道的东西：如口令、密码。

（2）用户所拥有的东西：如智能卡、身份证。

（3）用户所具有的生物特征：如指纹、声音、视网膜扫描、DNA等。

3. 有哪两种主要的存储口令的方式，各是如何实现口令验证的？

1. 直接明文存储口令

有很大风险，只要得到了存储口令的数据库，就可以得到全体人员的口令。比如攻击者可以设法得到一个低优先级的帐号和口令，进入系统后得到明文存储口令的文件，这样他就可以得到全体人员的口令。

2. Hash散列存储口令

散列函数的目的是为文件、报文或其他分组数据产生“指纹”。对于每一个用户，系统存储帐号和散列值对在一个口令文件中，当用户登录时，用户输入口令x，系统计算F(x)，然后与口令文件中相应的散列值进行比对，成功即允许登录。

5. 使用口令进行身份认证的优缺点？

优点在于黑客即使得到了口令文件，通过散列值想要计算出原始口令在计算上也是不可能的，这就相对增加了安全性。

严重的安全问题（单因素的认证），安全性仅依赖于口令，而且用户往往选择容易记忆、

容易被猜测的口令（安全系统最薄弱的突破口），口令文件也可被进行离线的字典式攻击。

6. 利用智能卡进行的双因素的认证方式的原理是什么？

智能卡具有硬件加密功能，有较高的安全性。每个用户持有一张智能卡，智能卡存储用户个性化的秘密信息，同时在验证服务器中也存放该秘密信息。进行认证时，用户输入PIN（个人身份识别码），智能卡认证PIN，成功后，即可读出智能卡中的秘密信息，进而利用该秘密信息与主机之间进行认证。

双因素的认证方式（PIN+智能卡），即使PIN或智能卡被窃取，用户仍不会被冒充。智能卡提供硬件保护措施和加密算法，可以利用这些功能加强安全性能。

7. 有哪些生物特征可以作为身份认证的依据，这种认证的过程是怎样的？

以人体唯一的、可靠的、稳定的生物特征（如指纹、虹膜、脸部、掌纹等）为依据，采用计算机强大的计算功能和网络技术进行图象处理和模式识别。该技术具有很好的安全性、可靠性和有效性。

所有的工作有4个步骤：抓图、抽取特征、比较和匹配。生物捕捉系统捕捉到生物特征的样品，唯一的特征将会被提取并且被转化成数字符号，这些符号被存成那个人的特征摸板，人们同识别系统交互进行身份认证，以确定匹配或不匹配

授权与访问控制

一、选择题

1. 访问控制是指确定（A）以及实施访问权限的过程。

A. 用户权限 B. 可给予哪些主体访问权利

C. 可被用户访问的资源 D. 系统是否遭受入侵

2. 下列对访问控制影响不大的是（D）。

A. 主体身份 B. 客体身份

C. 访问类型 D. 主体与客体的类型

3. 为了简化管理，通常对访问者（A），以避免访问控制表过于庞大。

A. 分类组织成组 B. 严格限制数量

C. 按访问时间排序，删除长期没有访问的用户

D. 不作任何限制

二、填空题

访问控制 的目的是为了限制访问主体对访问客体的访问权限。

三、问答题

解释访问控制的基本概念。

访问控制是建立在身份认证基础上的，通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

访问控制的目的：限制主体对访问客体的访问权限（安全访问策略），从而使计算机系统在合法范围内使用。

2. 访问控制有几种常用的实现方法？它们各有什么特点？

1 访问控制矩阵

行表示客体（各种资源），列表示主体（通常为用户），行和列的交叉点表示某个主体对某个客体的访问权限。通常一个文件的Own权限表示可以授予（Authorize）或撤消（Revoke）其他用户对该文件的访问控制权限。

2 访问能力表

实际的系统中虽然可能有很多的主体与客体，但两者之间的权限关系可能并不多。为了减轻系统的开销与浪费，我们可以从主体（行）出发，表达矩阵某一行的信息，这就是访问能力表（Capabilities）。

只有当一个主体对某个客体拥有访问的能力时，它才能访问这个客体。但是要从访问能力表获得对某一特定客体有特定权限的所有主体就比较困难。在一个安全系统中，正是客体本身需要得到可靠的保护，访问控制服务也应该能够控制可访问某一客体的主体集合，于是出现了以客体为出发点的实现方式——ACL。

3 访问控制表

也可以从客体（列）出发，表达矩阵某一列的信息，这就是访问控制表（Access Control

List）。它可以对某一特定资源指定任意一个用户的访问权限，还可以将有相同权限的用户分组，并授予组的访问权。

4 授权关系表

授权关系表（Authorization Relations）的每一行表示了主体和客体的一个授权关系。对表按客体进行排序，可以得到访问控制表的优势；对表按主体进行排序，可以得到访问能力表的优势。适合采用关系数据库来实现。

3. 访问控制表ACL有什么优缺点？

ACL的优点：表述直观、易于理解，比较容易查出对某一特定资源拥有访问权限的所有用户，有效地实施授权管理。

ACL应用到规模大的企业内部网时，有问题：

（1）网络资源很多，ACL需要设定大量的表项，而且修改起来比较困难，实现整个组织

范围内一致的控制政策也比较困难。

（2）单纯使用ACL，不易实现最小权限原则及复杂的安全政策。

4. 有哪几种访问控制策略？

三种不同的访问控制策略：自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC），前两种属于传统的访问控制策略，而RBAC是90年代后期出现的，有很大的优势，所以发展很快。

每种策略并非是绝对互斥的，我们可以把几种策略综合起来应用从而获得更好、更安全的系统保护——多重的访问控制策略。

PKI技术

一、选择题

1. PKI支持的服务不包括（D）。

A. 非对称密钥技术及证书管理 B. 目录服务

C. 对称密钥的产生和分发 D. 访问控制服务

2. PKI的主要组成不包括（B）。

A. 证书授权CA B. SSL

C. 注册授权RA D. 证书存储库CR

3. PKI管理对象不包括（A）。

A. ID和口令 B. 证书

C. 密钥 D. 证书撤消

4. 下面不属于PKI组成部分的是（D）。

A. 证书主体 B. 使用证书的应用和系统

C. 证书权威机构 D. AS

PKI能够执行的功能是（A）和（C）。

A. 鉴别计算机消息的始发者 B. 确认计算机的物理位置

C. 保守消息的机密 D. 确认用户具有的安全性特权

二、问答题

1. 为什么说在PKI中采用公钥技术的关键是如何确认某个人真正的公钥？如何确认？

信息的可认证性是信息安全的一个重要方面。认证的目的有两个：一个是验证信息发送者的真实性，确认他没有被冒充；另一个是验证信息的完整性，确认被验证的信息在传递或存储过程中没有被篡改、重组或延迟。

在认证体制中，通常存在一个可信的第三方，用于仲裁、颁发证书和管理某些机密信息。公钥密码技术可以提供网络中信息安全的全面解决方案。采用公钥技术的关键是如何确认某个人真正的公钥。在PKI中，为了确保用户及他所持有密钥的正确性，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心(CA)，来确认声称拥有公开密钥的人的真正身份。

要确认一个公共密钥，CA首先制作一张“数字证书”，它包含用户身份的部分信息及用户所持有的公开密钥，然后CA利用本身的私钥为数字证书加上数字签名。

任何想发放自己公钥的用户，可以去认证中心(CA)申请自己的证书。CA中心在认证该人的真实身份后，颁发包含用户公钥的数字证书，它包含用户的真实身份、并证实用户公钥的有效期和作用范围(用于交换密钥还是数字签名)。其他用户只要能验证证书是真实的，并且信任颁发证书的CA，就可以确认用户的公钥。

2. 什么是数字证书？现有的数字证书由谁颁发，遵循什么标准，有什么特点？

数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心(CA)作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。认证中心颁发的数字证书均遵循X.509 V3标准。X.509标准在编排公共密钥密码格式方面已被广为接受。X.509证书已应用于许多网络安全，其中包括IPSec(IP安全)、SSL、SET、S/MIME。

3. X.509规范中是如何定义实体A信任实体B的？在PKI中信任又是什么具体含义？

X.509规范中给出了适用于我们目标的定义：

当实体A假定实体B严格地按A所期望的那样行动，则A信任B。在PKI中，我们可以把这个定

义具体化为：如果一个用户假定CA可以把任一公钥绑定到某个实体上，则他信任该CA。

5. 简述认证机构的严格层次结构模型的性质？

层次结构中的所有实体都信任惟一的根CA。在认证机构的严格层次结构中，每个实体(包括中介CA和终端实体)都必须拥有根CA的公钥，该公钥的安装是在这个模型中为随后进行的所有通信进行证书处理的基础，因此，它必须通过一种安全（带外）的方式来完成。

值得注意的是，在一个多层的严格层次结构中．终端实体直接被其上层的CA认证(也就是颁发证书)，但是它们的信任锚是另一个不同的CA (根CA)。

6. Web信任模型有哪些安全隐患？

Web模型在方便性和简单互操作性方面有明显的优势，但是也存在许多安全隐患。例如，因为浏览器的用户自动地信任预安装的所有公钥，所以即使这些根CA中有一个是“坏的”(例如，该CA从没有认真核实被认证的实体)，安全性将被完全破坏。

另外一个潜在的安全隐患是没有实用的机制来撤消嵌入到浏览器中的根密钥。如果发现一个根密钥是“坏的”(就像前而所讨论的那样)或者与根的公钥相应的私钥被泄密了，要使全世界数百万个浏览器都自动地废止该密钥的使用是不可能的。

7. 以用户为中心的信任模型是怎样实现信任关系的？哪个实际系统是使用这种模型的？

PGP最能说明以用户为中心的信任模型，在PGP中，一个用户通过担当CA（签署其他实体的公钥）并使其公钥被其他人所认证来建立（或参加）所谓的信任网（Web of Trust）。

例如，当A1ice收到一个据称属于Bob的证书时，她将发现这个证书是由她不认识的David签署的，但是David的证书是由她认识并且信任的Catherine签署的。在这种情况下，Alice可以决定信任Bob的密钥（即信任从Catherine到David再到Bob的密钥链），也可以决定不信任Bob的密钥（认为“未知的”Bob与“已知的”Catherine之间的“距离大远”）。

因为要依赖于用户自身的行为和决策能力，因此以用户为中心的模型在技术水平较高和利害关系高度一致的群体中是可行的，但是在一般的群体（它的许多用户有极少或者没有安全及PKI的概念）中是不现实的。

10. 构造证书库的最佳方法是什么？

证书库是证书的集中存放地，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。构造证书库的最佳方法是采用支持LDAP协议的目录系统，用户或相关的应用通过LDAP来访问证书库。系统必须确保证书库的完整性，防止伪造、篡改证书。

11. 掌握证书管理有哪3个阶段组成，每个阶段包括哪些具体内容？

1 证书管理

（1）初始化阶段

1. 终端实体注册

终端实体注册是单个用户或进程的身份被建立和验证的过程。注册过程能够通过不同的方法来实现，图示说明了一个实体初始化包括一个RA和一个CA的可能的方案（注意RA部件根本不存在的其他可能方案也是可用的）。终端实体注册是在线执行的，是用注册表格的交换来说明的。注册过程一般要求包括将一个或更多的共享秘密赋给终端实体以便后来在初始化过程中CA确认那个个体。

2. 密钥对产生

密钥资料可以在终端实体注册过程之前或直接响应终端实体注册过程时产生。在RA中或在CA中产生密钥资料是可能的。每个终端实体多个密钥可以被用做支持分离的和截然不同的服务。例如，一个密钥对可以被用作支持不可否认性服务而另一个密钥对可以被用作支持机密性或密钥管理功能（双密钥对模型）。

3. 证书创建和密钥/证书分发

无论密钥在哪里产生，证书创建的职责都将单独地落在被授权的CA上。如果公钥是被终端实体而不是CA所产生的，那么该公钥必须被安全地传送到CA以便其能够被放入证书。

一旦密钥资料和相关的证书已经被产生，它们必须被适当分发。请求证书和从可信实体（即CA）取回证书（以及相关的密钥，如果适用的话）的必要条件是要求一个安全协议机制。

4. 证书分发

如果私钥和相应的公钥证书已经被分发，那么有一种或多种传送给另一个实体的方法：

• 带外分发；

• 在一个公众的资料库或数据库中公布，以使查询和在线检索简便；

• 带内协议分发，例如，包括带有安全E-mail报文的适用的验证证书。

被用做数字签名目的的证书可以仅需要分发给它们的所有者，被用做机密性目的的证书对于发信方必须是容易获得的。

5. 密钥备份和托管

一定比例的加密密钥将因为许多原因（忘记密码、磁盘被破坏、失常的智能卡或雇员被解雇）使这些密钥的所有者无法访问，这就需要事先进行密钥备份。

密钥托管是指把一个秘密的密钥或私钥交由第三方保管，这样做的问题是哪些密钥应委托保管以及谁是可以信任的第三方（政府？）。

（2）颁布阶段

1. 证书检索

证书检索与访问一个终端实体证书的能力有关。检索一个终端实体证书的需求可能被两个不同的使用要求所驱动。

• 加密发给其他实体的数据的需求；

• 验证一个从另一个实体收到的数字签名的需求。

2. 证书验证

证书验证与评估一个给定证书的合法性和证书颁发者的可信赖性有关。证书验证是在基于那个证书被准许加密操作之前进行的。

3. 密钥恢复

密钥管理生命周期包括从远程备份设施（如可信密钥恢复中心或CA）中恢复私有加密密钥的能力。 密钥的恢复能使PKI管理员和终端用户的负担减至最小，这个过程必须尽可能最大程度自动化。

4. 密钥更新

当证书被颁发时，其被赋与一个固定的生存期。当证书“接近”过期时，必须颁发一个新的公/私钥和相关证书，这被称为密钥更新。应该允许一个合理的转变时间使依托方取得新证书，从而避免与过期证书所有有关的服务中断。这个过程是自动的，并对终端用户完全透明。

（3）取消阶段

1. 证书过期

证书在颁布时被赋与一个固定的生存期，在其被建立的有效期结束后，证书将会过期。当一个证书过期后，与该证书有关的终端实体可能发生三件事：

• 没有活动：终端实体不在参加PKI；

• 证书恢复：相同的公钥被加入新有效期的新证书（当与最初证书的颁布有关的环境没有变化时使用，并且它仍然认为是可靠的）；

• 证书更新：一个新的公/私钥对被产生，并且一个新的证书被颁发。

2. 证书撤消

在证书自然过期之前对给定证书的即时取消（可疑的密钥损害、作业状态的变化或者雇佣终止等）。

一个终端用户个人可以亲自初始化自己的证书撤消（例如由于相应私有密钥的可疑损害）。RA可以代表终端用户被用做初始化证书撤消。经授权的管理者也可以有能力撤消终端实体的证书。

3. 密钥历史

由于机密性加密密钥最后要过期，因此可靠安全地存储用做解密的私有密钥是必须的，这被称作密钥历史，否则无法恢复。

4. 密钥档案

可靠地保存已经过期的用于验证数字签名的公钥，以便对历史文档的数字签名进行验证。

12. 什么是X.500目录服务？

X.500是一种CCITT针对已经被ISO接受的目录服务系统的建议，它定义了一个机构如何在一个企业的全局范围内共享名字和与它们相关的对象。

一个完整的X.500系统称为一个“目录”，X.500是层次性的，其中的管理性域(机构、分支、部门和工作组)可以提供这些域内的用户和资源的信息。它被认为是实现一个目录服务的最好途径。

X.500目录服务是一种用于开发一个单位内部人员目录的标准方法，这个目录可以成为全球目录的一部分，任何人都可以查询这个单位中人员的信息。这个目录有一个树型结构：国家，单位(或组织)，部门和个人。一个知名和最大的X.500目录是用于管理域名注册的InterNIC。

X.500目录服务可以向需要访问网络任何地方资源的电子函件系统和应用，或需要知道在网络上的实体名字和地点的管理系统提供信息。这个目录是一个目录信息数据库(DIB)。

13. 什么是X.509方案，它是如何实现数字签名的？

X.509是一种行业标准或者行业解决方案——X.509公共密钥证书，在X.509方案中，默认的加密体制是公钥密码体制。

为进行身份认证，X.509标准及公共密钥加密系统提供了数字签名的方案。用户可生成一段信息及其摘要(指纹)。用户用专用密钥对摘要加密以形成签名，接收者用发送者的公共密钥对签名解密，并将之与收到的信息“指纹”进行比较，以确定其真实性。

15. X.500和LDAP有什么联系和区别？

LDAP协议基于X.500标准，但是比较简单，并且可以根据需要定制，LDAP支持TCP/IP。在企业范围内实现LDAP可以让运行在几乎所有计算机平台上的所有的应用程序从LDAP目录中获取信息（电子邮件地址、邮件路由信息、人力资源数据、公用密钥、联系人列表）。

16. 实施PKI的过程中产生了哪些问题，如何解决？

首先是实施的问题，PKI定义了严格的操作协议和信任层次关系。任何向CA申请数字证书的人必须经过线下(offline)的身份验证(通常由RA完成)，这种身份验证工作很难扩展到整个Internet范围，因此，现今构建的PKI系统都局限在一定范围内，这造成了PKI系统扩展问题。

由于不同PKI系统都定义了各自的信任策略，在进行互相认证的时候，为了避免由于信任策略不同而产生的问题，普遍的做法是忽略信任策略。这样，本质上是管理Internet上的信任关系的PKI就仅仅起到身份验证的作用了。

提出用PMI解决。

17．什么是证书链？根CA证书由谁签发？

由于一个公钥用户拥有的可信证书管理中心数量有限，要与大量不同管理域的用户建立安全通信需要CA建立信任关系，这样就要构造一个证书链。证书链是最常用的用于验证实体它的公钥之间的绑定的方法。一个证书链一般是从根CA证书开始，前一个证书主体是后一个证书的签发者。也就是说，该主题对后一个证书进行了签名。而根CA证书是由根自己签发的。

18．叙述基于X.509数字证书在PKI中的作用。

X.509数字证书是各实体在网络中的身份证明，它证书了实体所声明的身份与其公钥的匹配关系。从公钥管理的机制讲，数字证书是非对称密码体制中密钥管理的媒介。即在非对称密码体制中，公钥的分发、传送是通过数字证书来实现的。通过数字证书，可以提供身份的认证与识别，完整性、保密性和不可否认等安全服务。

电子邮件的安全

一、问答题

1. 电子邮件存在哪些安全性问题？

1）垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷，影响网络传输速度，占用邮件服务器的空间。

2）诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜，发信人能迅速让大量受害者上当。

3）邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为，信箱不能承受时就会崩溃。

4）通过电子邮件传播的病毒通常用VBScript编写，且大多数采用附件的形式夹带在电子邮件中。当收信人打开附件后，病毒会查询他的通讯簿，给其上所有或部分人发信，并将自身放入附件中，以此方式继续传播扩散。

端到端的安全电子邮件技术，能够保证邮件从发出到接收的整个过程中的哪三种安全性？

端到端的安全电子邮件技术，保证邮件从被发出到被接收的整个过程中，内容保密、无法修改、并且不可否认。目前的Internet上，有两套成型的端到端安全电子邮件标准：PGP和S/MIME。它一般只对信体进行加密和签名， 而信头则由于邮件传输中寻址和路由的需要，必须保证原封不动。

为什么PGP在加密明文之前先压缩它？

PGP内核使用Pkzip算法来压缩加密前的明文。一方面对电子邮件而言，压缩后加密再经过7位编码密文有可能比明文更短，这就节省了网络传输的时间。另一方面，经过压缩的明文，实际上相当于多经过了一次变换，信息更加杂乱无章，能更强地抵御攻击。

在服务器端和用户端各有哪些方式防范垃圾邮件？

在服务器端，应该设置发信人身份认证，以防止自己的邮件服务器被选做垃圾邮件的传递者。现在包括不少国内知名电子邮件提供者在内的诸多邮件服务器被国外的拒绝垃圾邮件组织列为垃圾邮件来源。结果是：所有来自该服务器的邮件全部被拒收!

在用户端，防范垃圾邮件有如下方式：

1）不随便公开自己的电子邮件地址，防止其被收入垃圾邮件的发送地址列表。因为有很多软件可以自动收集这些新闻组文章或者论坛中出现过的电子邮件地址。一旦被收入这些

垃圾邮件的地址列表中，一些不怀好意的收集者将出售这些电子邮件地址牟利，然后，很不幸地，这个地址将可能源源不断地收到各种垃圾邮件。

2）尽量采用转发的方式收信，避免直接使用ISP提供的信箱。申请一个转发信箱地址，结合垃圾邮件过滤，然后再转发到自己的真实信箱。实践证明，这的确是一个非常有效的方法。只有结合使用地址过滤和字符串特征过滤才能取得最好的过滤效果。

不要回复垃圾邮件，这是一个诱人进一步上当的花招。

Web与电子商务的安全

一、选择题

1. SSL产生会话密钥的方式是（C）。

A. 从密钥管理数据库中请求获得

B. 每一台客户机分配一个密钥的方式

C. 随机由客户机产生并加密后通知服务器

D. 由服务器产生并分配给客户机

2. （C）属于Web中使用的安全协议。

A. PEM、SSL B. S-HTTP、S/MIME

C. SSL、S-HTTP D. S/MIME、SSL

3. 传输层保护的网络采用的主要技术是建立在（A）基础上的（A）。

A. 可靠的传输服务，安全套接字层SSL协议

B. 不可靠的传输服务，S-HTTP协议

C. 可靠的传输服务， S-HTTP协议

D. 不可靠的传输服务，安全套接字层SSL协议

二、问答题

9、什么是SET电子钱包？

SET交易发生的先决条件是，每个持卡人(客户)必须拥有一个惟一的电子(数字)证书，且由客户确定口令，并用这个口令对数字证书、私钥、信用卡号码及其他信息进行加密存储，这些与符合SET协议的软件一起组成了一个SET电子钱包。

10、简述一个成功的SET交易的标准流程。

(1) 客户在网上商店选中商品并决定使用电子钱包付款，商家服务器上的POS软件发报文给客户的浏览器要求电子钱包付款。

(2) 电子钱包提示客户输入口令后与商家服务器交换“握手”消息，确认客户、商家均为合法，初始化支付请求和支付响应。

(3) 客户的电子钱包形成一个包含购买订单、支付命令(内含加密了的客户信用卡号码)的报文发送给商家。

(4) 商家POS软件生成授权请求报文(内含客户的支付命令)，发给收单银行的支付网关。

(5) 支付网关在确认客户信用卡没有超过透支额度的情况下，向商家发送一个授权响应报文。

(6) 商家向客户的电子钱包发送一个购买响应报文，交易结束，客户等待商家送货上

防火墙技术

一、选择题

1. 一般而言，Internet防火墙建立在一个网络的（C）。

A. 内部子网之间传送信息的中枢

B. 每个子网的内部

C. 内部网络与外部网络的交叉点

D. 部分内部网络与外部网络的结合处

2. 包过滤型防火墙原理上是基于（C）进行分析的技术。

A. 物理层 B. 数据链路层

C. 网络层 D. 应用层

3. 为了降低风险，不建议使用的Internet服务是（D）。

A. Web服务 B. 外部访问内部系统

C. 内部访问Internet D. FTP服务

4. 对非军事DMZ而言，正确的解释是（D）。

A. DMZ是一个真正可信的网络部分

B. DMZ网络访问控制策略决定允许或禁止进入DMZ通信

C. 允许外部用户访问DMZ系统上合适的服务

D. 以上3项都是

5. 对动态网络地址交换（NAT），不正确的说法是（B）。

A. 将很多内部地址映射到单个真实地址

B. 外部网络地址和内部地址一对一的映射

C. 最多可有64000个同时的动态NAT连接

D. 每个连接使用一个端口

以下（D）不是包过滤防火墙主要过滤的信息？

A. 源IP地址 B. 目的IP地址 C. TCP源端口和目的端口 D. 时间

防火墙用于将Internet和内部网络隔离，（B）。

A. 是防止Internet火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

二、填空题

防火墙是位于两个 网络之间 ，一端是 内部网络 ，另一端是 外部网络 。

防火墙系统的体系结构分为 双宿主机体系结构 、屏蔽主机体系结构 、屏蔽子网体系结构。

三、问答题

1. 什么是防火墙，为什么需要有防火墙？

防火墙是一种装置，它是由软件/硬件设备组合而成，通常处于企业的内部局域网与Internet之间，限制Internet用户对内部网络的访问以及管理内部用户访问Internet的权限。换言之，一个防火墙在一个被认为是安全和可信的内部网络和一个被认为是不那么安全和可信的外部网络(通常是Internet)之间提供一个封锁工具。

如果没有防火墙，则整个内部网络的安全性完全依赖于每个主机，因此，所有的主机都必须达到一致的高度安全水平，这在实际操作时非常困难。而防火墙被设计为只运行专用的访问控制软件的设备，没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞，这就使得安全管理变得更为方便，易于控制，也会使内部网络更加安全。

防火墙所遵循的原则是在保证网络畅通的情况下，尽可能保证内部网络的安全。它是一种被动的技术，是一种静态安全部件。

2. 防火墙应满足的基本条件是什么？

作为网络间实施网间访问控制的一组组件的集合，防火墙应满足的基本条件如下：

(1) 内部网络和外部网络之间的所有数据流必须经过防火墙。

(2) 只有符合安全策略的数据流才能通过防火墙。

(3) 防火墙自身具有高可靠性，应对渗透(Penetration)免疫，即它本身是不可被侵入的。

3. 列举防火墙的几个基本功能？

(1) 隔离不同的网络，限制安全问题的扩散，对安全集中管理，简化了安全管理的复杂程度。

(2) 防火墙可以方便地记录网络上的各种非法活动，监视网络的安全性，遇到紧急情况报警。

(3) 防火墙可以作为部署NAT的地点，利用NAT技术，将有限的IP地址动态或静态地与内部的IP地址对应起来，用来缓解地址空间短缺的问题或者隐藏内部网络的结构。

(4) 防火墙是审计和记录Internet使用费用的一个最佳地点。

(5) 防火墙也可以作为IPSec的平台。

(6) 内容控制功能。根据数据内容进行控制，比如防火墙可以从电子邮件中过滤掉垃圾邮件，可以过滤掉内部用户访问外部服务的图片信息。只有代理服务器和先进的过滤才能实现。

防火墙有哪些局限性？

(1) 网络上有些攻击可以绕过防火墙（如拨号）。

(2) 防火墙不能防范来自内部网络的攻击。

(3) 防火墙不能对被病毒感染的程序和文件的传输提供保护。

(4) 防火墙不能防范全新的网络威胁。

(5) 当使用端到端的加密时，防火墙的作用会受到很大的限制。

(6) 防火墙对用户不完全透明，可能带来传输延迟、瓶颈以及单点失效等问题。

(7) 防火墙不能防止数据驱动式攻击。有些表面无害的数据通过电子邮件或其他方式发送到主机上，一旦被执行就形成攻击（附件）。

包过滤防火墙的过滤原理是什么？

包过滤防火墙也称分组过滤路由器，又叫网络层防火墙，因为它是工作在网络层。路由器便是一个网络层防火墙，因为包过滤是路由器的固有属性。它一般是通过检查单个包的地址、协议、端口等信息来决定是否允许此数据包通过，有静态和动态两种过滤方式。

这种防火墙可以提供内部信息以说明所通过的连接状态和一些数据流的内容，把判断的信息同规则表进行比较，在规则表中定义了各种规则来表明是否同意或拒绝包的通过。包过滤防火墙检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则能符合，防火墙就会使用默认规则（丢弃该包）。在制定数据包过滤规则时，一定要注意数据包是双向的。

状态检测防火墙的原理是什么，相对包过滤防火墙有什么优点？

状态检测又称动态包过滤，所以状态检测防火墙又称动态防火墙，最早由CheckPoint提出。

状态检测是一种相当于4、5层的过滤技术，既提供了比包过滤防火墙更高的安全性和更灵活的处理，也避免了应用层网关的速度降低问题。要实现状态检测防火墙，最重要的是实现连接的跟踪功能，并且根据需要可动态地在过滤规则中增加或更新条目。防火墙应当包含关于包最近已经通过它的“状态信息”，以决定是否让来自Internet的包通过或丢弃。

应用层网关的工作过程是什么？它有什么优缺点？

主要工作在应用层，又称为应用层防火墙。它检查进出的数据包，通过自身复制传递数据，防止在受信主机与非受信主机间直接建立联系。应用层网关能够理解应用层上的协议，能够做复杂的访问控制，并做精细的注册和审核。

基本工作过程是：当客户机需要使用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后再由代理服务器将数据传输给客户机。

常用的应用层网关已有相应的代理服务软件，如HTTP、SMTP、FTP、Telnet等，但是对于新开发的应用，尚没有相应的代理服务，它们将通过网络层防火墙和一般的代理服务。

应用层网关有较好的访问控制能力，是目前最安全的防火墙技术。能够提供内容过滤、用户认证、页面缓存和NAT等功能。但实现麻烦，有的应用层网关缺乏“透明度”。应用层网关每一种协议需要相应的代理软件，使用时工作量大，效率明显不如网络层防火墙。

代理服务器有什么优缺点？

代理服务技术的优点是：隐蔽内部网络拓扑信息；网关理解应用协议，可以实施更细粒度的访问控制；较强的数据流监控和报告功能。（主机认证和用户认证）缺点是对每一类应用都需要一个专门的代理，灵活性不够；每一种网络应用服务的安全问题各不相同，分析困难，因此实现困难。速度慢。

静态包过滤和动态包过滤有什么不同？

静态包过滤在遇到利用动态端口的协议时会发生困难，如FTP，防火墙事先无法知道哪些端口需要打开，就需要将所有可能用到的端口打开，会给安全带来不必要的隐患。

而状态检测通过检查应用程序信息(如FTP的PORT和PASV命令)，来判断此端口是否需要临时打开，而当传输结束时，端口又马上恢复为关闭状态。

VPN技术

一、选择题

1. 通常所说的移动VPN是指（A）。

A. Access VPN B. Intranet VPN

C. Extranet VPN D. 以上皆不是

2. 属于第二层的VPN隧道协议有（B）。

A. IPSec B. PPTP C.GRE D. 以上皆不是

3. GRE协议的乘客协议是（D）。

A. IP B. IPX C. AppleTalk D. 上述皆可

4. VPN的加密手段为（C）。

A. 具有加密功能的防火墙

B. 具有加密功能的路由器

C. VPN内的各台主机对各自的信息进行相应的加密

D. 单独的加密设备

6. 将公司与外部供应商、客户及其他利益相关群体相连接的是（B）。

A. 内联网VPN B. 外联网VPN C. 远程接入VPN D. 无线VPN

7. PPTP、L2TP和L2F隧道协议属于（B）协议。

A. 第一层隧道 B. 第二层隧道 C. 第三层隧道 D. 第四层隧道

8．不属于隧道协议的是（C）。

A. PPTP B. L2TP C. TCP/IP D. IPSec

不属于VPN的核心技术是（C）。

A. 隧道技术 B. 身份认证 C. 日志记录 D. 访问控制

10．目前，VPN使用了（A）技术保证了通信的安全性。

隧道协议、身份认证和数据加密

身份认证、数据加密

隧道协议、身份认证

隧道协议、数据加密

（A）通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部

网的远程访问。

A. Access VPN B. Intranet VPN C. Extranet VPN D. Internet VPN

13．L2TP隧道在两端的VPN服务器之间采用（A）来验证对方的身份。

A. 口令握手协议CHAP B. SSL

C. Kerberos D. 数字证书

二、问答题

1. 解释VPN的基本概念。

VPN是Virtual Private Network的缩写，是将物理分布在不同地点的网络通过公用骨干网，尤其是Internet连接而成的逻辑上的虚拟子网。

Virtual是针对传统的企业“专用网络”而言的。VPN则是利用公共网络资源和设备建立一个逻辑上的专用通道，尽管没有自己的专用线路，但它却可以提供和专用网络同样的功能。

Private表示VPN是被特定企业或用户私有的，公共网络上只有经过授权的用户才可以使用。在该通道内传输的数据经过了加密和认证，保证了传输内容的完整性和机密性。

2．简述VPN使用了哪些主要技术。

1）隧道（封装）技术是目前实现不同VPN用户业务区分的基本方式。一个VPN可抽象为一个没有自环的连通图，每个顶点代表一个VPN端点（用户数据进入或离开VPN的设备端口），相邻顶点之间的边表示连结这两对应端点的逻辑通道，即隧道。

隧道以叠加在IP主干网上的方式运行。需安全传输的数据分组经一定的封装处理，从信源的一个VPN端点进入VPN，经相关隧道穿越VPN（物理上穿越不安全的互联网），到达信宿的另一个VPN端点，再经过相应解封装处理，便得到原始数据。（不仅指定传送的路径，在中转节点也不会解析原始数据）

2）当用户数据需要跨越多个运营商的网络时，在连接两个独立网络的节点该用户的数据分组需要被解封装和再次封装，可能会造成数据泄露，这就需要用到加密技术和密钥管理技术。目前主要的密钥交换和管理标准有SKIP和ISAKMP（安全联盟和密钥管理协议）。

3）对于支持远程接入或动态建立隧道的VPN，在隧道建立之前需要确认访问者身份，是否可以建立要求的隧道，若可以，系统还需根据访问者身份实施资源访问控制。这需要访问者与设备的身份认证技术和访问控制技术。

安全扫描技术

一、问答题

1. 简述常见的黑客攻击过程。

1 目标探测和信息攫取

先确定攻击日标并收集目标系统的相关信息。一般先大量收集网上主机的信息，然后根据各系统的安全性强弱确定最后的目标。

1) 踩点（Footprinting）

黑客必须尽可能收集目标系统安全状况的各种信息。Whois数据库查询可以获得很多关于目标系统的注册信息，DNS查询(用Windows/UNIX上提供的nslookup命令客户端)也可令黑客获得关于目标系统域名、IP地址、DNS务器、邮件服务器等有用信息。此外还可以用traceroute工具获得一些网络拓扑和路由信息。

2) 扫描（Scanning）

在扫描阶段，我们将使用各种工具和技巧(如Ping扫射、端口扫描以及操作系统检测等)确定哪些系统存活着、它们在监听哪些端口(以此来判断它们在提供哪些服务)，甚至更进一步地获知它们运行的是什么操作系统。

3) 查点（Enumeration）

从系统中抽取有效账号或导出资源名的过程称为查点，这些信息很可能成为目标系统的祸根。比如说，一旦查点查出一个有效用户名或共享资源，攻击者猜出对应的密码或利用与资源共享协议关联的某些脆弱点通常就只是一个时间问题了。查点技巧差不多都是特定于操作系统的，因此要求使用前面步骤汇集的信息。

2 获得访问权（Gaining Access）

通过密码窃听、共享文件的野蛮攻击、攫取密码文件并破解或缓冲区溢出攻击等来获得系统的访问权限。

3 特权提升（Escalating Privilege）

在获得一般账户后，黑客经常会试图获得更高的权限，比如获得系统管理员权限。通常可以采用密码破解(如用L0phtcrack破解NT的SAM文件)、利用已知的漏洞或脆弱点等技术。

4 窃取（Stealing）

对敏感数据进行篡改、添加、删除及复制（如Windows系统的注册表、UNIX的rhost文件等）。

5 掩盖踪迹（Covering Tracks）

此时最重要就隐藏自己踪迹，以防被管理员发觉，比如清除日志记录、使用rootkits等工具。

6 创建后门（Creating Bookdoor）

在系统的不同部分布置陷阱和后门，以便入侵者在以后仍能从容获得特权访问。

入侵检测与安全审计

一、填空题

1．IDS的物理实现不同，按检测的监控位置划分，入侵检测系统可分为基于 主机的入侵检测系统、基于 网络的入侵检测系统 和 分布式入侵检测系统。

二、问答题

1. 什么是IDS，它有哪些基本功能？

入侵检测系统IDS，它从计算机网络系统中的若干关键点收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门。

1）监测并分析用户和系统的活动，查找非法用户和合法用户的越权操作；

2）核查系统配置和漏洞并提示管理员修补漏洞；

3）评估系统关键资源和数据文件的完整性；

4）识别已知的攻击行为，统计分析异常行为；

5）操作系统日志管理，并识别违反安全策略的用户活动等。

网络病毒防范

一、选择题

1. 计算机病毒是计算机系统中一类隐藏在（C）上蓄意破坏的捣乱程序。

A. 内存 B. 软盘 C. 存储介质 D. 网络

二、填空题

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

2．恶意代码的基本形式还有 后门、逻辑炸弹、特洛伊木马、蠕虫、细菌。

蠕虫是通过 网络 进行传播的。

4．计算机病毒的工作机制有潜伏机制、传染机制、表现机制。

三、问答题

了解基本的计算机病毒防范措施。

计算机病毒防范，是指通过建立合理的计算机病毒防范体系和制度，及时发现计算机病毒侵入，并采取有效的手段阻止计算机病毒的传播和破坏，恢复受影响的计算机系统和数据。

计算机病毒利用读写文件能进行感染，利用驻留内存、截取中断向量等方式能进行传染和破坏。预防计算机病毒就是要监视、跟踪系统内类似的操作，提供对系统的保护，最大限度地避免各种计算机病毒的传染破坏。

9．什么是病毒的特征代码？它有什么作用？

病毒的特征代码是病毒程序编制者用来识别自己编写程序的唯一代码串。因此检测病毒程序可利用病毒的特征代码来检测病毒，以防止病毒程序感染。

10．什么是网络蠕虫？它的传播途径是什么？

网络蠕虫是一种可以通过网络（永久连接网络或拨号网络）进行自身复制的病毒程序。一旦在系统中激活，蠕虫可以表现得象计算机病毒或细菌。可以向系统注入特洛伊木马程序，或者进行任何次数的破坏或毁灭行动。普通计算机病毒需要在计算机的硬件或文件系统中繁殖，而典型的蠕虫程序会在内存中维持一个活动副本。蠕虫是一个独立运行的程序，自身不改变其他的程序，但可以携带一个改变其他程序功能的病毒。

一、判断题

1.根据IS0 13335标准，信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。 正确

2.信息安全保障阶段中，安全策略是核心，对事先保护、事发检测和响应、事后恢复起到了统一指导作用。 错误

3. 只要投资充足，技术措施完备，就能够保证百分之百的信息安全。 错误

4. 我国在2006年提出的《2006～2020年国家信息化发展战略》将“建设国家信息安全保障体系”作为9大战略发展方向之一。 正确

5.2003年7月国家信息化领导小组第三次会议发布的27号文件，是指导我国信息安全保障工作和加快推进信息化的纲领性文献。 正确

6.在我国，严重的网络犯罪行为也不需要接受刑法的相关处罚。 错误

7.安全管理的合规性，主要是指在有章可循的基础之上，确保信息安全工作符合国家法律、法规、行业标准、机构内部的方针和规定。 正确

8.Windows 2000／xp系统提供了口令安全策略，以对帐户口令安全进行保护。 正确

9.信息安全等同于网络安全。 错误

10.GB 17859与目前等级保护所规定的安全等级的含义不同，GB 17859中等级划分为现在的等级保护奠定了基础。 正确

11.口令认证机制的安全性弱点，可以使得攻击者破解合法用户帐户信息，进而非法获得系统和资源访问权限。正确

12.PKI系统所有的安全操作都是通过数字证书来实现的。 正确

13.PKI系统使用了非对称算法、对称算法和散列算法。 正确

14.一个完整的信息安全保障体系，应当包括安全策略(Policy)、保护(Protection)、检测(Detection)、响应(Reaction)、恢复Restoration)五个主要环节。 正确

15.信息安全的层次化特点决定了应用系统的安全不仅取决于应用层安全机制，同样依赖于底层的物理、网络和系统等层面的安全状况。 正确

16. 实现信息安全的途径要借助两方面的控制措施：技术措施和管理措施，从这里就能看出技术和管理并重的基本思想，重技术轻管理，或者重管理轻技术，都是不科学，并且有局限性的错误观点。正确

17.按照BS 7799标准，信息安全管理应当是一个持续改进的周期性过程。 正确

18.虽然在安全评估过程中采取定量评估能获得准确的分析结果，但是由于参数确定较为困难，往往实际评估多采取定性评估，或者定性和定量评估相结合的方法。 正确

19.一旦发现计算机违法犯罪案件，信息系统所有者应当在2天内迅速向当地公安机关报案，并配合公安机关的取证和调查。错误

20. 定性安全风险评估结果中，级别较高的安全风险应当优先采取控制措施予以应对。 正确

21.网络边界保护中主要采用防火墙系统，为了保证其有效发挥作用，应当避免在内网和外网之间存在不经过防火墙控制的其他通信连接。 正确

22.网络边统，在内网和外网之间存在不经过防火墙控制的其他通信连接，不会影响到防火墙的有效保护作用。 错误

23. 防火墙虽然是网络层重要的安全机制，但是它对于计算机病毒缺乏保护能力。 正确

24. 我国刑法中有关计算机犯罪的规定，定义了3种新的犯罪类型。错误

25. 信息技术基础设施库(ITIL)，是由英国发布的关于IT服务管理最佳实践的建议和指导方针，旨在解决IT服务质量不佳的情况。正确

26.美国国家标准技术协会NIST发布的《SP 800-30》中详细阐述了IT系统风险管理内容。 正确

27.防火墙在静态包过滤技术的基础上，通过会话状态检测技术将数据包的过滤处理效率大幅提高。 正确

28. 通常在风险评估的实践中，综合利用基线评估和详细评估的优点，将二者结合起来。正确

29. 脆弱性分析技术，也被通俗地称为漏洞扫描技术。该技术是检测远程或本地系统安全脆弱性的一种安全技术。 正确

二．单项选择题

30.下列关于信息的说法 \_\_\_\_是错误的。D

A 信息是人类社会发展的重要支柱           B 信息本身是无形的

C 信息具有价值，需要保护           D 信息可以以独立形态存在

31. 信息安全经历了三个发展阶段，以下\_\_\_\_不属于这三个发展阶段。B

A 通信保密阶段           B 加密机阶段           C 信息安全阶段           D 安全保障阶段

32.信息安全在通信保密阶段对信息安全的关注局限在\_\_\_\_安全属性。C

A 不可否认性           B 可用性           C 保密性           D 完整性

33.信息安全在通信保密阶段中主要应用于\_\_\_\_领域。A

A 军事           B 商业           C 科研           D 教育

34.信息安全阶段将研究领域扩展到三个基本属性，下列\_\_\_\_不属于这三个基本属性。C

A 保密性           B 完整性           C 不可否认性           D 可用性

35.安全保障阶段中将信息安全体系归结为四个主要环节，下列\_\_\_\_是正确的。D

A 策略、保护、响应、恢复           B 加密、认证、保护、检测

C 策略、网络攻防、密码学、备份           D 保护、检测、响应、恢复

36. 下面所列的\_\_\_\_安全机制不属于信息安全保障体系中的事先保护环节。A

A 杀毒软件           B 数字证书认证           C 防火墙           D 数据库加密

37. 根据ISO的信息安全定义，下列选项中\_\_\_\_是信息安全三个基本属性之一。B

A 真实性           B 可用性           C 可审计性           D 可靠性

38. 为了数据传输时不发生数据截获和信息泄密，采取了加密机制。这种做法体现了信息安全的\_\_\_\_属性。A

A 保密性           B 完整性           C 可靠性           D 可用性

39. 定期对系统和数据进行备份，在发生灾难时进行恢复。该机制是为了满足信息安全的\_\_\_\_属性。D

A 真实性           B 完整性           C 不可否认性           D 可用性

40. 数据在存储过程中发生了非法访问行为，这破坏了信息安全的\_\_\_\_属性。A

A 保密性           B 完整性           C 不可否认性           D 可用性

41. 网上银行系统的一次转账操作过程中发生了转账金额被非法篡改的行为，这破坏了信息安全的\_\_\_属性。B   A 保密性           B 完整性           C 不可否认性           D 可用性

42. PDR安全模型属于\_\_\_\_类型。A

A 时间模型           B 作用模型           C 结构模型           D 关系模型

43. 《信息安全国家学说》是\_\_\_\_的信息安全基本纲领性文件。C

A 法国           B 美国           C 俄罗斯           D 英国

44.下列的\_\_\_\_犯罪行为不属于我国刑法规定的与计算机有关的犯罪行为。A

A 窃取国家秘密           B 非法侵入计算机信息系统

C 破坏计算机信息系统           D 利用计算机实施金融诈骗

45.我国刑法\_\_\_\_规定了非法侵入计算机信息系统罪。B

A 第284条           B 第285条           C 第286条           D 第287条

46.信息安全领域内最关键和最薄弱的环节是\_\_\_\_。D

A 技术           B 策略           C 管理制度           D 人

47.信息安全管理领域权威的标准是\_\_\_\_。B

A ISO 15408           B ISO 17799／IS0 27001           C IS0 9001           D ISO 14001

48.IS0 17799／IS0 27001最初是由\_\_\_\_提出的国家标准。C

A 美国           B 澳大利亚           C 英国           D 中国

49.IS0 17799的内容结构按照\_\_\_\_进行组织。C

A 管理原则           B 管理框架           C 管理域一控制目标一控制措施           D 管理制度

50.\_\_\_\_对于信息安全管理负有责任。D

A 高级管理层           B 安全管理员           C IT管理员           D 所有与信息系统有关人员

52. 《计算机信息系统安全保护条例》是由中华人民共和国\_\_\_\_第147号发布的。A

A 国务院令           B 全国人民代表大会令           C 公安部令           D 国家安全部令

53. 《互联网上网服务营业场所管理条例》规定，\_\_\_\_负责互联网上网服务营业场所安全审核和对违反网络安全管理规定行为的查处。B

A 人民法院           B 公安机关           C 工商行政管理部门           D 国家安全部门

54. 计算机病毒最本质的特性是\_\_\_\_。C

A 寄生性           B 潜伏性           C 破坏性           D 攻击性

55. \_\_\_\_安全策略是得到大部分需求的支持并同时能够保护企业的利益。A

A 有效的           B 合法的           C 实际的           D 成熟的

56. 在PDR安全模型中最核心的组件是\_\_\_\_。A

A 策略           B 保护措施           C 检测措施           D 响应措施

57. 制定灾难恢复策略，最重要的是要知道哪些是商务工作中最重要的设施，在发生灾难后，这些设施的\_\_。B

A 恢复预算是多少           B 恢复时间是多长C 恢复人员有几个           D 恢复设备有多少

58. 在完成了大部分策略的编制工作后，需要对其进行总结和提炼，产生的成果文档被称为\_\_\_\_。A

A 可接受使用策略AUP           B 安全方针           C 适用性声明           D 操作规范

59. 防止静态信息被非授权访问和防止动态信息被截取解密是\_\_\_\_。D

A 数据完整性           B 数据可用性           C 数据可靠性           D 数据保密性

60. 用户身份鉴别是通过\_\_\_\_完成的。A

A 口令验证           B 审计策略           C 存取控制           D 查询功能

61. 故意输入计算机病毒以及其他有害数据，危害计算机信息系统安全的个人，由公安机关处以\_\_\_\_。B

A 3年以下有期徒刑或拘役           B 警告或者处以5000元以下的罚款

C 5年以上7年以下有期徒刑           D 警告或者15000元以下的罚款

62. 网络数据备份的实现主要需要考虑的问题不包括\_\_\_\_。A

A 架设高速局域网B 分析应用环境           C 选择备份硬件设备           D 选择备份管理软件

63. 《计算机信息系统安全保护条例》规定，对计算机信息系统中发生的案件，有关使用单位应当在\_\_\_\_向当地县级以上人民政府公安机关报告。C

A 8小时内           B 12小时内           C 24小时内           D 48小时内

64. 公安部网络违法案件举报网站的网址是\_\_\_\_。C

A www.netpolice.cn   B www.gongan.cn    C http://www.cyberpolice.cn           D [www.110.cn](http://www.110.cn/)

65. 对于违反信息安全法律、法规行为的行政处罚中，\_\_\_\_是较轻的处罚方式。A

A 警告           B 罚款           C 没收违法所得           D 吊销许可证

66. 对于违法行为的罚款处罚，属于行政处罚中的\_\_\_\_。C

A 人身自由罚           B 声誉罚           C 财产罚           D 资格罚

67. 对于违法行为的通报批评处罚，属于行政处罚中的\_\_\_\_。B

A 人身自由罚           B 声誉罚           C 财产罚           D 资格罚

68. 1994年2月国务院发布的《计算机信息系统安全保护条例》赋予\_\_\_\_对计算机信息系统的安全保护工作行使监督管理职权。C

A 信息产业部           B 全国人大           C 公安机关           D 国家工商总局

69. 《计算机信息网络国际联网安全保护管理办法》规定，互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构)，应当自网络正式联通之日起\_\_\_\_日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。D

A 7           B 10           C 15           D 30

70.互联网服务提供者和联网使用单位落实的记录留存技术措施，应当具有至少保存\_\_\_天记录备份的功能。C

A 10           B 30           C 60           D 90

71. 对网络层数据包进行过滤和控制的信息安全技术机制是\_\_\_\_。A

A 防火墙           B IDS           C Sniffer           D IPSec

72. 下列不属于防火墙核心技术的是\_\_\_\_。D

A (静态／动态)包过滤技术           B NAT技术           C 应用代理技术           D 日志审计

73. 应用代理防火墙的主要优点是\_\_\_\_。B

A 加密强度更高           B 安全控制更细化、更灵活           C 安全服务的透明性更好           D 服务对象更广泛

74. 安全管理中经常会采用“权限分离”的办法，防止单个人员权限过高，出现内部人员的违法犯罪行为，“权限分离”属于\_\_\_\_控制措施。A

A 管理           B 检测           C 响应           D 运行

75.安全管理中采用的“职位轮换”或者“强制休假”办法是为了发现特定的岗位人员是否存在违规操作行为，属于\_\_\_\_控制措施。B

A 管理           B 检测           C 响应           D 运行

76. 下列选项中不属于人员安全管理措施的是\_\_\_\_。A

A 行为监控           B 安全培训           C 人员离岗           D 背景／技能审查

77. 《计算机病毒防治管理办法》规定，\_\_\_\_主管全国的计算机病毒防治管理工作。C

A 信息产业部           B 国家病毒防范管理中心

C 公安部公共信息网络安全监察           D 国务院信息化建设领导小组

78. 计算机病毒的实时监控属于\_\_\_\_类的技术措施。B

A 保护           B 检测           C 响应           D 恢复

79. 针对操作系统安全漏洞的蠕虫病毒根治的技术措施是\_\_\_\_。B

A 防火墙隔离     B 安装安全补丁程序     C 专用病毒查杀工具    D 部署网络入侵检测系统

80. 下列能够有效地防御未知的新病毒对信息系统造成破坏的安全措施是\_\_\_\_。A

A 防火墙隔离B 安装安全补丁程序C 专用病毒查杀工具    D 部署网络入侵检测系统

81. 下列不属于网络蠕虫病毒的是\_\_\_\_。C

A 冲击波           B SQLSLAMMER           C CIH           D 振荡波

82. 传统的文件型病毒以计算机操作系统作为攻击对象，而现在越来越多的网络蠕虫病毒将攻击范围扩大到了\_\_\_\_等重要网络资源。A

A 网络带宽           B 数据包           C 防火墙           D LINUX

83. 不是计算机病毒所具有的特点\_\_\_\_。D

A 传染性           B 破坏性           C 潜伏性           D 可预见性

84. 关于灾难恢复计划错误的说法是\_\_\_\_。C

A 应考虑各种意外情况           B 制定详细的应对处理办法

C 建立框架性指导原则，不必关注于细节           D 正式发布前，要进行讨论和评审

85. 对远程访问型VPN来说，\_\_产品经常与防火墙及NAT机制存在兼容性问题，导致安全隧道建立失败。A

A IPSec VPN           B SSL VPN           C MPLS VPN           D L2TP VPN

86. 1999年，我国发布的第一个信息安全等级保护的国家标准GB 17859—1999，提出将信息系统的安全等级划分为\_\_\_\_个等级，并提出每个级别的安全功能要求。D

A 7           B 8           C 6           D 5

87. 等级保护标准GB l7859主要是参考了\_\_\_\_而提出。B

A 欧洲ITSEC           B 美国TCSEC           C CC           D BS 7799

88. 我国在1999年发布的国家标准\_\_\_\_为信息安全等级保护奠定了基础。C

A GB 17799           B GB 15408           C GB 17859           D GB 14430

89. 信息安全等级保护的5个级别中，\_\_\_\_是最高级别，属于关系到国计民生的最关键信息系统的保护。B

A 强制保护级           B 专控保护级    C 监督保护级           D 指导保护级           E 自主保护级

90. 《信息系统安全等级保护实施指南》将\_\_\_\_作为实施等级保护的第一项重要内容。A

A 安全定级           B 安全评估           C 安全规划           D 安全实施

91. \_\_\_是进行等级确定和等级保护管理的最终对象。C

A 业务系统           B 功能模块           C 信息系统           D 网络系统

92. 当信息系统中包含多个业务子系统时，对每个业务子系统进行安全等级确定，最终信息系统的安全等级应当由\_\_\_\_所确定。B

A 业务子系统的安全等级平均值           B 业务子系统的最高安全等级

C 业务子系统的最低安全等级           D 以上说法都错误

93. 下列关于风险的说法，\_\_\_\_是错误的。C

A 风险是客观存在的           B 导致风险的外因是普遍存在的安全威胁

C 导致风险的外因是普遍存在的安全脆弱性           D 风险是指一种可能性

94. 下列关于风险的说法，\_\_\_\_是正确的。B

A 可以采取适当措施，完全清除风险           B 任何措施都无法完全清除风险

C 风险是对安全事件的确定描述           D 风险是固有的，无法被控制

95. 风险管理的首要任务是\_\_\_\_。A

A 风险识别和评估           B 风险转嫁           C 风险控制           D 接受风险

96. 关于资产价值的评估，\_\_\_\_说法是正确的。D

A 资产的价值指采购费用           B 资产的价值无法估计

C 资产价值的定量评估要比定性评估简单容易           D 资产的价值与其重要性密切相关

97. 采取适当的安全控制措施，可以对风险起到\_\_\_\_作用。C

A 促进           B 增加           C 减缓           D 清除

98. 当采取了安全控制措施后，剩余风险\_\_\_\_可接受风险的时候，说明风险管理是有效的。C

A 等于           B 大于           C 小于           D 不等于

99. 安全威胁是产生安全事件的\_\_\_\_。B

A 内因           B 外因           C 根本原因           D 不相关因素

100. 安全脆弱性是产生安全事件的\_\_\_\_。A

A 内因           B 外因           C 根本原因           D 不相关因素

101. 下列关于用户口令说法错误的是\_\_\_\_。C

A 口令不能设置为空 B 口令长度越长，安全性越高

C 复杂口令安全性足够高，不需要定期修改 D 口令认证是最常见的认证机制

102. 在使用复杂度不高的口令时，容易产生弱口令的安全脆弱性，被攻击者利用，从而破解用户帐户，下列\_\_\_\_具有最好的口令复杂度。B

A morrison B Wm.$\*F2m5@ C 27776394 D wangjingl977

103. 按照通常的口令使用策略，口令修改操作的周期应为\_\_\_\_天。A

A 60 B 90 C 30 D 120

104. 对口令进行安全性管理和使用，最终是为了\_\_\_\_。B

A 口令不被攻击者非法获得 B 防止攻击者非法获得访问和操作权限

C 保证用户帐户的安全性 D 规范用户操作行为

105. 人们设计了\_\_\_\_，以改善口令认证自身安全性不足的问题。D

A 统一身份管理 B 指纹认证 C 数字证书认证 D 动态口令认证机制

106. PKI是\_\_\_\_。C

A Private Key lnfrastructure B Public Key lnstitute

C Public Key lnfrastructure D Private Key lnstitute

107. 公钥密码基础设施PKI解决了信息系统中的\_\_\_\_问题。A

A 身份信任 B 权限管理 C 安全审计 D 加密

108. PKI所管理的基本元素是\_\_\_\_。C

A 密钥 B 用户身份 C 数字证书 D 数字签名

109. 最终提交给普通终端用户，并且要求其签署和遵守的安全策略是\_\_\_\_。C

A 口令策略 B 保密协议 C 可接受使用策略 D 责任追究制度

110. 下列关于信息安全策略维护的说法，\_\_\_\_是错误的。B

A 安全策略的维护应当由专门的部门完成 B 安全策略制定完成并发布之后，不需要再对其进行修改

C 应当定期对安全策略进行审查和修订 D 维护工作应当周期性进行

111. 链路加密技术是在OSI协议层次的第二层，数据链路层对数据进行加密保护，其处理的对象是\_\_。C

A 比特流 B IP数据包 C 数据帧 D 应用数据

112. 防火墙最主要被部署在\_\_\_\_位置。A

A 网络边界 B 骨干线路 C 重要服务器 D 桌面终端

113. 下列关于防火墙的错误说法是\_\_\_\_。D

A 防火墙工作在网络层 B 对IP数据包进行分析和过滤

C 重要的边界保护机制 D 部署防火墙，就解决了网络安全问题

114. IPSec协议工作在\_\_\_\_层次。B

A 数据链路层 B 网络层 C 应用层 D 传输层

115. IPSec协议中涉及到密钥管理的重要协议是\_\_\_\_。A

A IKE B AH C ESP D SSL

116. 信息安全管理中，\_\_\_负责保证安全管理策略与制度符合更高层法律、法规的要求，不发生矛盾和冲突。B

A 组织管理 B 合规性管理 C 人员管理 D 制度管理

117. 下列\_\_\_\_机制不属于应用层安全。C

A 数字签名 B 应用代理 C 主机入侵检测 D 应用审计

118. 保证用户和进程完成自己的工作而又没有从事其他操作可能，这样能够使失误出错或蓄意袭击造成的危害降低，这通常被称为\_\_\_\_。B

A 适度安全原则 B 授权最小化原则 C 分权原则 D 木桶原则

119. 入侵检测技术可以分为误用检测和\_\_\_\_两大类。C

A 病毒检测 B 详细检测 C 异常检测 D 漏洞检测

120. 安全审计是一种很常见的安全控制措施，它在信息安全保障体系中，属于\_\_\_\_措施。B

A 保护 B 检测 C 响应 D 恢复

121. \_\_\_\_不属于必需的灾前预防性措施。D

A 防火设施 B 数据备份

C 配置冗余设备 D 不间断电源，至少应给服务器等关键设备配备

122. 对于人员管理的描述错误的是\_\_\_\_。B

A 人员管理是安全管理的重要环节 B 安全授权不是人员管理的手段

C 安全教育是人员管理的有力手段 D 人员管理时，安全审查是必须的

123. 根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行\_\_\_\_。B

A 逻辑隔离 B 物理隔离 C 安装防火墙 D VLAN划分

124. 安全评估技术采用\_\_\_\_这一工具，它是一种能够自动检测远程或本地主机和网络安全性弱点的程序。A

A 安全扫描器 B 安全扫描仪 C 自动扫描器 D 自动扫描仪

125. \_\_\_最好地描述了数字证书。A

A 等同于在网络上证明个人和公司身份的身份证 B 浏览器的一标准特性，它使得黑客不能得知用户的身份 C 网站要求用户使用用户名和密码登陆的安全机制 D 伴随在线交易证明购买的收据

126. 根据BS 7799的规定，建立的信息安全管理体系ISMS的最重要特征是\_\_\_\_。B

A 全面性 B 文档化 C 先进性 D 制度化

127. 根据BS 7799的规定，对信息系统的安全管理不能只局限于对其运行期间的管理维护，而要将管理措施扩展到信息系统生命周期的其他阶段，BS7799中与此有关的一个重要方面就是\_C

A 访问控制 B 业务连续性 C 信息系统获取、开发与维护 D 组织与人员

128. 如果一个信息系统，其业务信息安全性或业务服务保证性受到破坏后，会对社会秩序和公共利益造成一定损害，但不损害国家安全；本级系统依照国家管理规范和技术标准进行自主保护，必要时，信息安全监管职能部门对其进行指导。那么该信息系统属于等级保护中的\_\_\_\_。C

A 强制保护级 B 监督保护级 C 指导保护级 D 自主保护级

129. 如果一个信息系统，其业务信息安全性或业务服务保证性受到破坏后，会对公民法人和其他组织的合法权益产生损害，但不损害国家安全、社会秩序和公共利益；本级系统依照国家管理规范和技术标准进行自主保护。那么其在等级保护中属于\_\_\_\_。D

A 强制保护级 B 监督保护级 C 指导保护级 D 自主保护级

130. 如果一个信息系统，主要对象为涉及国家安全、社会秩序和公共利益的重要信息系统，其业务信息安全性或业务服务保证性受到破坏后，会对国家安全、社会秩序和公共利益造成较大损害；本级系统依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查。这应当属于等级保护的\_\_\_\_。B

A 强制保护级 B 监督保护级 C 指导保护级 D 自主保护级

131. 如果一个信息系统，主要对象为涉及国家安全、社会秩序和公共利益的重要信息系统，其业务信息安全性或业务服务保证性受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害；本级系统依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查。这应当属于等级保护的\_\_A\_\_。

A 强制保护级 B 监督保护级 C 指导保护级 D 自主保护级

132. 如果一个信息系统，主要对象为涉及国家安全、社会秩序和公共利益的重要信息系统的核心子系统，其业务信息安全性或业务服务保证性受到破坏后，会对国家安全、社会秩序和公共利益造成特别严重损害；本级系统依照国家管理规范和技术标准进行自主保护，国家指定专门部门、专门机构进行专门监督、检查。这应当属于等级保护的\_\_\_\_。A

A 专控保护级 B 监督保护级 C 指导保护级 D 自主保护级

133. GB l7859借鉴了TCSEC标准，这个TCSEC是\_\_\_\_国家标准。C

A 英国 B 意大利 C 美国 D 俄罗斯

134. 关于口令认证机制，下列说法正确的是\_\_\_\_。B

A 实现代价最低，安全性最高 B 实现代价最低，安全性最低

C 实现代价最高，安全性最高 D 实现代价最高，安全性最低

135. 根据BS 7799的规定，访问控制机制在信息安全保障体系中属于\_\_\_\_环节。A

A 保护 B 检测 C 响应 D 恢复

136. 身份认证的含义是\_\_\_\_。C

A 注册一个用户 B 标识一个用户 C 验证一个用户 D 授权一个用户

137. 口令机制通常用于\_\_\_\_ 。A

A 认证 B 标识 C 注册 D 授权

138. 对日志数据进行审计检查，属于\_\_\_\_类控制措施。B

A 预防 B 检测 C 威慑 D 修正

139. 《信息系统安全等级保护测评准则》将测评分为安全控制测评和\_\_\_\_测评两方面。A

A 系统整体 B 人员 C 组织 D 网络

140. 根据风险管理的看法，资产\_\_\_\_价值，\_\_\_\_脆弱性，被安全威胁\_\_\_\_，\_\_\_\_风险。B

A 存在 利用 导致 具有 B 具有 存在 利用 导致

C 导致 存在 具有 利用 D 利用 导致 存在 具有

141. 根据定量风险评估的方法，下列表达式正确的是\_\_\_\_。A

A SLE=AV x EF B ALE=AV x EF C ALE=SLE x EF D ALE=SLE x AV

142. 防火墙能够\_\_\_\_。B

A 防范恶意的知情者 B 防范通过它的恶意连接

C 防备新的网络安全问题 D 完全防止传送已被病毒感染的软件和文件

143. 下列四项中不属于计算机病毒特征的是\_\_\_\_。C

A 潜伏性 B 传染性 C 免疫性 D 破坏性

144. 关于入侵检测技术，下列描述错误的是\_\_\_\_。A

A 入侵检测系统不对系统或网络造成任何影响 B 审计数据或系统日志信息是入侵检测系统的一项主要信息来源 C 入侵检测信息的统计分析有利于检测到未知的入侵和更为复杂的入侵 D 基于网络的入侵检测系统无法检查加密的数据流

145. 安全扫描可以\_\_\_\_。C

A 弥补由于认证机制薄弱带来的问题 B 弥补由于协议本身而产生的问题

C 弥补防火墙对内网安全威胁检测不足的问题 D 扫描检测所有的数据包攻击，分析所有的数据流

146. 下述关于安全扫描和安全扫描系统的描述错误的是\_\_\_\_。B

A 安全扫描在企业部署安全策略中处于非常重要地位B 安全扫描系统可用于管理和维护信息安全设备的安全

C 安全扫描系统对防火墙在某些安全功能上的不足不具有弥补性 D 安全扫描系统是把双刃剑

147. 关于安全审计目的描述错误的是\_\_\_\_。D

A 识别和分析未经授权的动作或攻击 B 记录用户活动和系统管理

C 将动作归结到为其负责的实体 D 实现对安全事件的应急响应

148. 安全审计跟踪是\_\_\_\_。A

A 安全审计系统检测并追踪安全事件的过程B 安全审计系统收集易于安全审计的数据 C 人利用日志信息进行安全事件分析和追溯的过程 D 对计算机系统中的某种行为的详尽跟踪和观察

149. 根据《计算机信息系统国际联网保密管理规定》的规定，凡向国际联网的站点提供或发布信息，必须经过\_\_\_\_。C

A 内容过滤处理 B 单位领导同意 C 备案制度 D 保密审查批准

150. 根据《计算机信息系统国际联网保密管理规定》的规定，上网信息的保密管理坚持\_\_\_\_的原则C

A 国家公安部门负责 B 国家保密部门负责 C “谁上网谁负责” D 用户自觉

151. 根据《计算机信息系统国际联网保密管理规定》的规定，保密审批实行部门管理，有关单位应当根据国家保密法规，建立健全上网信息保密审批\_\_\_\_。A

A 领导责任制 B 专人负责制 C 民主集中制 D 职能部门监管责任制

152. 网络信息未经授权不能进行改变的特性是\_\_\_\_。A

A 完整性 B 可用性 C 可靠性 D 保密性

153. 确保信息在存储、使用、传输过程中不会泄露给非授权的用户或者实体的特性是\_\_\_\_。D

A 完整性 B 可用性 C 可靠性 D 保密性

154. 确保授权用户或者实体对于信息及资源的正常使用不会被异常拒绝，允许其可靠而且及时地访问信息及资源的特性是\_\_\_\_。B

A 完整性 B 可用性 C 可靠性 D 保密性

155. \_\_\_国务院发布《计算机信息系统安全保护条例》。B

A 1990年2月18日B 1994年2月18日 C 2000年2月18日 D 2004年2月18日

156. 在目前的信息网络中，\_\_\_\_病毒是最主要的病毒类型。C

A 引导型 B 文件型 C 网络蠕虫 D 木马型

157. 在ISO／IEC 17799中，防止恶意软件的目的就是为了保护软件和信息的\_\_\_\_。B

A 安全性 B 完整性 C 稳定性 D 有效性

158. 在生成系统帐号时，系统管理员应该分配给合法用户一个\_\_\_\_，用户在第一次登录时应更改口令。A

A 唯一的口令 B 登录的位置 C 使用的说明 D 系统的规则

159. 关于防火墙和VPN的使用，下面说法不正确的是\_\_\_\_。B

A 配置VPN网关防火墙的一种方法是把它们并行放置，两者独立

B 配置VPN网关防火墙一种方法是把它们串行放置，防火墙广域网一侧，VPN在局域网一侧

C 配置VPN网关防火墙的一种方法是把它们串行放置，防火墙局域网一侧，VPN在广域网一侧

D 配置VPN网关防火墙的一种方法是把它们并行放置，两者要互相依赖

160.环境安全策略应该\_\_\_\_。D

A 详细而具体 B 复杂而专业 C 深入而清晰 D 简单而全面

161. 《计算机信息系统安全保护条例》规定，计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的\_\_\_\_的安全。C

A 计算机 B 计算机软件系统 C 计算机信息系统 D 计算机操作人员

162. 《计算机信息系统安全保护条例》规定，国家对计算机信息系统安全专用产品的销售实行\_\_\_\_。A

A 许可证制度 B 3C认证 C IS09000认证 D 专卖制度

163. 《互联网上网服务营业场所管理条例》规定，互联网上网服务营业场所经营单位\_\_\_\_。C

A 可以接纳未成年人进入营业场所 B 可以在成年人陪同下，接纳未成年人进入营业场所

C 不得接纳未成年人进入营业场所 D 可以在白天接纳未成年人进入营业场所

164. \_\_\_\_是一种架构在公用通信基础设施上的专用数据通信网络，利用IPSec等网络层安全协议和建立在PKI的加密与签名技术来获得私有性。C

A SET B DDN C VPN D PKIX

165. 《计算机信息系统安全保护条例》规定，运输、携带、邮寄计算机信息媒体进出境的，应当如实向\_\_。B

A 国家安全机关申报 B 海关申报 C 国家质量检验监督局申报 D 公安机关申报

166. 《计算机信息系统安全保护条例》规定，故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以\_\_\_\_的罚款、对单位处以\_\_\_\_的罚款。A

A 5000元以下 15000元以下 B 5000元 15000元

C 2000元以下 10000元以下 D 2000元 10000元

167. 计算机犯罪，是指行为人通过\_\_\_\_所实施的危害\_\_\_\_安全以及其他严重危害社会的并应当处以刑罚的行为。A

A 计算机操作 计算机信息系统 B 数据库操作 计算机信息系统

C 计算机操作 应用信息系统 D 数据库操作 管理信息系统

168. 策略应该清晰，无须借助过多的特殊一通用需求文档描述，并且还要有具体的\_\_\_\_。C

A 管理支持 C 实施计划 D 补充内容 B 技术细节

169．系统备份与普通数据备份的不同在于，它不仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速\_\_\_\_。A

A 恢复整个系统B 恢复所有数据 C 恢复全部程序 D 恢复网络设置

170．在一个企业网中，防火墙应该是\_\_\_\_的一部分，构建防火墙时首先要考虑其保护的范围。D

A 安全技术 B 安全设置 C 局部安全策略 D 全局安全策略

171． 信息安全策略的制定和维护中，最重要是要保证其\_\_\_\_和相对稳定性。A

A 明确性 B 细致性 C 标准性 D 开放性

172． \_\_\_\_是企业信息安全的核心。C

A 安全教育 B 安全措施 C 安全管理 D 安全设施

173．编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码是\_\_\_\_。A

A 计算机病毒 B 计算机系统 C 计算机游戏 D 计算机程序

174．许多与PKI相关的协议标准(如PKIX、S／MIME、SSL、TLS、IPSec)等都是在\_\_\_\_基础上发展起来的。B

A X.500 B X.509 C X.519 D X.505

175． \_\_\_\_是PKI体系中最基本的元素，PKI系统所有的安全操作都是通过该机制采实现的。D

A SSL B IARA C RA D 数字证书

176． 基于密码技术的访问控制是防止\_\_\_\_的主要防护手段。A

A 数据传输泄密 B 数据传输丢失 C 数据交换失败 D 数据备份失败

177． 避免对系统非法访问的主要方法是\_\_\_\_。C

A 加强管理 B 身份认证 C 访问控制 D 访问分配权限

178． 对保护数据来说，功能完善、使用灵活的\_\_\_\_必不可少。B

A 系统软件 B 备份软件 C 数据库软件 D 网络软件 179．信息安全PDR模型中，如果满足\_\_\_\_，说明系统是安全的。A

A Pt>Dt+Rt B Dt>Pt+Rt C Dt< font> D Pt< font>

180． 在一个信息安全保障体系中，最重要的核心组成部分为\_\_\_\_。B

A 技术体系 B 安全策略 C 管理体系 D 教育与培训

181．国家信息化领导小组在《关于加强信息安全保障工作的意见》中，针对下一时期的信息安全保障工作提出了\_\_\_\_项要求。C

A 7 B 6 C 9 D 10

182． 《确保网络空间安全的国家战略》是\_\_\_\_发布的国家战略。D

A 英国 B 法国 C 德国 D 美国

183．《计算机信息系统安全保护条例》规定，\_\_\_\_主管全国计算机信息系统安全保护工作。A

A 公安部 B 国务院信息办 C 信息产业部 D 国务院

184． 下列\_\_\_\_不属于物理安全控制措施。C

A 门锁 B 警卫 C 口令 D 围墙

185． 灾难恢复计划或者业务连续性计划关注的是信息资产的\_\_\_\_属性。A

A 可用性 B 真实性 C 完整性 D 保密性

186． VPN是\_\_\_\_的简称。B

A Visual Private Network B Virtual Private NetWork

C Virtual Public Network D Visual Public Network

187． 部署VPN产品，不能实现对\_\_\_\_属性的需求。C

A 完整性 B 真实性 C 可用性 D 保密性

188． \_\_\_\_是最常用的公钥密码算法。A

A RSA B DSA C 椭圆曲线 D 量子密码

189． PKI的主要理论基础是\_\_\_\_。B

A 对称密码算法 B 公钥密码算法 C 量子密码 D 摘要算法

190． PKI中进行数字证书管理的核心组成模块是\_\_\_\_ 。B

A 注册中心RA B 证书中心CA C 目录服务器 D 证书作废列表

191． 信息安全中的木桶原理，是指\_\_\_\_。A

A 整体安全水平由安全级别最低的部分所决定

B 整体安全水平由安全级别最高的部分所决定

C 整体安全水平由各组成部分的安全级别平均值所决定 D 以上都不对

192． 关于信息安全的说法错误的是\_\_\_\_。C

A 包括技术和管理两个主要方面 B 策略是信息安全的基础

C 采取充分措施，可以实现绝对安全 D 保密性、完整性和可用性是信息安全的目标

193． PDR模型是第一个从时间关系描述一个信息系统是否安全的模型，PDR模型中的P代表\_\_\_\_、D代表\_\_\_\_、R代表\_\_\_\_。A

A 保护 检测响应 B 策略 检测响应 C 策略 检测 恢复 D 保护 检测 恢复 194．《计算机信息系统安全保护条例》规定，任何组织或者个人违反条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担\_\_\_\_。B

A 刑事责任 B 民事责任 C 违约责任 D 其他责任

195． 在信息安全管理中进行\_\_\_\_，可以有效解决人员安全意识薄弱问题。B

A 内容监控B 责任追查和惩处 C 安全教育和培训 D 访问控制

196． 关于信息安全，下列说法中正确的是\_\_\_\_。C

A 信息安全等同于网络安全 B 信息安全由技术措施实现

C 信息安全应当技术与管理并重 D 管理措施在信息安全中不重要

197． 在PPDRR安全模型中，\_\_\_\_是属于安全事件发生后的补救措施。B

A 保护 B 恢复 C 响应 D 检测

198． 根据权限管理的原则，—个计算机操作员不应当具备访问\_\_\_\_的权限。C

A 操作指南文档 B 计算机控制台 C 应用程序源代码 D 安全指南

199． 要实现有效的计算机和网络病毒防治，\_\_\_\_应承担责任。D

A 高级管理层 B 部门经理 C 系统管理员 D 所有计算机用户

200． 统计数据表明，网络和信息系统最大的人为安全威胁来自于\_\_\_\_。B

A 恶意竞争对手 B 内部人员 C 互联网黑客 D 第三方人员

201. 双机热备是一种典型的事先预防和保护措施，用于保证关键设备和服务的\_\_\_\_属性。B

A 保密性 B 可用性 C 完整性 D 真实性

202. 在安全评估过程中，采取\_\_\_\_手段，可以模拟黑客入侵过程，检测系统安全脆弱。C

A 问卷调查 B 人员访谈 C 渗透性测试 D 手工检查

203. 我国正式公布了电子签名法，数字签名机制用于实现\_\_\_\_需求。A

A 抗否认 B 保密性 C 完整性 D 可用性

204. 在需要保护的信息资产中，\_\_\_\_是最重要的。C

A 环境 B 硬件 C 数据 D 软件

205. \_\_\_手段，可以有效应对较大范围的安全事件的不良影响，保证关键服务和数据的可用性。B

A 定期备份 B 异地备份 C 人工备份 D 本地备份

206. \_\_\_\_能够有效降低磁盘机械损坏给关键数据造成的损失。C

A 热插拔 B SCSI C RAID D FAST-ATA

207. 相对于现有杀毒软件在终端系统中提供保护不同，\_\_在内外网络边界处提供更加主动和积极的病毒保护。B

A 防火墙 B 病毒网关 C IPS D IDS

208. 信息安全评测标准CC是\_\_\_\_标准。B

A 美国 B 国际 C 英国 D 澳大利亚

209. 《信息系统安全等级保护基本要求》中，对不同级别的信息系统应具备的基本安全保护能力进行了要求，共划分为\_\_\_\_级。A

A 4 B 5 C 6 D 7

三．多项选择题

210. 在互联网上的计算机病毒呈现出的特点是\_\_\_\_。ABCD

A 与因特网更加紧密地结合，利用一切可以利用的方式进行传播 B 所有的病毒都具有混合型特征，破坏性大大增强 C 因为其扩散极快，不再追求隐蔽性，而更加注重欺骗性 D 利用系统漏洞传播病毒 E 利用软件复制传播病毒

211. 全国人民代表大会常务委员会《关于维护互联网安全的决定》规定，利用互联网实施违法行为，尚不构成犯罪的，对直接负责的主管人员和其他直接责任人员，依法给予\_\_\_\_或者\_\_\_\_。AB

A 行政处分 B 纪律处分 C 民事处分 D 刑事处分

212. 《计算机信息网络国际联网安全保护管理办法》规定，任何单位和个人不得从事下列危害计算机信息网络安全的活动\_\_\_\_。ABCD

A 故意制作、传播计算机病毒等破坏性程序的 B 未经允许，对计算机信息网络功能进行删除、修改或者增加的 C 未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的 D 未经允许，进入计算机信息网络或者使用计算机信息网络资源的

213. 用于实时的入侵检测信息分析的技术手段有\_\_\_\_。AD

A 模式匹配 B 完整性分析 C 可靠性分析 D 统计分析 E 可用性分析

214. 《互联网上网服务营业场所管理条例》规定，\_\_\_\_负责互联网上网服务营业场所经营许可审批和服务质量监督。ABC

A 省电信管理机构 B 自治区电信管理机构

C 直辖市电信管理机构 D 自治县电信管理机构 E 省信息安全管理机构

215. 《互联网信息服务管理办法》规定，互联网信息服务提供者不得制作、复制、发布、传播的信息内容有。ADE

A 损害国家荣誉和利益的信息 B 个人通信地址 C 个人文学作品

D 散布淫秽、色情信息 E 侮辱或者诽谤他人，侵害他人合法权益的信息

216. 《计算机信息系统安全保护条例》规定，\_\_\_\_由公安机关处以警告或者停机整顿。ABCDE

A 违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的 B 违反计算机信息系统国际联网备案制度的 C 有危害计算机信息系统安全的其他行为的

D 不按照规定时间报告计算机信息系统中发生的案件的 E 接到公安机关要求改进安全状况的通知后，在限期内拒不改进的

217. 与计算机有关的违法案件，要\_\_\_\_，以界定是属于行政违法案件，还是刑事违法案件。ABD

A 根据违法行为的情节和所造成的后果进行界定B 根据违法行为的类别进行界定

C 根据违法行为人的身份进行界定 D 根据违法行为所违反的法律规范来界定

218. 对于违法行为的行政处罚具有的特点是\_\_\_\_。ABCD

A 行政处罚的实施主体是公安机关 B 行政处罚的对象是行政违法的公民、法人或其他组织

C 必须有确定的行政违法行为才能进行行政处罚 D 行政处罚具有行政强制性

219.\_\_\_是行政处罚的主要类别。ABCDE

A 人身自由罚 B 声誉罚 C 财产罚 D 资格罚 E 责令作为与不作为罚

220. 互联网服务提供者和联网使用单位应当落实的互联网安全保护技术措施包括\_\_\_\_ ABCD

A 防范计算机病毒、网络入侵和攻击破坏等危害网络安全事项或者行为的技术措施

B 重要数据库和系统主要设备的冗灾备份措施

C 记录并留存用户登录和退出时间、主叫号码、帐号、互联网地址或域名、系统维护日志的技术措施

D 法律、法规和规章规定应当落实的其他安全保护技术措施

221. 在刑法中，\_\_\_\_规定了与信息安全有关的违法行为和处罚依据。ABD

A 第285条 B 第286条 C 第280条 D 第287条

222. \_\_\_可能给网络和信息系统带来风险，导致安全事件。ABCDE

A 计算机病毒B 网络入侵C 软硬件故障 D 人员误操作 E 不可抗灾难事件

223. \_\_\_安全措施可以有效降低软硬件故障给网络和信息系统所造成的风险。ABCD

A 双机热备 B 多机集群 C 磁盘阵列 D 系统和数据备份 E 安全审计

224. 典型的数据备份策略包括\_\_\_\_。ABD

A 完全备份 B 增量备份 C 选择性备份 D 差异备份 E 手工备份

225. 我国信息安全等级保护的内容包括\_\_\_\_。ABD

A 对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输和处理这些信息的信息系统分等级实行安全保护 B 对信息系统中使用的信息安全产品实行按等级管理 C 对信息安全从业人员实行按等级管理 D 对信息系统中发生的信息安全事件按照等级进行响应和处置 E 对信息安全违反行为实行按等级惩处

226. 目前，我国在对信息系统进行安全等级保护时，划分了5个级别，包括\_\_\_\_。ABCDE

A 专控保护级 B 强制保护级 C 监督保护级 D 指导保护级 E 自主保护级

227. 下列\_\_\_\_因素，会对最终的风险评估结果产生影响。BCDE

A 管理制度 B 资产价值 C 威胁 D 脆弱性 E 安全措施

228. 下列\_\_\_\_因素与资产价值评估有关。ACD

A 购买资产发生的费用 B 软硬件费用 C 运行维护资产所需成本 D 资产被破坏所造成的损失 E 人工费用

229. 安全控制措施可以分为\_\_\_\_。ABD

A 管理类 B 技术类 C 人员类 D 操作类 E 检测类

230安全脆弱性，是指安全性漏洞，广泛存在于\_\_\_\_。ABC

A 协议设计过程 B 系统实现过程C 运行维护过程 D 安全评估过程 E 审计检查过程

231. 信息安全技术根据信息系统自身的层次化特点，也被划分了不同的层次，这些层次包括\_\_\_\_。ACDE

A 物理层安全 B 人员安全C 网络层安全 D 系统层安全 E 应用层安全

232. 物理层安全的主要内容包括\_\_\_\_。ABD

A 环境安全 B 设备安全 C 线路安全 D 介质安全 E 人员安全

233. 根据BS 7799的规定，信息安全管理体系ISMS的建立和维护，也要按照PDCA的管理模型周期性进行，主要包含\_\_\_\_环节。BCDE

A 策略Policy B 建立Plan C 实施Do D 检查Check E 维护改进Act

234. 在BS 7799中，访问控制涉及到信息系统的各个层面，其中主要包括\_\_\_\_。ABDE

A 物理访问控制 B 网络访问控制 C 人员访问控制 D 系统访问控制 E 应用访问控制

235. 英国国家标准BS 7799，经国际标准化组织采纳为国家标准\_\_\_\_。AD

A ISO 17799 B ISO 15408 C ISO 13335 D ISO 27001 E ISO 24088

236. 计算机信息系统安全的三个相辅相成、互补互通的有机组成部分是\_\_\_\_。ABD

A 安全策略 B 安全法规 C 安全技术 D 安全管理

237. 为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有\_\_\_\_。ABCDE

A 口令／帐号加密B 定期更换口令C 限制对口令文件的访问 D 设置复杂的、具有一定位数的口令

238. 关于入侵检测和入侵检测系统，下述正确的选项是\_\_\_\_。ABCE

A 入侵检测收集信息应在网络的不同关键点进行 B 入侵检测的信息分析具有实时性

C 基于网络的入侵检测系统的精确性不及基于主机的入侵检测系统的精确性高

D 分布式入侵检测系统既能检测网络的入侵行为，又能检测主机的入侵行为

E 入侵检测系统的主要功能是对发生的入侵事件进行应急响应处理

239. 目前广泛使用的主要安全技术包括\_\_\_\_。ABCDE

A 防火墙 B 入侵检测 C PKI D VPN E 病毒查杀

240. 《计算机信息网络国际联网安全保护管理办法》规定，任何单位和个人不得制作、复制、发布、传播的信息内容有\_\_\_\_。ADE

A 损害国家荣誉和利益的信息 B 个人通信地址 C 个人文学作品

D 淫秽、色情信息 E 侮辱或者诽谤他人，侵害他人合法权益的信息

241. 基于角色对用户组进行访问控制的方式有以下作用：\_\_\_\_。CDE

A 使用户分类化 B 用户的可管理性得到加强 C 简化了权限管理，避免直接在用户和数据之间进行授权和取消 D 有利于合理划分职责 E 防止权力滥用

242. 在网络中身份认证时可以采用的鉴别方法有\_\_\_\_。ABD

A 采用用户本身特征进行鉴别 B 采用用户所知道的事进行鉴别 C 采用第三方介绍方法进行鉴别

D 使用用户拥有的物品进行鉴别 E 使用第三方拥有的物品进行鉴别

243. 在ISO／IECl7799标准中，信息安全特指保护\_\_\_\_。ABD

A 信息的保密性 B 信息的完整性 C 信息的流动性 D 信息的可用性

244. PKI是生成、管理、存储、分发和吊销基于公钥密码学的公钥证书所需要的\_\_\_\_的总和。ABCDE

A 硬件 B 软件 C 人员 D 策略 E 规程

245. SSL主要提供三方面的服务，即\_\_\_\_。BDE

A 数字签名 B 认证用户和服务器 C 网络传输

D 加密数据以隐藏被传送的数据 E 维护数据的完整性

246. 经典密码学主要包括两个既对立又统一的分支，即\_\_\_\_。AC

A 密码编码学 B 密钥密码学 C 密码分析学 D 序列密码 E 古典密码

247. 全国人民代表大会常务委员会《关于维护互联网安全的决定》规定，为了维护社会主义市场经济秩序和社会管理秩序，\_\_\_\_行为，构成犯罪的，依照刑法有关规定追究刑事责任。ABCDE

A 利用互联网销售伪劣产品或者对商品、服务作虚假宣传 B 利用互联网侵犯他人知识产权

C 利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息

D 利用互联网损害他人商业信誉和商品声誉

E 在互联网上建立淫秽网站、网页，提供淫秽站点链接服务，或者传播淫秽书刊、影片、音像、图片

248. 有多种情况能够泄漏口令，这些途径包括\_\_\_\_。ACDE

A 猜测和发现口令 B 口令设置过于复杂 C 将口令告诉别人

D 电子监控 E 访问口令文件

249. 信息系统常见的危险有\_\_\_\_。ABCD

A 软硬件设计故障导致网络瘫痪 B 黑客入侵 C 敏感信息泄露 D 信息删除 E 电子邮件发送

250. 对于计算机系统，由环境因素所产生的安全隐患包括\_\_\_\_。ABCDE

A 恶劣的温度、湿度、灰尘、地震、风灾、火灾等 B 强电、磁场等 C 雷电 D 人为的破坏

251. 在局域网中计算机病毒的防范策略有\_\_\_\_。ADE

A 仅保护工作站 B 保护通信系统 C 保护打印机 D 仅保护服务器 E 完全保护工作站和服务器

252. 一个安全的网络系统具有的特点是\_\_\_\_。ABCE

A 保持各种数据的机密 B 保持所有信息、数据及系统中各种程序的完整性和准确性

C 保证合法访问者的访问和接受正常的服务 D 保证网络在任何时刻都有很高的传输速度

E 保证各方面的工作符合法律、规则、许可证、合同等标准

253. 任何信息安全系统中都存在脆弱点，它可以存在于\_\_\_\_。ABCDE

A 使用过程中 B 网络中 C 管理过程中 D 计算机系统中 E 计算机操作系统中

254. \_\_\_\_是建立有效的计算机病毒防御体系所需要的技术措施。ABCDE

A 杀毒软件 B 补丁管理系统 C 防火墙 D 网络入侵检测 E 漏洞扫描

255. 信息系统安全保护法律规范的作用主要有\_\_\_\_。ABCDE

A 教育作用 B 指引作用 C 评价作用 D 预测作用 E 强制作用

256. 根据采用的技术，入侵检测系统有以下分类：\_\_\_\_。BC

A 正常检测 B 异常检测 C 特征检测 D 固定检测 E 重点检测

257. 在安全评估过程中，安全威胁的来源包括\_\_\_\_。ABCDE

A 外部黑客 B 内部人员 C 信息技术本身 D 物理环境 E 自然界

258. 安全评估过程中，经常采用的评估方法包括\_\_\_\_。ABCDE

A 调查问卷 B 人员访谈 C 工具检测 D 手工审核 E 渗透性测试

259. 根据IS0定义，信息安全的保护对象是信息资产，典型的信息资产包括\_\_\_\_。ABD

A 硬件 B 软件 C 人员 D 数据 E 环境

260. 根据IS0定义，信息安全的目标就是保证信息资产的三个基本安全属性，包括\_\_\_\_。BCD

A 不可否认性 B 保密性 C 完整性 D 可用性 E 可靠性

261. 治安管理处罚法规定，\_\_\_\_行为，处5日以下拘留；情节较重的，处5日以上10日以下拘留。ABCDE

A 违反国家规定，侵入计算机信息系统，造成危害的

B 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行

C 违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的

D 故意制作、传播计算机病毒等破坏性程序，影口向计算机信息系统正常运行的

262. 网络蠕虫病毒越来越多地借助网络作为传播途径，包括\_\_\_\_。ABCDE

A 互联网浏览 B 文件下载 C 电子邮件 D 实时聊天工具 E 局域网文件共享

263. 在信息安全管理中进行安全教育与培训，应当区分培训对象的层次和培训内容，主要包括\_\_\_\_。ABCDE

264. A 高级管理层 B 关键技术岗位人员 C 第三方人员 D 外部人员 E 普通计算机用户

265. 网络入侵检测系统，既可以对外部黑客的攻击行为进行检测，也可以发现内部攻击者的操作行为，通常部署在\_\_\_\_。BC

A 关键服务器主机B 网络交换机的监听端口 C 内网和外网的边界 D 桌面系统 E 以上都正确

266．IPSec是网络层典型的安全协议，能够为IP数据包提供\_\_\_\_安全服务。ABE

A 保密性 B 完整性 C 不可否认性 D 可审计性 E 真实性

267. 信息安全策略必须具备\_\_\_\_属性。ACE

A 确定性 B 正确性 C 全面性 D 细致性 E 有效性

268. 涉密安全管理包括\_\_\_\_。BCDE

A 涉密设备管理 B 涉密信息管理 C 涉密人员管理 D 涉密场所管理

信息安全试题（1/共3）

一、 单项选择题（每小题2分，共20分）

1．信息安全的基本属性是＿＿＿。

A. 保密性 B.完整性

C. 可用性、可控性、可靠性 D. A，B，C都是

2．假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于＿＿＿。

A. 对称加密技术 B. 分组密码技术

C. 公钥加密技术 D. 单向函数密码技术

3．密码学的目的是＿＿＿。

A. 研究数据加密 B. 研究数据解密

C. 研究数据保密 D. 研究信息安全

4．A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送数字签名M，对信息M加密为：M’= KB公开（KA秘密（M））。B方收到密文的解密方案是＿＿＿。

A. KB公开（KA秘密（M’）） B. KA公开（KA公开（M’））

C. KA公开（KB秘密（M’）） D. KB秘密（KA秘密（M’））

5．数字签名要预先使用单向Hash函数进行处理的原因是＿＿＿。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

6．身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是＿＿。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

7．防火墙用于将Internet和内部网络隔离＿＿＿。

A. 是防止Internet火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

8．PKI支持的服务不包括＿＿＿。

A. 非对称密钥技术及证书管理 B. 目录服务

C. 对称密钥的产生和分发 D. 访问控制服务

9．设哈希函数H有128个可能的输出(即输出长度为128位)，如果H的k个随机输入中至少有两个产生相同输出的概率大于0.5，则k约等于＿＿。

A．2128 B．264

C．232 D．2256

10．Bell-LaPadula模型的出发点是维护系统的＿＿＿，而Biba模型与Bell-LaPadula模型完全对立，它修正了Bell-LaPadula模型所忽略的信息的＿＿＿问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A．保密性 可用性 B．可用性 保密性

C．保密性 完整性 D．完整性 保密性

二、 填空题（每空1分，共20分）

1．ISO 7498-2确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。同时，ISO 7498-2也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。

2．古典密码包括 代替密码和置换密码两种，对称密码体制和非对称密码体制都属于现代密码体制。传统的密码系统主要存在两个缺点：一是 密钥管理与分配问题 ；二是 认证问题 。在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3．根据使用密码体制的不同可将数字签名分为 基于对称密码体制的数字签名 和 基于公钥密码体制的数字签名 ，根据其实现目的的不同，一般又可将其分为 直接数字签名 和 可仲裁数字签名 。

4. DES算法密钥是64位，其中密钥有效位是56位。RSA算法的安全是基于分解两个大素数的积的困难。

5．密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式有两种：一种是由中心集中生成，另一种是由个人分散生成。

6．认证技术包括站点认证、报文认证和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、生理特征识别、零知识证明。

7．NAT的实现方式有三种，分别是静态转换、动态转换、端口多路复用。

8．数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、 计算题（每小题8分，共24分）

1．用置换矩阵Ek=〔 〕对明文Now we are having a test加密，并给出其解密矩阵及求出可能的解密矩阵总数。

解：设明文长度L=5，最后一段不足5则加字母x，经过置换后，得到的密文为 Wnewo haaer gvani ttxse

其解密矩阵为

Dk=〔 〕

L=5时可能的解密矩阵总数为 5！= 120

2．DES的密码组件之一是S盒。根据S盒表计算S3(101101)的值,并说明S函数在DES算法中的作用。

解：令101101的第1位和最后1位表示的二进制数为i，则i=(11)2=(3)10

令101101的中间4位表示的二进制数为j，则j=(0110)2=(6)10

查S3盒的第3行第6列的交叉处即为8，从而输出为1000

S函数的作用是将6位的输入变为4位的输出

3．求963和657的最大公约数(963, 657)，并表示成963，657的线性组合。

解：运用广义欧几里得除法，有

963=1\*657+306

657=2\*306+45

306=6\*45+36

45=1\*36+9

36=4\*9+0

（根据给出的最后一个定理）则(963, 657)=9

从广义欧几里得除法逐次消去r(n-1),r(n-2), …,r(3),r(2)，即

9=45-1\*36

=45-（306-6\*45）

=7\*45-306

=7\*（657-2\*306）-306

=7\*657-3\*306

=7\*657-3\*（963-657）

=22\*657-15\*963

所以此线性组合为 9=22\*657-15\*963

四、 问答题（每小题7分，共21分）

1．S拥有所有用户的公开密钥,用户A使用协议

A → S：A || B || Ra

S → A: S || Ss(S || A || Ra || Kb)

其中Ss( )表示S利用私有密钥签名

向S申请B的公开密钥Kb。上述协议存在问题吗？若存在，请说明此问题；若不存在，请给出理由。

答：存在。

由于S没有把公钥和公钥持有人捆绑在一起，A就无法确定它所收到的公钥是不是B的，即B的公钥有可能被伪造。如果攻击者截获A发给S的信息，并将协议改成

A → S：A || C || Ra

S收到消息后，则又会按协议

S → A: S || Ss(S || A || Ra || Kc)

将Kc发送给A，A收到信息后会认为他收到的是Kb ，而实际上收到的是Kc ，但是A会把它当作Kb ，因为他无法确认。

2．请你利用认证技术设计两套系统，一套用于实现商品的真伪查询，另一套用于防止电脑彩票伪造问题。

答：(1)系统产生一随机数并存储此数，然后对其加密，再将密文贴在商品上。当客户购买到此件商品并拨打电话查询时，系统将客户输入的编码(即密文)解密，并将所得的明文与存储在系统中的明文比较，若匹配则提示客户商品是真货，并从系统中删了此明文；若不匹配则提示客户商品是假货。

(2)首先，系统给彩票编好码，习惯称之为条形码；然后，将条形码通过MD5运算，得到相应的消息摘要；接着，对消息摘要进行加密，得到相应密文；最后，系统将条形码与密文绑定在一起并存储，若需要查询时只要查看条形码与密文是否相关联即可。这样，即可实现电脑彩票防伪，因为伪造者是无法伪造密文的。

3．防火墙的实现技术有哪两类？防火墙存在的局限性又有哪些？

答：防火墙的实现从层次上可以分为两类：数据包过滤和应用层网关，前者工作在网络层，而后者工作在应用层。

防火墙存在的局限性主要有以下七个方面

(1) 网络上有些攻击可以绕过防火墙（如拨号）。

(2) 防火墙不能防范来自内部网络的攻击。

(3) 防火墙不能对被病毒感染的程序和文件的传输提供保护。

(4) 防火墙不能防范全新的网络威胁。

(5) 当使用端到端的加密时，防火墙的作用会受到很大的限制。

(6) 防火墙对用户不完全透明，可能带来传输延迟、瓶颈以及单点失效等问题。

(7) 防火墙不能防止数据驱动式攻击。有些表面无害的数据通过电子邮件或其他方式发送到主机上，一旦被执行就形成攻击（附件）。

五、 分析题（15分）

1．下图表示的是P2DR2动态安全模型，请从信息安全安全角度分析此模型？

答：(主要理解一下黑体字部分，然后按照这个思路自由发挥)

P2DR2动态安全模型研究的是基于企业网对象、依时间及策略特征的（Policy， Protection， Detection，Response，Restore）动态安全模型结构，由策略、防护、检测、响应和恢复等要素构成，是一种基于闭环控制、主动防御的动态安全模型。通过区域网络的路由及安全策略分析与制定，在网络内部及边界建立实时检测、监测和审计机制，采取实时、快速动态响应安全手段，应用多样性系统灾难备份恢复、关键系统冗余设计等方法，构造多层次、全方位和立体的区域网络安全环境。

一个良好的网络安全模型应在充分了解网络系统安全需求的基础上，通过安全模型表达安全体系架构，通常具备以下性质：精确、无歧义；简单和抽象；具有一般性；充分体现安全策略。

1． P2DR2模型的时间域分析

P2DR2模型可通过数学模型，作进一步理论分析。作为一个防御保护体系，当网络遭遇入侵攻击时，系统每一步的安全分析与举措均需花费时间。设Pt为设置各种保护后的防护时间，Dt为从入侵开始到系统能够检测到入侵所花费的时间，Rt为发现入侵后将系统调整到正常状态的响应时间，则可得到如下安全要求：

Pt >( Dt + Rt) （1）

由此针对于需要保护的安全目标，如果满足公式（1），即防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前，这种入侵行为就能够被检测到并及时处理。同样，我们假设Et为系统暴露给入侵者的时间，则有

Et=Dt+Rt （如果Pt=0） （2）

公式（2）成立的前提是假设防护时间为0，这种假设对Web Server这样的系统可以成立。

通过上面两个公式的分析，实际上给出了一个全新的安全定义：及时的检测和响应就是安全，及时的检测和恢复就是安全。不仅于此，这样的定义为解决安全问题给出了明确的提示：提高系统的防护时间Pt、降低检测时间Dt和响应时间Rt，是加强网络安全的有效途径。

图1为P2DR2 安全模型的体系结构。在P2DR2动态安全模型中，采用的加密、访问控制等安全技术都是静态防御技术，这些技术本身也易受攻击或存在问题。那么攻击者可能绕过了静态安全防御技术，进入系统，实施攻击。模型认可风险的存在，绝对安全与绝对可靠的网络系统是不现实的，理想效果是期待网络攻击者穿越防御层的机会逐层递减，穿越第5层的概率趋于零。

图2 P2DR2 安全模型体系结构

2． P2DR2模型的策略域分析

网络系统是由参与信息交互的各类实体元素构成，可以是独立计算机、局域网络或大规模分布式网络系统。实体集合可包括网络通信实体集、通信业务类型集和通信交互时间集。

通信实体集的内涵表示发起网络通信的主体，如：进程、任务文件等资源；对于网络系统，表示各类通信设备、服务器以及参与通信的用户。网络的信息交互的业务类型存在多样性，根据数据服务类型、业务类型，可以划分为数据信息、图片业务、声音业务；根据IP数据在安全网关的数据转换服务，业务类型可以划分为普通的分组；根据TCP/IP协议传输协议，业务类型可以划分为 ICMP、TCP、UDP分组。信息安全系统根据不同安全服务需求，使用不同分类法则。通信交互时间集则包含了通信事件发生的时间区域集。

安全策略是信息安全系统的核心。大规模信息系统安全必须依赖统一的安全策略管理、动态维护和管理各类安全服务。安全策略根据各类实体的安全需求，划分信任域，制定各类安全服务的策略。

在信任域内的实体元素，存在两种安全策略属性，即信任域内的实体元素所共同具有的有限安全策略属性集合,实体自身具有的、不违反Sa的特殊安全策略属性Spi 。由此我们不难看出，S=Sa+ΣSpi.

安全策略不仅制定了实体元素的安全等级，而且规定了各类安全服务互动的机制。每个信任域或实体元素根据安全策略分别实现身份验证、访问控制、安全通信、安全分析、安全恢复和响应的机制选择。

信息安全试题（2/共3）

一．名词解释

信息安全：建立在网络基础上的现代信息系统，其安全定义较为明确，那就是：保护信息系统的硬件软件及其相关数据，使之不因偶然或是恶意侵犯而遭受破坏，更改及泄露，保证信息系统能够连续正常可靠的运行。

VPN：一般是指建筑在因特网上能够自我管理的专用网络，是一条穿过混乱的公共网络的安全稳定的隧道。通过对网络数据的封包和加密传输，在一个公用网络建立一个临时的，安全的连接，从而实现早公共网络上传输私有数据达到私有网络的级别。

数字证书：是指各实体（持卡人、个人、商户、企业、网关、银行等）在网上信息交流及交易活动中的身份证明。

选择题

1.、加密算法分为（对称密码体制和非对称密码体制）

2。、口令破解的最好方法是（B）

A暴力破解 B组合破解 C字典攻击 D生日攻击

3、杂凑码最好的攻击方式是（D）

A 穷举攻击 B中途相遇 C字典攻击 D生日攻击

4、可以被数据完整性机制防止的攻击方式是（D）

A假冒\*\*\* B抵赖\*\*\*\* C数据中途窃取 D数据中途篡改

5、会话侦听与劫持技术属于（B）技术

A密码分析还原 B协议漏洞渗透 C应用漏洞分析与渗透 D DOS攻击

6、PKI的主要组成不包括（B）

A CA B SSL C RA D CR

7，恶意代码是（指没有作用却会带来危险的代码D）

A 病毒\*\*\* B 广告\*\*\* C间谍\*\* D 都是

8，社会工程学常被黑客用于（踩点阶段信息收集A）

A 口令获取 B ARP C TCP D DDOS

9，windows中强制终止进程的命令是（C）

A Tasklist B Netsat C Taskkill D Netshare

10，现代病毒木马融合了（D）新技术

A 进程注入 B注册表隐藏 C漏洞扫描 D都是

11，网络蜜罐技术使用于（.迷惑入侵者，保护服务器诱捕网络罪犯

）

12，利用三次握手攻击的攻击方式是（DOS\DDOS\DRDOS）

13，溢出攻击的核心是（A）

A 修改堆栈记录中进程的返回地址 B利用Shellcode C 提升用户进程权限 D 捕捉程序漏洞

14，在被屏蔽的主机体系中，堡垒主机位于（A）中，所有的外部连接都经过滤路由器到它上面去。

A 内部网络 B周边网络 C外部网络 D自由连接

15，外部数据包经过过滤路由只能阻止（D）唯一的ip欺骗

A 内部主机伪装成外部主机IP B内部主机伪装成内部主机IP

C外部主机伪装成外部主机IP D外部主机伪装成内部主机IP

17，ICMP数据包的过滤主要基于（D）

A目标端口 B 源端口 C消息源代码 D协议prot

18，网络安全的特征包含保密性，完整性（D）四个方面

A可用性和可靠性 B 可用性和合法性 C可用性和有效性 D可用性和可控性

三，简答题

1，信息安全有哪些常见的威胁？信息安全的实现有哪些主要技术措施？

答：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。信息安全的实现可以通过物理安全技术，系统安全技术，网络安全技术，应用安全技术，数据加密技术，认证授权技术，访问控制技术，审计跟踪技术，防病毒技术，灾难恢复和备份技术

2，什么是密码分析，其攻击类型有哪些？DES算法中S盒的作用是什么？

答：密码分析是指研究在不知道密钥的情况下来恢复明文的科学。攻击类型有只有密文的攻击，已知明文的攻击，选择明文的攻击，适应性选择明文攻击，选择密文的攻击，选择密钥的攻击，橡皮管密码攻击。S盒是DES算法的核心。其功能是把6bit数据变为4bit数据。

3，试画图说明kerberos认证原理

4，用户A需要通过计算机网络安全地将一份机密文件传送给用户B，请问如何实现？

如果这份机密文件数据量非常大，B希望A今后对该份机密文件无法抵赖，请问如何实

现，试画图说明。

答：（1）假定通信双方分别为Alice和Bob

加密方Alice将商定的密钥秘密地传递给解密方Bob 。

Alice 用商定的密钥加密她的消息，然后传送给Bob。

Bob用Alice传来的密钥解密Alice的消息。

(2)假定通信双方分别为Alice和Bob

Alice和Bob选用一个公开密钥密码系统

Bob将他的公开密钥传送给Alice

(2)假定通信双方分别为Alice和Bob

Alice和Bob选用一个公开密钥密码系统

Bob将他的公开密钥传送给Alice

Alice用Bob的公开密钥加密她的消息，然后传送给Bob

Bob用他的私人密钥解密Alice的消息。

5，防火墙有哪些体系结构？其中堡垒主机的作用是什么？

检测计算机病毒的方法主要有哪些？

答：防火墙的体系结构有屏蔽路由器（Screening Router）和屏蔽主机（Screening Host），双宿主网关（Dual Homed Gateway），堡垒主机（Bastion Host），屏蔽子网（Screened Subnet）防火墙

检测计算机病毒的方法主要有外观检测，特征代码法，系统数据对比法，实时监控法，软件模拟法，检测常规内存数

6，试说明黑客攻击的一般流程及其技术和方法

信息安全试题（3/共3）

1、关于密码学的讨论中，下列（ D ）观点是不正确的。

A、密码学是研究与信息安全相关的方面如机密性、完整性、实体鉴别、抗否认等的综

合技术

B、密码学的两大分支是密码编码学和密码分析学

C、密码并不是提供安全的单一的手段，而是一组技术

D、密码学中存在一次一密的密码体制，它是绝对安全的

2、在以下古典密码体制中，属于置换密码的是（ B）。

A、移位密码 B、倒序密码

C、仿射密码 D、PlayFair密码

3、一个完整的密码体制，不包括以下（ C ）要素。

A、明文空间 B、密文空间

C、数字签名 D、密钥空间

4、关于DES算法，除了（C ）以外，下列描述DES算法子密钥产生过程是正确的。

A、首先将 DES 算法所接受的输入密钥 K（64 位），去除奇偶校验位，得到56位密钥（即经过PC-1置换，得到56位密钥）

B、在计算第i轮迭代所需的子密钥时，首先进行循环左移，循环左移的位数取决于i的值，这些经过循环移位的值作为下一次循环左移的输入

C、在计算第i轮迭代所需的子密钥时，首先进行循环左移，每轮循环左移的位数都相同，这些经过循环移位的值作为下一次循环左移的输入

D、然后将每轮循环移位后的值经PC-2置换，所得到的置换结果即为第i轮所需的子密钥Ki

5、2000年10月2日，NIST正式宣布将（ B ）候选算法作为高级数据加密标准，该算法是由两位比利时密码学者提出的。

A、MARS B、Rijndael

C、Twofish D、Bluefish

6、根据所依据的数学难题，除了（ A ）以外，公钥密码体制可以分为以下几类。

A、模幂运算问题 B、大整数因子分解问题

C、离散对数问题 D、椭圆曲线离散对数问题

7、密码学中的杂凑函数（Hash函数）按照是否使用密钥分为两大类：带密钥的杂凑函数和不带密钥的杂凑函数，下面（ C ）是带密钥的杂凑函数。

A、MD4 B、SHA-1

C、whirlpool D、MD5

8、完整的数字签名过程（包括从发送方发送消息到接收方安全的接收到消息）包括（C ）和验证过程。

A、加密 B、解密

C、签名 D、保密传输

9、除了（ D ）以外，下列都属于公钥的分配方法。

A、公用目录表 B、公钥管理机构

C、公钥证书 D、秘密传输

10、密码学在信息安全中的应用是多样的，以下（ A ）不属于密码学的具体应用。

A、生成种种网络协议 B、消息认证，确保信息完整性

C、加密技术，保护传输信息 D、进行身份认证

得分 评卷人

1、信息安全中所面临的威胁攻击是多种多样的，一般将这些攻击分为两大类（主动攻击）和被动攻击。其中被动攻击又分为（消息内容的泄露）和（进行业务流分析）。

2、密码技术的分类有很多种，根据加密和解密所使用的密钥是否相同，可以将加密算法分为：对称密码体制和（非对称密码体制），其中对称密码体制又可分为两类，按字符逐位加密的（序列密码）和按固定数据块大小加密的（分组密码）。

3、密码分析是研究密码体制的破译问题，根据密码分析者所获得的数据资源，可以将密码分析（攻击）分为：（惟密文分析）、已知明文分析（攻击）、（选择明文分析）和选择密文分析（攻击）。

4、古典密码学体制对现代密码学的研究和学习具有十分重要的意义，实现古典密码体制的两种基本方法（代换）和（置换）仍是构造现代对称分组密码的核心方式。

5、（DES）是美国国家标准局公布的第一个数据加密标准，它的分组长度为（64）位，密钥长度为（64（56））位。

6、1976年，美国两位密码学者Diffe和Hellman在该年度的美国计算机会议上提交了一篇论文，提出了（公钥密码体制）的新思想，它为解决传统密码中的诸多难题提出了一种新思路。

7、Elgamal算法的安全性是基于（离散对数问题），它的最大特点就是在加密过程中引入了一个随机数，使得加密结果具有（不确定性），并且它的密文长度是明文长度的（两）倍。该算法的变体常用来进行数据签名。

8、密码系统的安全性取决于用户对于密钥的保护，实际应用中的密钥种类有很多，从密钥管理的角度可以分（初始密钥）、（会话密钥）、密钥加密密钥和（主密钥）。

得分 评卷人

1、 古典密码体制中代换密码有哪几种，各有什么特点？

2、 描述说明DES算法的加解密过程（也可以画图说明）。

3、 以DES为例，画出分组密码的密码分组链接（CBC）模式的加密解密示意图，假设加密时明文一个比特错误，对密文造成什么影响，对接收方解密会造成什么影响？

4、简述公钥密码体制的基本思想以及其相对于传统密码体制的优势。

5、 简述数字签名的基本原理及过程。

四、计算题（每题10分，共20分）

1、 计算通过不可约多项式X8+X4+X3+X+1构造的GF（28）上，元素（83）H的乘法逆元。

2、 RSA算法中，选择p=7,q=17,e=13,计算其公钥与私钥，并采用快速模乘（反复平方乘）方法，加密明文m=（19）10。

1、 答：在古典密码学中，有四种类型的代替密码：

①简单代替密码（或单表代替密码）（1分），它将明文字母表中的每个字母用密文字母表中的相应字母来代替，明密文表字母存在惟一的一一对应关系，然后通过明密文对照表来进行加解密，容易受到频率统计分析攻击，例如：恺撒密码、仿射密码等（1分）。②多名码代替密码（1分），将明文中的每个字母按一定规律映射到一系列密文字母，这一系列密文字母称为同音字母，它的密文的相关分布会接近于平的，能够较好挫败频率分析，较简单代替密码难破译（1分）。③多字母代替密码（1分），通过一次加密一组字母来使密码分析更加困难，例如Playfair密码（1分）。④多表代替密码（1分），使用从明文字母到密文字母的多个映射，每个映射像简单代替密码中的一一对应，比简单代替密码更安全一些，例如，维吉尼亚密码等（1分）。

2、 答：DES算法是一个分组加密算法，它以64位分组（0.5分）对数据进行加密，其

初始密钥也是64位，它的加密过程可以描述如下：①64位密钥经子密钥产生算法产生出16个子密钥：K1，K2，…K16，分别供第一次，第二次， …，第十六次加密迭代使用（1分）。②64位明文经初始置换IP（0.5分），将数据打乱重排并分成左右两半。左边为L0，右边为R0： X=L0R0=IP(x)。③16轮（0.5分）轮变换，每轮（第i轮）操作如下：在轮子密钥Ki的控制下，由轮函数f对当前轮输入数据的右半部分Ri-1进行加密：第一步，将Ri-1经过E盒置换扩展成48位（0.5分），第二步，将Ri-1与48位的轮子密钥Ki逐比特异或（0.5分），第三步，对Ri-1进行S盒压缩代换，将其压缩为32位（0.5分），第四步，对Ri-1进行P盒置换（0.5分）。然后，将Ri-1与当前轮输入的左半部分Li-1进行逐比特异或，将该运算结果作为当前轮（第i轮）右半部份的输出Ri=Li-1⊕f(Ri-1,Ki)（0.5分）；将本轮输入的右半部分数据作为本轮输出的左半部分数据：Li=Ri-1（0.5分）。④16轮变换结束后，交换输出数据的左右两部分：X=R16L16（1分）。⑤经过逆初始变换IP-1输出密文（0.5分）。对于DES算法来说，其解密过程与加密过程是同一过程，只不过使用子密钥的顺序相反（1分）。

3、答：因为计算机数据自身的特殊性以及不同场合对于数据加密速度及效率的不同需求，再采用分组对称密码进行数据加密时往往要选择相应的工作模式，密文链接模式（CBC）就是其中的一种。①以DES分组密码为例，CBC模式的加密示意图如下（2分）：

②以DES分组密码为例，CBC模式的解密示意图如下（2分）：

③加密时明文的一个比特错误，会导致该组加密密文发生变化，然后这个错误反馈值会作为下一次DES加密的输入值，再经过DES加密变换。会导致后面的密文都受到影响（2分）。④对于接收方来说，加密明文的一个比特错误，只会影响对应明文块所产生的密文的正常解密，其他数据块可以正常准确地解密（2分）。

4、答：①公钥密码体制的基本思想是把密钥分成两个部分：公开密钥和私有密钥（简称公钥和私钥），公钥可以向外公布，私钥则是保密的（1分）；密钥中的任何一个可以用来加密，另一个可以用来解密（1分）；公钥和私钥必须配对使用，否则不能打开加密文件（1分）；已知密码算法和密钥中的一个，求解另一个在计算上是不可行的（1分）。②相对于传统密码体制来说，公钥密码体制中的公钥可被记录在一个公共数据库里或以某种可信的方式公开发放，而私有密钥由持有者妥善地秘密保存。这样，任何人都可以通过某种公开的途径获得一个用户的公开密要，然后进行保密通信，而解密者只能是知道私钥的密钥持有者（1分），该体制简化了密钥的分配与分发（1分）；同时因为公钥密码体制密钥的非对称性以及私钥只能由持有者一个人私人持有的特性（1分），使得公钥密码体制不仅能像传统密码体制那样用于消息加密，实现秘密通信，还可以广泛应用于数字签名、认证等领域（1分）。

5、答：数字签名与加密不同，它的主要目的是保证数据的完整性和真实性，一般包括两部分：签名算法和验证算法，通常由公钥密码算法和杂凑函数（Hash算法）结合实现。假设发送方A要向接收方B发送一消息M，并对该消息进行数字签名，其具体的原理和过程如下：①发送方A采用杂凑函数生成要发送消息M的消息摘要：Hash（M）（2分）；②发送方A采用自己的私钥Pra对消息M的消息摘要加密，实现签名：EPRa(Hash(M))，并将签名与消息M并联形成最终要发送的消息：M|| EPRa(Hash(M)),然后发送该消息（2分）；③接收方B接收到消息后，采用发送方A的公钥Pua解密签名，恢复原始消息的摘要：Hash(M)=DPUa(EPRa(Hash(M)))（2分）；④接收方B采用杂凑函数，重新计算消息M的消息摘要：H’ash(M)，并与从发送方A接收到的消息摘要进行比较,若相等，则说明消息确实是发送方A发送的，并且消息的内容没有被修改过（2分）。数字签名技术对网络安全通信及各种电子交易系统的成功有重要的作用。

1、解：①将元素（83）H转换为二进制数据为（10000011）2（0.5分）；

②将二进制数据（10000011）2转换为给定有限域上的多项式：X7+X+1（0.5分）；

③利用欧几里得扩展算法求解以上多项式在指定有限域上的逆多项式（每步（行）2分））：

Q（X） A1（X） A2（X） A3（X） B1(X) B2（X） B3(X)

—— 1 0 X8+X4+X3+X+1 0 1 X7+X+1

X 0 1 X7+X+1 1 X X4+X3+X2+1

X3+X2+1 1 X X4+X3+X2+1 X3+X2+1 X4+X3+X+1 X

X3+X2+X X3+X2+1 X4+X3+X+1 X X6+X2+X+1 X7 1

由以上计算可知，在给定有限域中X7+X+1的逆多项式为X7；

④将多项式X7用二进制数据表示为：（10000000）2（0.5分）；

⑤将二进制数据（10000000）2转换为十六进制（80）H（0.5分）；

⑥元素（83）H在给定有限域上的乘法逆元为（80）H。

3、 解：①密钥的生成：

● 模数n=p×q=7×17=119，f(n)=（p-1）×（q-1）=6×16=96（0.5分）；

● 因为加密指数e和私密钥d满足：ed mod f(n) =1,所以d=e-1 mod f(n) ,私钥d的计算过程如下（1分）：

Q A1 A2 A3 B1 B2 B3

—— 1 0 96 0 1 13

7 0 1 13 1 -7 5

2 1 -7 5 -2 15 3

1 -2 15 3 3 -22 2

1 3 -22 2 -5 37 1

由以上计算可知私密钥d=37。

● 公钥为（e,n）=(13,119),私钥为的d=37（0.5分）。

②使用以上密钥对，采用反复平方乘方法加密明文m=（19）10，计算过程如下：

● 采用RSA算法加密明文，密文c=me mod n=1913 mod 119

● 将加密指数e=13用二进制表示：（1101）2，则有（每步（计算行）2分）：

k bi d

3 1 ((12 mod 119) ×19)mod119 = 19

2 1 ((192 mod 119) ×19) mod 119 = 76

1 0 (76)2 mod 119 = 64

0 1 ((64)2 mod 119) ×19) mod 119 = 117

由以上计算可知，密文为（117）10。

第一部分　判断题(共65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。

参考答案：对

2、由于传输的不同，电力线可以与网络线同槽铺设。

参考答案：错

3、机房供电线路和电力、照明用电可以用同一线路。

参考答案：错

4、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。

参考答案：对

5、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。

参考答案：对

6、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。

参考答案：错

7、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。

参考答案：错

8、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。

参考答案：对

9、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。

参考答案：对

10、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。

参考答案：对

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

参考答案：错

12、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又是该组成员，则Lois也有此权限。

参考答案：对

13、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。

参考答案：对

14、每个UNIX/Linux系统中都只有一个特权用户，就是root帐号。

参考答案：错

15、SQL注入攻击不会威胁到操作系统的安全。

参考答案：错

16、不需要对数据库应用程序的开发者制定安全策略。

参考答案：错

17、防火墙安全策略一旦设定，就不能再做任何改变。

参考答案：错

18、只要使用了防火墙，企业的网络安全就有了绝对的保障。

参考答案：错

19、半连接扫描也需要完成TCP协议的三次握手过程。

参考答案：错

20、防火墙是设置在内部网络与外部网络（如互联网）之间、或不同内部网络之间，实施访问控制策略的一个或一组系统。

参考答案：对

21、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

参考答案：对

22、与入侵检测系统不同，入侵防御系统采用在线（inline）方式运行。

参考答案：对

23、企业内部只需要在网关和各服务器上安装防病毒软件，客户端不需要安装。

参考答案：错

24、运行防病毒软件可以帮助防止遭受网页仿冒欺诈。

参考答案：对

25、包含收件人个人信息的邮件是可信的。

参考答案：错

26、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。

参考答案：错

27、网络边界保护中主要采用防火墙系统，为了保证其有效发挥作用，应当避免在内网和外网之间存在不经过防火墙控制的其他通信连接。

参考答案：对

28、根据ISO13335标准，信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。

参考答案：错

29、在我国严重的网络犯罪行为也不需要接受刑法的相关处罚。

参考答案：错

30、安全管理的合规性，主要是指在有章可循的基础上，确保信息安全工作符合国家法律、法规、行业标准、机构内部的方针和规定。

参考答案：对

31、从事国际联网经营活动和非经营活动的介入单位在不符合条件时，其国际联网经营许可证由发证机关吊销。

参考答案：错

32、公安部、国家安全部、国家保密局、国务院是计算机信息系统安全保护工作的主管部门。

参考答案：错

33、任何单位和个人不得自行建立或者使用其他信道进行国际联网。

参考答案：对

34、经营国际联网业务的单位，有违法行为的，公安机关可以吊销其经营许可证或者取消其联网资格。

参考答案：错

35、已经联网的用户有对计算机信息信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的权利。

参考答案：错

36、互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织当发现本网络中有危害国家利益的内容的地址、目录时，应当按照规定把它删除。

参考答案：对

37、过滤王控制台必须和同步代理软件安装在同一电脑上

参考答案：对

38、临时卡必须每次刷卡都输入姓名证件号码

参考答案：对

39、过滤王管理中心地址是:221.136.69.81

参考答案：对

40、上网卡密码不可以修改

参考答案：对

第二部分　单项选择题(共118题)

1、下列（ ）行为，情节较重的，处以5日以上10日以下的拘留。

A、未经允许重装系统

B、故意卸载应用程序

C、在互联网上长时间聊天的

D、故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行

参考答案：D

2、公然侮辱他人或者捏造事实诽谤他人的，处（ ）。

A、5日以下拘留或者500元以下罚款

B、10日以上拘留或者500元以下罚款

C、5日以下拘留或者1000元以下罚款

D、10日以上拘留或者1000以下罚款

参考答案：A

3、违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的，处（ ）日以下拘留。

A、5

B、15

C、20

D、30

参考答案：A

4、计算机信息系统，是指由（ ）及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、储存、传输、检索等处理的人机系统。

A、计算机硬件

B、计算机

C、计算机软件

D、计算机网络

参考答案： B

5、过滤王连接公安中心端的地址是（）

A、221.136.69.81

B、221.136.69.82

C、221.136.69.137

D、221.136.69.137

参考答案：A

6、过滤王日志是存放在Winfgate目录下的哪个文件夹下的（）

A、sys

B、log

C、date

D、日志

参考答案： B

7、过滤王用户上网日志是存放在哪个文件夹下的（）

A、access\_log

B、alert\_log

C、sys\_log

D、user\_log

参考答案：A

8、过滤王服务端上网日志需保存（）天以上

A、7

B、15

C、30

D、60

参考答案：D

9、下列哪类证件不得作为有效身份证件登记上网（）

A、驾驶证

B、户口本

C、护照

D、暂住证

参考答案： B

10、下列哪一个日志文件的大小是正常的()

A、1KB

B、20KB

C、7,023KB

D、123,158KB

参考答案：D

11、过滤王上网的用户日志是存放在哪个文件夹下的（）

A、access\_log

B、alert\_log

C、sys\_log

D、user\_log

参考答案：D

12、代表了当灾难发生后，数据的恢复程度的指标是\_\_\_\_\_\_\_。

A、PRO

B、RTO

C、NRO

D、SDO

参考答案：A

13、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、SDO

参考答案： B

14、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\_\_\_\_\_\_\_。

A、磁盘

B、磁带

C、光盘

D、软盘

参考答案： B

15、下列叙述不属于完全备份机制特点描述的是\_\_\_\_\_\_\_。

A、每次备份的数据量较大

B、每次备份所需的时间也就较大

C、不能进行得太频繁

D、需要存储空间小

参考答案：D

16、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

参考答案： B

17、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

参考答案：D

18、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

参考答案：A

19、容灾的目的和实质是\_\_\_\_\_\_\_。

A、数据备份

B、心理安慰

C、保质信息系统的业务持续性

D、系统的有益补充

参考答案：C

20、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

参考答案：A

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

A、-1

B、0

C、1

D、2

参考答案： B

22、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

参考答案： B

23、在正常情况下，Windows 2000中建议关闭的服务是\_\_\_\_\_\_\_。

A、TCP/IP NetBIOS Helper Service

B、Logical Disk Manager

C、Remote Procedure Call

D、Security Accounts Manager

参考答案：A

24、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/group

C、设置足够强度的帐号密码

D、使用shadow密码

参考答案：A

25、下面不是SQL Server支持的身份认证方式的是\_\_\_\_\_\_\_。

A、Windows NT集成认证

B、SQL Server认证

C、SQL Server混合认证

D、生物认证

参考答案：D

26、下面不是Oracle数据库支持的备份形式的是\_\_\_\_\_\_\_。

A、冷备份

B、温备份

C、热备份

D、逻辑备份

参考答案： B

27、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\_\_\_\_\_\_\_。

A、本地帐号

B、域帐号

C、来宾帐号

D、局部帐号

参考答案：C

28、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\_\_\_\_\_\_\_。

A、上午8点

B、中午12点

C、下午3点

D、凌晨1点

参考答案：D

29、下面不是UNIX/Linux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

参考答案：D

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

A、chmod命令

B、/bin/passwd命令

C、chgrp命令

D、/bin/su命令

参考答案：D

31、下面不是保护数据库安全涉及到的任务是\_\_\_\_\_\_\_。

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

参考答案：C

32、有关数据库加密，下面说法不正确的是\_\_\_\_\_\_\_。

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

参考答案：C

33、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

参考答案：A

34、关于NAT说法错误的是\_\_\_\_\_\_\_

A、NAT允许一个机构专用Intranet中的主机透明地连接到公共域中的主机，无需每台内部主机都拥有注册的（已经越来越缺乏的）全局互联网地址

B、静态NAT是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法地址

C、动态NAT主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态NAT就会分配给用户一个IP地址，当用户断开时，这个IP地址就会被释放而留待以后使用

D、动态NAT又叫网络地址端口转换NAPT

参考答案：D

35、通用入侵检测框架(CIDF)模型中,\_\_\_\_\_\_\_的目的是从整个计算环境中获得事件,并向系统的其他部分提供此事件。

A、事件产生器

B、事件分析器

C、事件数据库

D、响应单元

参考答案：A

36、基于网络的入侵检测系统的信息源是\_\_\_\_\_\_\_。

A、系统的审计日志

B、事件分析器

C、应用程序的事务日志文件

D、网络中的数据包

参考答案：D

37、误用入侵检测技术的核心问题是\_\_\_\_\_\_\_的建立以及后期的维护和更新。

A、异常模型

B、规则集处理引擎

C、网络攻击特征库

D、审计日志

参考答案：C

38、下面说法错误的是\_\_\_\_\_\_\_。

A、由于基于主机的入侵检测系统可以监视一个主机上发生的全部事件，它们能够检测基于网络的入侵检测系统不能检测的攻击

B、基于主机的入侵检测系统可以运行在交换网络中

C、基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描

D、基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击，因为应用程序日志并不像操作系统审计追踪日志那样被很好地保护

参考答案：C

39、网络隔离技术，根据公认的说法，迄今已经发展了\_\_\_\_\_\_\_个阶段。

A、六

B、五

C、四

D、三

参考答案： B

40、当您收到您认识的人发来的电子邮件并发现其中有附件，您应该\_\_\_\_\_\_\_。

A、打开附件，然后将它保存到硬盘

B、打开附件，但是如果它有病毒，立即关闭它

C、用防病毒软件扫描以后再打开附件

D、直接删除该邮件

参考答案：C

41、不能防止计算机感染病毒的措施是\_\_\_\_\_\_\_。

A、定时备份重要文件

B、经常更新操作系统

C、除非确切知道附件内容，否则不要打开电子邮件附件

D、重要部门的计算机尽量专机专用，与外界隔绝

参考答案：A

42、下面关于DMZ区的说法错误的是\_\_\_\_\_\_\_

A、通常DMZ包含允许来自互联网的通信可进入的设备，如Web服务器、FTP服务器、SMTP服务器和DNS服务器等

B、内部网络可以无限制地访问外部网络DMZ区

C、DMZ可以访问内部网络

D、有两个DMZ的防火墙环境的典型策略是主防火墙采用NAT方式工作，而内部防火墙采用透明模式工作以减少内部网络结构的复杂程度

参考答案：C

43、使用漏洞库匹配的扫描方法，能发现\_\_\_\_\_\_\_。

A、未知的漏洞

B、已知的漏洞

C、自行设计的软件中的漏洞

D、所有的漏洞

参考答案： B

44、下面关于隔离网闸的说法，正确的是\_\_\_\_\_\_\_

A、能够发现已知的数据库漏洞

B、可以通过协议代理的方法，穿透网闸的安全控制

C、任何时刻，网闸两端的网络之间不存在物理连接

D、在OSI的二层以上发挥作用

参考答案：C

45、某病毒利用RPCDCOM缓冲区溢出漏洞进行传播，病毒运行后，在%System%文件夹下生成自身的拷贝nvchip4.exe，添加注册表项，使得自身能够在系统启动时自动运行。通过以上描述可以判断这种病毒的类型为\_\_\_\_\_\_\_。

A、文件型病毒

B、宏病毒

C、网络蠕虫病毒

D、特洛伊木马病毒

参考答案：C

46、包过滤防火墙工作在OSI网络参考模型的\_\_\_\_\_\_\_

A、物理层

B、数据链路层

C、网络层

D、应用层

参考答案：C

47、防火墙提供的接入模式不包括\_\_\_\_\_\_\_

A、网关模式

B、透明模式

C、混合模式

D、旁路接入模式

参考答案：D

48、下列技术不支持密码验证的是：

A、S/MIME

B、PGP

C、AMTP

D、SMTP

参考答案：D

49、下列不属于垃圾邮件过滤技术的是：

A、软件模拟技术

B、贝叶斯过滤技术

C、关键字过滤技术

D、黑名单技术

参考答案：A

50、下列技术不能使网页被篡改后能够自动恢复的是：

A、限制管理员的权限

B、轮询检测

C、事件触发技术

D、核心内嵌技术

参考答案：A

51、如果您认为您已经落入网络钓鱼的圈套，则应采取（ ）措施。

A、向电子邮件地址或网站被伪造的公司报告该情形

B、更改帐户的密码

C、立即检查财务报表

D、以上全部都是

参考答案：D

52、下面技术中不能防止网络钓鱼攻击的是：

A、在主页的底部设有一个明显链接，以提醒用户注意有关电子邮件诈骗的问题

B、利用数字证书（如USB KEY）进行登录

C、根据互联网内容分级联盟（ICRA）提供的内容分级标准对网站内容进行分级

D、安装杀毒软件和防火墙、及时升级、打补丁、加强员工安全意识

参考答案：C

53、以下不会帮助减少收到的垃圾邮件数量的是：

A、使用垃圾邮件筛选器帮助阻止垃圾邮件

B、共享电子邮件地址或即时消息地址时应小心谨慎

C、安装入侵检测软件

D、收到垃圾邮件后向有关部门举报

参考答案：C

54、内容过滤技术的含义不包括:

A、过滤互联网请求从而阻止用户浏览不适当的内容和站点

B、过滤流入的内容从而阻止潜在的攻击进入用户的网络系统

C、过滤流出的内容从而阻止敏感数据的泄露

D、过滤用户的输入从而阻止用户传播非法内容

参考答案：D

55、下列内容过滤技术中在我国没有得到广泛应用的是:

A、内容分级审查

B、关键字过滤技术

C、启发式内容过滤技术

D、机器学习技术

参考答案：A

56、会让一个用户的“删除”操作去警告其他许多用户的垃圾邮件过滤技术是：

A、黑名单

B、白名单

C、实时黑名单

D、分布式适应性黑名单

参考答案：D

57、不需要经常维护的垃圾邮件过滤技术是：

A、指纹识别技术

B、简单DNS测试

C、黑名单技术

D、关键字过滤

参考答案： B

58、《计算机信息系统安全保护条例》规定，故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品，由公安机关处以警告或者对个人处以( )的罚款、对单位处以（ ）的罚款

A、5000元以下 15000元以下

B、5000元 15000元

C、2000元以下 10000元以下

D、2000元 10000元

参考答案：A

59、PDR模型是第一个从时间关系描述一个信息系统是否安全的模型，PDR模型中的P，D，R代表分别代表（ ）。

A、保护 检测 响应

B、策略 检测 响应

C、策略 检测 恢复

D、保护 检测 恢复

参考答案：A

60、根据权限管理的原则，一个计算机操作员不应当具备访问（ ）的权限。

A、操作指南文档

B、计算机控制台

C、应用程序源代码

D、安全指南

参考答案：C

61、双机热备是一种典型的事先预防和保护措施，用于保证关键设备和服务的（ ）属性。

A、保密性

B、可用性

C、完整性

D、第三方人员

参考答案： B

62、（ ）手段可以有效应对较大范围的安全事件的不良影响，保证关键服务和数据的可用性。

A、定期备份

B、异地备份

C、人工备份

D、本地备份

参考答案： B

63、相对于现有杀毒软件在终端系统中提供保护不同，（ ）在内外边界处提供更加主动和积极的病毒保护。

A、防火墙

B、病毒网关

C、IPS

D、IDS

参考答案： B

64、《信息系统安全等级保护基本要求》中对不同级别的信息系统应具备的基本安全保护能力进行了要求，共划分为（ ）级。

A、4

B、5

C、6

D、7

参考答案：A

65、统计数据表明，网络和信息系统最大的人为安全威胁来自于（ ）

A、恶意竞争对手

B、内部人员

C、互联网黑客

D、第三方人员

参考答案： B

66、1999年，我国发布第一个信息安全等级保护的国家标准GB17859-1999，提出将信息系统的安全等级划分为（ ）个等级。

A、7

B、8

C、4

D、5

参考答案：D

67、互联网服务提供者和联网使用单位落实的记录留存技术措施，应当具有至少保存（ ）天记录备份的功能。

A、10

B、30

C、60

D、90

参考答案：C

68、定期对系统和数据进行备份，在发生灾难时进行恢复。该机制时为了满足信息安全的（ ）属性。

A、真实性

B、完整性

C、不可否认性

D、可用性

参考答案：D

69、公安部网络违法案件举报网站的网址是（ ）

A、www.netpolice.cn

B、www.gongan.cn

C、http://www.cyberpolice.cn

D、www.110.cn

参考答案：C

70、信息安全经历了三个发展阶段，以下（ ）不属于这个阶段。

A、通信保密阶段

B、加密机阶段

C、信息安全阶段

D、安全保障阶段

参考答案： B

71、信息安全在通信保密阶段对信息安全的关注局限在（ ）安全属性。

A、不可否认性

B、可用性

C、保密性

D、完整性

参考答案：C

72、信息安全管理领域权威的标准是（ ）。

A、ISO15408

B、ISO17799/ISO27001

C、ISO9001

D、ISO14001

参考答案： B

73、在PPDRR安全模式中，（ ）是属于安全事件发生后补救措施。

A、保护

B、恢复

C、响应

D、检测

参考答案： B

74、根据风险管理的看法，资产( )价值，( )脆弱性，被安全威胁( )，( )风险。

A、存在 利用 导致 具有

B、具有 存在 利用 导致

C、导致 存在 具有 利用

D、利用 导致 存在 具有

参考答案： B

75、互联网站链接境外新闻网站，登载境外新闻媒体和互联网站发布的新闻，必须另行报（ ）批准。

A、国务院新闻办公室

B、文化部

C、教育部

D、信息产业部

参考答案：A

76、（ ）在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项

A、公安部

B、国家安全部

C、中科院

D、司法部

参考答案：A

77、《中华人民共和国治安管理处罚法》规定，利用计算机信息网络传播淫秽信息的，处（ ）以下拘留，可以并处三千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

A、五日以下

B、五日以上十日以下

C、十日以上十五日

D、十五日

参考答案：C

78、互联单位主管部门对经营性接入单位实行（ ）制度。

A、月检

B、半年检

C、年检

D、周检

参考答案：C

79、计算机信息系统是指由指由（ ）及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理系统。

A、计算机硬件

B、计算机

C、计算机软件

D、计算机网络

参考答案： B

80、我国计算机信息系统实行（ ）保护。

A、责任制

B、主任值班制

C、安全等级

D、专职人员资格

参考答案：C

81、故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，（ ）的，应依法处5年以下有期徒刑或者拘役。

A、后果严重

B、产生危害

C、造成系统失常

D、信息丢失

参考答案：A

82、中华人民共和国进内的计算机信息网络进行国际联网，应当依照（ ）办理。

A、《中华人民共和国计算机信息系统安全保护条例》

B、《中华人民共和国计算机信息网络国际联网暂行规定实施办法》

C、《中华人民共和国计算机互联网国际联网管理办法》

D、《中国互联网络域名注册暂行管理办法》

参考答案： B

83、违反《计算机信息系统安全保护条例》的规定，构成（ ）的，依照《治安管理处罚法》的有关规定处罚。

A、犯罪

B、违反《刑法》

C、违反治安管理行为

D、违反计算机安全行为

参考答案：C

84、涉及国家事务、经济建设、国防建设、尖端科技等重要领域的单位的计算机信息网络与（ ），应当采取相应的安全保护措施。

A、任何单位

B、外单位

C、国内联网

D、国际联网

参考答案：D

85、电子公告服务提供者应当记录在电子公告服务系统中发布的信息内容及其发布时间、互联网地址或者域名。记录备份应当保存（ ）日。

A、90

B、60

C、30

D、10

参考答案： B

86、涉及国家秘密的计算机信息系统，（ ）地与国际互联网或者其他公共信息网络相连，必须实行物理隔离。

A、不得直接或者间接

B、不得直接

C、不得间接

D、不得直接和间接

参考答案：A

87、国际联网采用（ ）制定的技术标准、安全标准、资费政策，以利于提高服务质量和水平。

A、企业统一

B、单位统一

C、国家统一

D、省统一

参考答案：C

88、企业计算机信息网络和其他通过专线进行国际联网的计算机信息网络，只限于（ ）使用。

A、企业

B、外部

C、内部

D、专人

参考答案：C

89、（ ）违反计算机信息系统安全保护条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

A、计算机操作人员

B、计算机管理人员

C、任何组织或者个人

D、除从事国家安全的专业人员以外的任何人

参考答案：C

90、互联单位应当自网络正式联通之日起（ ）内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

A、15

B、30

C、45

D、60

参考答案： B

91、《计算机信息网络国际联网安全保护管理办法》规定，未建立安全保护管理制度的，采取安全技术保护措施，由公安机关（ ），给予（ ），还可（ ）；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可（ ）

A、责令限期改正 警告 没收违法所得 并处罚款

B、通报批评 警告 没收违法所得 并处罚款

C、通报批评 拘留 没收违法所得 并处罚款

D、责令限期改正 警告 没收违法所得 并处拘留

参考答案：A

92、根据《互联网电子公告服务管理规定》规定，（ ）发现电子公告服务系统中出现明显属于该办法第九条所列的禁止信息内容之一的，应当立即删除，保存有关记录，并向国家有关机关报告。

A、电子公告用户

B、电子公告浏览者

C、互联单位

D、电子公告服务提供者

参考答案：D

93、过滤王软件最多监控多少客户端?

A、100

B、200

C、300

D、400

参考答案：C

94、备份过滤王数据是备份哪些内容?

A、过滤控制台目录

B、过滤核心目录

C、核心目录下的ACCERS目录

D、核心目录下的几个目录

参考答案： B

95、安装过滤王核心的逻辑盘要留至少多少空闲空间?

A、1G

B、2G

C、3G

D、15G

参考答案：D

第三部分　多项选择题(共38题)

1、下列（ ）行为，情节较重的，可以处5日以上10日以下拘留，可以并处500元以下罚款。

A、偷窥、偷拍、窃听、散布他人隐私的

B、未经他人允许向其发送邮件的

C、利用手机向他人发送短信息的

D、捏造事实诬告陷害他人，企图使他人受到刑事追究或者受到治安管理处罚的

参考答案：A D

2、下列哪些是互联网提供的功能。（ ）

A、E-mail

B、BBS

C、FTP

D、WWW

参考答案：A B C D

2、对违反行政管理秩序的公民、法人或者其他组织，将要作出（ ）的行政处罚之前，行政处罚机关应制作《违法行为处理通知书》，并送达当事人。

A、警告

B、较大数额罚款

C、责令停产停业

D、暂扣或者吊销许可证

参考答案： B C D

4、系统数据备份包括对象有\_\_\_\_\_\_\_。

A、配置文件

B、日志文件

C、用户文档

D、系统设备文件

参考答案：A B D

5、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

参考答案：A B C D E

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\_\_\_\_\_\_\_。

A、Domain Admins组

B、Domain Users组

C、Domain Replicators组

D、Domain Guests组

参考答案：A B D

7、UNIX/Linux系统中的Apache服务器的主要安全缺陷表现在攻击者可以\_\_\_\_\_\_\_。

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

参考答案：A B C

8、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（Security Account Manager，简称SAM）模块

B、Windows系统的注册（WinLogon）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

参考答案：A B C

9、SQL Server中的预定义服务器角色有\_\_\_\_\_\_\_。

A、sysadmin

B、serveradmin

C、setupadmin

D、securityadmin

E、processadmin

参考答案：A B C D E

10、可以有效限制SQL注入攻击的措施有\_\_\_\_\_\_\_。

A、限制DBMS中sysadmin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

参考答案： B C D E

11、防火墙的局限性包括\_\_\_\_\_\_\_

A、防火墙不能防御绕过了它的攻击

B、防火墙不能消除来自内部的威胁

C、防火墙不能对用户进行强身份认证

D、防火墙不能阻止病毒感染过的程序和文件进出网络

参考答案：A B D

12、网络安全扫描能够\_\_\_\_\_\_\_

A、发现目标主机或网络

B、判断操作系统类型

C、确认开放的端口

D、识别网络的拓扑结构

E、测试系统是否存在安全漏洞

参考答案：A B C D E

13、入侵防御技术面临的挑战主要包括\_\_\_\_\_\_\_

A、不能对入侵活动和攻击性网络通信进行拦截

B、单点故障

C、性能“瓶颈”

D、误报和漏报

参考答案： B C D

14、病毒传播的途径有\_\_\_\_\_\_\_

A、移动硬盘

B、内存条

C、电子邮件

D、聊天程序

E、网络浏览

参考答案：A C D E

15、下列邮件为垃圾邮件的有：

A、收件人无法拒收的电子邮件

B、收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件

C、含有病毒、色情、反动等不良信息或有害信息的电子邮件

D、隐藏发件人身份、地址、标题等信息的电子邮件

E、含有虚假的信息源、发件人、路由等信息的电子邮件

参考答案：A C D E

16、内容过滤的目的包括：

A、阻止不良信息对人们的侵害

B、规范用户的上网行为，提高工作效率

C、防止敏感数据的泄露

D、遏制垃圾邮件的蔓延

E、减少病毒对网络的侵害

参考答案：A B C D E

17、所有进入网络和信息系统工作的人员，必须签订保密协议，具体协议保密协议的人员范围包括：（ ）

A、网络使用者

B、正式雇员

C、离职雇员

D、第三方人员

参考答案： B C D

18、我国信息网络重点单位一共分为12类，下列属于信息网络重点单位包括（ ）

A、党政机关

B、金融机构、邮电、广电部门、能源单位、交通运输单位

C、所有工程建设单位、互联网管理中心和重要网站

D、尖端科研单位、社会应急服务部门、重要物资储备单位

参考答案：A B C D

19、信息系统安全等级保护的核心是对信息系统分等级、按标准进行建设、管理和监督。信息系统安全等级保护实施过程中应遵循以下基本原则有（ ）

A、自主保护原则

B、重点保护原则

C、同步建设原则

D、动态调整原则

参考答案：A B C D

20、计算机病毒具有以下特点（ ）

A、传染性

B、隐蔽性

C、潜伏性

D、可预见性

E、破坏性

参考答案：A B C E

21、公安机关对计算机信息系统安全保护工作行使下列监督职权：（ ）

A、监督、检查、指导计算机信息系统安全保护工作

B、查处危害计算机信息系统安全的违法犯罪案件

C、履行计算机信息系统安全保护工作的其他监督职责

D、就涉及计算机信息系统安全的特定事项发布专项通令

参考答案：A B C D

22、违反《计算机信息系统安全保护条例》的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：（ ）

A、违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的

B、违反计算机信息系统国际联网备案制度的

C、按照规定时间报告计算机信息系统中发生的案件的

D、接到公安机关要求改进安全状况的通知后，在限期内拒不改进的

参考答案：A B D

23、任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款，情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚法的规定处罚；构成犯罪的，依法追究刑事责任： （ ）

A、捏造或者歪曲事实，散布谣言，扰乱社会秩序的

B、煽动抗拒、破坏宪法和法律、行政法规实施的

C、公然侮辱他人或者捏造事实诽谤他人的

D、表示对国家机关不满的

参考答案：A B C

24、任何人不得在电子公告服务系统中发布含有下列内容之一的信息： （ ）

A、反对宪法所确定的基本原则的、危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的

B、损害国家荣誉和利益的；煽动民族仇恨、民族歧视，破坏民族团结的

C、破坏国家宗教政策，宣扬邪教和封建迷信的

D、散布谣言、淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的

参考答案：A B C D

25、互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责 （ ）

A、负责本网络的安全保护管理工作，建立健全落实安全保护管理制度

B、负责对本网络用户的安全教育和培训

C、对委托发布信息的单位和个人进行登记，并对所提供的信息内容进行审核

D、发现计算机案件应当保留有关原始记录，并在二十四小时内向当地公安机关报告

参考答案：A B C D

26、为了保障互联网的运行安全，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：（ ）

A、侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统

B、故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害

C、违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行

D、非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密

参考答案：A B C D

27、安装过滤王核心需要哪些数据

A、网吧代码

B、管理中心地址

C、序列号

D、计算机名

参考答案：A B C

28、目前使用的过滤王核心的版本是多少?

A、5.0.00.141

B、5.0.00.142

C、5.0.00.143

D、5.0.00.146

参考答案：A B C D

29、过滤王可以过滤哪些类型的网站

A、赌博

B、邪教

C、暴力

D、色情

参考答案：A B C D

第四部分　填空题(共25题)

1、对发现人员身份信息录入有误的会员卡要及时\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，重新做新卡。

参考答案：注销

2、发行会员卡时必须严格核对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_后正确录入保存

参考答案：上网人员身份信息

3、与安装过滤王核心电脑相连接的交换机上，必须具有\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

参考答案：镜像端口

4、物理安全是指物理介质层次上对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_的网络信息的安全保护，是网络信息安全的最基本保障。

参考答案：存储和传输

5、容灾就是减少灾难事件发生的可能性以及限制灾难对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_所造成的影响的一整套行为。

参考答案：关键业务流程

6、数据备份是目的是为了\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_在崩溃时能够快速地恢复数据。

参考答案：系统数据

7、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是PKI系统安全的核心。

参考答案：CA

8、公钥密码体制有两种基本模型：一种是加密模型；另一种是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_模型。

参考答案：认证

9、著名的DES数据加密标准是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_加密系统

参考答案：对称

10、数据库恢复技术中，建立冗余数据最常用的技术有两种：第一种是数据备份，第二种是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

参考答案：日志文件

11、数据库访问控制的粒度可分为4个层次，分别是数据库级、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_、记录级（行级）和属性级（字段级）。

参考答案：表级

12、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是在密罐技术上逐步发展起来的一个新的概念，在其中可以部署一个或者多个密罐，来构成一个黑客诱捕网络体系架构。

参考答案：密网

13、在PDRR模型中，\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是静态防护转化为动态的关键，是动态相应的依据。

参考答案：检测

14、ISO 17799/ISO 27001最初是由\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_提出的国家标准。

参考答案：英国

15、凡是违反国家法律、危害计算机信息系统安全以及利用计算机信息系统实施的违法犯罪活动，统称计算机案件，计算机案件主要分为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_两类。

参考答案：刑事案件和行政案件

16、一个完整的信息安全保障体系，应当包括\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_五个主要环节，这就是PPDRR模型的内容。

参考答案：安全策略、保护、检测、响应、恢复

17、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是国家授权对信息安全和网络安全进行监控和管理的职能机构，各单位、组织都应当密切配合。

参考答案：公安部

18、GB 17859-1999的全称是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是建立计算机信息系统安全等级保护制度，实施安全等级管理的基础性标准。

参考答案：计算机信息系统安全保护等级划分准则

19、从事国际联网业务的单位和个人应当接受\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

参考答案：公安机关

20、任何单位发现有违反规定的有害信息的，应当保留原始纪录后及时删除，并在\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_小时内向当地公安机关报告；发现计算机犯罪案件，应立即向公安网监部门报案，并保护好现场。

参考答案：24

21、违反国家规定，对计算机信息系统功能进行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

参考答案：删除、修改、增加、干扰

22、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

参考答案：任何单位和个人

23、《计算机信息网络国际联网安全保护管理办法》规定了备案制度与罚则，\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_均为备案对象。

参考答案：接入服务单位、数据中心、信息服务单位、联网单位

24、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,是指互联网上一切可能对现存法律秩序和其他公序良俗造成破坏或者威胁的数据、新闻和知识等信息。

参考答案：互联网上的有害信息

25、过滤王自动保存最近\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_天的上网记录

参考答案：60

1．以下厂商为电子商务提供信息产品硬件的是\_\_\_C\_\_\_\_

A. AOL

B．YAHOO

C．IBM

D．MICROSOFT

2．把明文变成密文的过程，叫作\_\_A\_\_\_\_\_

A.加密

B．密文

C．解密

D．加密算法

3．以下加密法中属于双钥密码体制的是\_\_D\_\_\_\_\_

A．DES

B．AES

C．IDEA

D．ECC

4．MD-4散列算法，输入消息可为任意长，按\_\_\_A\_\_\_\_比特分组。

A．512

B．64

C．32

D．128

5．SHA算法中，输入的消息长度小于264比特，输出压缩值为\_\_\_\_C\_\_\_比特。

A．120

B．140

C．160

D．264

6.计算机病毒最重要的特征是\_\_\_B\_\_\_\_

A．隐蔽性

B．传染性

C．潜伏性

D．表现性

7．主要用于防火墙的VPN系统，与互联网密钥交换IKE有关的框架协议是\_\_A\_\_\_\_\_

A．IPSec

B．L2F

C．PPTP

D．GRE

8．Access VPN又称为\_\_\_A\_\_\_\_

A．VPDN

B．XDSL

C．ISDN

D．SVPN

9．以下不是接入控制的功能的是\_\_\_\_B\_\_\_

A．阻止非法用户进入系统

B．组织非合法人浏览信息

C．允许合法用户人进入系统

D．使合法人按其权限进行各种信息活动

10.在通行字的控制措施中，限制通行字至少为\_\_\_B\_\_\_\_字节以上。

A．3～6

B．6～8

C．3～8

D．4～6

11.用数字办法确认、鉴定、认证网络上参与信息交流者或服务器的身份是指\_\_\_B\_\_\_\_

A．接入控制

B．数字认证

C．数字签名

D．防火墙

12．关于密钥的安全保护下列说法不正确的是\_\_\_\_A\_\_\_

A．私钥送给CA

B．公钥送给CA

C．密钥加密后存人计算机的文件中

D．定期更换密钥

13. \_\_\_D\_\_\_\_在CA体系中提供目录浏览服务。

A．安全服务器

B．CA服务器

C．注册机构RA

D．LDAP服务器

14. Internet上很多软件的签名认证都来自\_\_\_D\_\_\_\_公司。

A．Baltimore

B．Entrust

C．Sun

D．VeriSign

15.目前发展很快的安全电子邮件协议是\_\_\_C\_\_\_\_ ，这是一个允许发送加密和有签名邮件的

协议。\_\_\_\_\_\_\_

A．IPSec

B．SMTP

C．S/MIME

D．TCP/1P

16.实现源的不可否认业务中，第三方既看不到原数据，又节省了通信资源的是\_\_\_C\_\_\_\_

A.源的数字签字

B．可信赖第三方的数字签字

C．可信赖第三方对消息的杂凑值进行签字

D．可信赖第三方的持证

17. SET的含义是\_\_\_B\_\_\_\_

A．安全电子支付协议

B．安全数据交换协议

C．安全电子邮件协议

D．安全套接层协议

18. 对SET软件建立了一套测试的准则。\_\_A\_\_\_\_\_

A．SETCo

B．SSL

C．SET Toolkit

D．电子钱包

19．CFCA认证系统的第二层为\_\_\_B\_\_\_\_

A．根CA

B．政策CA

C．运营CA

D．审批CA

20. SHECA提供了\_\_\_\_A\_\_\_种证书系统。

A．2

B．4

C．5

D．7

1. 信息安全受到的威胁有人为因素的威胁和非人为因素威胁，非人为因素的威胁包括　自然灾害　　　、　　系统故障　　、　技术缺陷　　。

2. 广义的信息安全是指网络系统的　　硬件　　、　软件　　及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，　网络服务　　　不中断，系统中的信息不因偶然的或恶意的原因而遭到　破坏　　　、　　更改　　和　　泄露　　　。

3. 密码学是一门关于　信息加密　　和　　密文破译　　的科学，包括　密码编码学　　　和 密码分析学 两门分支。

4. 信息隐藏技术的4个主要分支是　隐写术　　　、　隐通道　　、　匿名通信　　和　版权标识　　。

1. 信息安全的狭义解释

指信息内容的安全，包括信息的保密性、真实性和完整性。

2. 密码系统

指用于加密和解密的系统。

3. 数字水印

在数字化的信息载体中嵌入不明显的记号隐藏起来，被嵌入的信息包括作品的版权所有者、发行者、购买者、作者的序列号、日期和有特殊意义的文本等。60

4. 消息认证码MAC

MAC就是带密钥的消息摘要函数或称为一种带密钥的数字指纹，它与普通的摘要函数是有本质区别的。

1. 简述数字签名的基本原理?

数字签名包含两个过程：签名过程和验证过程。由于从公开密钥不能推算出私有密钥，因此公开密钥不会损害私有密钥的安全性；公开密钥无需保密，可以公开传播，而私有密钥必须保密。因此若某人用其私有密钥加密消息，并且用其公开密钥正确解密，就可肯定该消息是某人签名的。因为其他人的公开密钥不可能正确解密该加密过的消息，其他人也不可能拥有该人的私有密钥而制造出该加密过的消息，这就是数字签名的原理。

2. 数据备份的种类有哪些？常用的方法有哪些？？

数据备份按照备份时所备份数据的特点可以分为三种：完全备份、增量备份和系统备份。根据数据备份所使用的存储介质种类可以将数据备份方法分成如下若干种：软盘备份、磁带备份、可移动存储备份、可移动硬盘备份、本机多硬盘备份和网络备份。

3. 简述密码策略和帐户策略？

账户策略定义在计算机上，然而却可以影响用户账户与计算机或域交互作用的方式。账户策略在安全区域有如下内容的属性。

（1）密码策略：对于域或本地用户账户，决定密码的设置，如强制性和期限。

（2）账户锁定策略：对于域或本地用户账户，决定系统锁定账户的时间以及锁定哪个账户。

（3）Kerberos策略：对于域用户账户，决定于Kerberos有关的设置，如账户有效期和强制性。

密码策略包含6个策略，及密码必须符合复杂性要求、密码长度最小值、密码最长存留期、密码最短存留期、强制密码历史、为域中所有用户使用可还原的加密来存储密码。

4. 简述Web安全目标及技术？。

Web安全目标是保护Web服务器及其数据的安全、保护Web服务器和用户之间传递信息的安全、保护终端用户计算机及其他人连入Internet的设备的安全。Web安全技术主要包括Web服务器安全技术、Web应用服务安全技术和Web浏览器安全技术。

5. 例举几种常见的攻击实施技术。

社会工程学攻击、口令攻击、漏洞攻击、欺骗攻击、拒绝服务攻击等。

1.通常为保证信息处理对象的认证性采用的手段是\_\_\_C\_\_\_\_\_\_\_

A.信息加密和解密 B.信息隐匿

C.数字签名和身份认证技术 D.数字水印

2.关于Diffie-Hellman算法描述正确的是\_\_\_\_B\_\_\_\_\_\_

A.它是一个安全的接入控制协议 B.它是一个安全的密钥分配协议

C.中间人看不到任何交换的信息 D.它是由第三方来保证安全的

3.以下哪一项不在证书数据的组成中? \_\_\_\_\_D\_\_\_\_\_

A.版本信息 B.有效使用期限

C.签名算法 D.版权信息

4．关于双联签名描述正确的是\_\_\_\_D\_\_\_\_\_\_

A．一个用户对同一消息做两次签名 B．两个用户分别对同一消息签名

C．对两个有联系的消息分别签名 D．对两个有联系的消息同时签名

5．Kerberos中最重要的问题是它严重依赖于\_\_\_\_C\_\_\_\_\_\_

A．服务器 B．口令

C．时钟 D．密钥

6．网络安全的最后一道防线是\_\_\_\_A\_\_\_\_\_\_

A．数据加密 B．访问控制

C．接入控制 D．身份识别

7．关于加密桥技术实现的描述正确的是\_\_\_\_A\_\_\_\_\_\_

A．与密码设备无关，与密码算法无关 B．与密码设备有关，与密码算法无关

C．与密码设备无关，与密码算法有关 D．与密码设备有关，与密码算法有关

8．身份认证中的证书由\_\_\_\_A\_\_\_\_\_\_

A．政府机构发行 B．银行发行

C．企业团体或行业协会发行 D．认证授权机构发行

9．称为访问控制保护级别的是\_\_\_\_C\_\_\_\_\_\_

A．C1 B．B1

C．C2 D．B2

10．DES的解密和加密使用相同的算法，只是将什么的使用次序反过来? \_\_\_\_C\_\_\_\_\_\_

A．密码 B．密文

C．子密钥 D．密钥

11．PKI的性能中，信息通信安全通信的关键是\_\_\_\_\_C\_\_\_\_\_

A．透明性 B．易用性

C．互操作性 D．跨平台性

12．下列属于良性病毒的是\_\_\_\_D\_\_\_\_\_

A．黑色星期五病毒 B．火炬病毒

C．米开朗基罗病毒 D．扬基病毒

13．目前发展很快的基于PKI的安全电子邮件协议是\_\_\_\_A\_\_\_\_\_\_

A．S／MIME B．POP

C．SMTP D．IMAP

14．建立计算机及其网络设备的物理环境，必须要满足《建筑与建筑群综合布线系统工程设计规范》的要求，计算机机房的室温应保持在\_\_\_A\_\_\_\_\_\_\_

A．10℃至25℃之间 B．15℃至30℃之间

C．8℃至20℃之间 D．10℃至28℃之间

15．SSL握手协议的主要步骤有\_\_\_\_B\_\_\_\_\_\_

A．三个 B．四个

C．五个 D．六个

16．SET安全协议要达到的目标主要有\_\_\_\_C\_\_\_\_\_\_

A．三个 B．四个

C．五个 D．六个

17．下面不属于SET交易成员的是\_\_\_\_\_B\_\_\_\_\_

A．持卡人 B．电子钱包

C．支付网关 D．发卡银行

18．使用加密软件加密数据时，往往使用数据库系统自带的加密方法加密数据，实施

\_\_\_\_\_A\_\_\_\_\_

A．DAC B．DCA

C．MAC D．CAM

19．CTCA指的是\_\_\_\_B\_\_\_\_\_\_

A．中国金融认证中心 B．中国电信认证中心

C．中国技术认证中心 D．中国移动认证中心

20．下列选项中不属于SHECA证书管理器的操作范围的是\_\_\_\_\_C\_\_\_\_\_

A．对根证书的操作 B．对个人证书的操作

C．对服务器证书的操作 D．对他人证书的操作

1. Windows系统安全模型由 登录流程 、 本地安全授权　、　安全账号管理器和　安全引用监视器　组合而成。

2. 注册表是按照　　子树　、　项　、子项和　值　　组成的分层结构。实际上注册表只有两个子树: 　 HKEY\_LOCAL\_MACHINE　　和　HKEY\_USERS　　，但为了便于检索，用注册表编辑器打开注册表时，展现为五个子树，这些子树的总体组成了Windows中所有的系统配置。

3. 在Windows 2000 网络中有两种主要的帐号类型:　　域用户账号　　和　　本地用户账号　　。

5. E-mail系统主要由　　邮件分发代理　、邮件传输代理、邮件用户代理及　邮件工作站　　组成。

6. 电子邮件安全技术主要包括　　身份证认证技术、　加密签名技术、　协议过滤技术、　防火墙技术和　　邮件病毒过滤技术　。

1. 信息安全的狭义解释

信息安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，信息安全就是指信息处理和传输的安全。它包括硬件系统的安全可靠运行、操作系统和应用软件的安全、数据库系统的安全、电磁信息泄露的防护等。狭义的信息安全，就是指信息内容的安全，包括信息的保密性、真实性和完整性。P5

2. 密码系统

密码系统指用于加密和解密的系统。加密时，系统输入明文和加密密钥，加密变换后，输出密文；解密时，系统输入密文和解密密钥，解密变换后，输出明文。一个密码系统由信源、加密变换、解密变换、信宿和攻击者组成。密码系统强调密码方案的实际应用，通常应当是一个包含软、硬件的系统。P19

3. 数字水印

数字水印类似于信息隐藏，是在数字化的信息载体中嵌入不明显的记号隐藏起来，被嵌入的信息包括作品的版权所有者、发行者、购买者、作者的序列号、日期和有特殊意义的文本等，但目的不是为了隐藏或传递这些信息，而是在发现盗版或发生知识产权纠纷时，用来证明数字作品的来源、版本、原作者、拥有者、发行人以及合法使用人等。数字水印是数字化的多媒体作品版权保护的关键技术之一，也是信息隐藏的重要分支。P60

4. 消息认证码MAC

通常表示为MAC=Ck(M)，其中：M是长度可变的消息；K是收、发双方共享的密钥；函数值Ck(M)是定长的认证码，也称为密码校验和。MAC是带密钥的消息摘要函数，即一种带密钥的数字指纹，它与不带密钥的数字指纹是又本质区别的。P73

1. 常见的网络踩点方法有哪些？常见的网络扫描技术有哪些?

P335-1

方法：域名相关信息的查询、公司性质的了解、对主页进行分析、对目标IP地址范围进行查询和网络勘察等。

技术：端口扫描、共享目录扫描、系统用户扫描和漏洞扫描。

2. 简述欺骗攻击的种类及其原理？？

P336-5

DNS欺骗：域名解析过程中，假设当提交给某个域名服务器的域名解析请求的数据包截获，然后按截获者的意图将一个虚假的IP地址作为应答信息返回给请求者。

Web欺骗：攻击者通过伪造某个WWW站点的影像拷贝，使改影像Web的入口进入攻击者的Web服务器，并经过攻击者计算机的过滤作用，从而达到攻击者监控受攻击者的任何活动以获取有用的信息为目的。

IP欺骗：在服务器不存在任何漏洞的情况下，通过利用TCP/IP协议本身存在的一些缺陷进行攻击的方法。

电子邮件欺骗：攻击者佯称自己为系统管理员，给用户发送邮件要求用户修改口令或在貌似正常的附件中加载病毒或其他木马程序。

ARP欺骗：利用主机从网上接收到的任何ARP应答都会更新自己的地址映射表，而不管是否是真实的缺陷实施的攻击形式。

3. 简述拒绝服务攻击的原理和种类？。

P336-3

拒绝服务攻击广义上可以指任何导致用户的服务器不能正常提供服务的攻击。DoS攻击具有各种各样的攻击模式，是分别针对各种不同的服务而产生的。它对目标系统进行的攻击可以分为以下三类：消耗稀少的、有限的并且无法再生的系统资源；破坏或者更改系统的配置信息；对网络部件和设施进行物理破坏和修改。

4. 例举几种常见的攻击实施技术。

P335-2

社会工程学攻击、口令攻击、漏洞攻击、欺骗攻击、拒绝服务攻击等。

5. 简述TCP/IP协议的封装过程？

P131 图9-1-2

1. 试述RAID 0、RAID 1、RAID 3、RAID 5方案。

（1）RAID0：无冗余、无校验的磁盘阵列。RAID0至少使用两个磁盘驱动器，并将数据分成从512字节到数兆节的若干块（数据条带），这些数据块被交替写到磁盘中。RAID0不适用于对可靠性要求高的关键任务环境，但却非常适合于对性能要求较高的视频或图像编辑。

（2）RAID1：镜像磁盘阵列。每一个磁盘驱动器都有一个镜像磁盘驱动器，镜像磁盘驱动器随时保持与原磁盘驱动器的内容一致。RAID1具有较高的安全性，但只有一半的磁盘空间被用来存储数据。为了实时保护镜像磁盘数据的一致性，RAID1磁盘控制器的负载相当大，在此性能上没有提高。RAID1主要用于在对数据安全性要求很高，而且要求能够快速恢复损坏的数据的场合。

（3）RAID3：带奇偶校验码的并行传送。RAID3使用一个专门的磁盘存放所有的校验数据，而在剩余的磁盘中创建带区集分散数据的读写操作。RAID3适合用于数据密集型环境或单一用户环境，尤其有益于要访问较长的连续记录，例如数据库和Web服务器等。

（4）RAID5：无独立校验盘的奇偶校验磁盘阵列。RAID5把校验块分散到所有的数据盘中。RAID5使用了一种特殊的算法，可以计算出任何一个带区校验块的存放位置，这样就可以确保任何对校验块进行的读写操作都会在所有的RAID磁盘中进行均衡，从而消除了产生瓶颈的可能。RAID5能提供较完美的性能，因而也是被广泛应用的一种磁盘阵列方案。它适合于I/O密集、高读/写比率的应用程序，如事务处理等。为了具有RAID5级的冗余度，我们至少需要三个磁盘组成的磁盘阵列。RAID5可以通过磁盘阵列控制器硬件实现，也可以通过某些网络操作系统软件实现。P108

**网络安全知识竞赛题库**

一、单选题

1、网页恶意代码通常利用（ C ）来实现植入并进行攻击。

A、 口令攻击

B、 U盘工具

C、 IE浏览器的漏洞

D、 拒绝服务攻击

2、要安全浏览网页，不应该（ A ）。

A、 在他人计算机上使用“自动登录”和“记住密码”功能

B、 禁止使用Active（错）控件和Java 脚本

C、 定期清理浏览器Cookies

D、 定期清理浏览器缓存和上网历史记录

3、用户暂时离开时，锁定Windows系统以免其他人非法使用。锁定系统的快捷方式为同时按住( ) 。

A、 WIN键和Z键

B、 F1键和L键

C、 WIN键和L键

D、 F1键和Z键

4、网站的安全协议是https时，该网站浏览时会进行（ D ）处理。

A、 口令验证B、 增加访问标记C、 身份验证D、 加密

6、为了防范垃圾电子邮件，互联网电子邮件服务提供者应当按照信息产业部制定的技术标准建设互联网电子邮件服务系统，电子邮件服务器( C )匿名转发功能。

A、使用 B、开启 C、关闭

7、互联网电子邮件服务提供者对用户的( A )和互联网电子邮件地址负有保密的义务。

A、个人注册信息 B、收入信息 C、所在单位的信息

8、任何组织或个人不得利用互联网电子邮件从事传播淫秽色情信息、窃取他人信息或者等违法犯罪活动，否则构成犯罪的，依法追究刑事责任，尚不构成犯罪的，由公安机关等依照有关法律、行政法规的规定予以处罚；电信业务提供者从事上述活动的，并由电信管理机构依据( A )有关行政法规处罚。

A、故意传播计算机病毒 B、发送商业广告 C、传播公益信息

11、如果您发现自己被手机短信或互联网站上的信息诈骗后，应当及时向( C )报案，以查处诈骗者，挽回经济损失。

A、消费者协会 B、电信监管机构 C、公安机关

12、为了有效抵御网络黑客攻击，可以采用作为安全防御措施。 ( C )

A、绿色上网软件 B、杀病毒软件 C、防火墙

13、按照《互联网电子公告服务管理规定》，任何人不得在互联网上的电子布告牌（BBS）、电子白板、电子论坛、( B )、留言板等电子公告服务系统中发布淫秽、色情、赌博、暴力、恐怖等违法有害信息。

A、网站 B、网络聊天室 C、电子邮箱

14、使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于什么攻击类型? （A）

A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

15、为了防御网络监听，最常用的方法是 ( B )

A、采用物理传输（非网络） B、信息加密 C、无线网 D、使用专线传输

16、向有限的空间输入超长的字符串是哪一种攻击手段？（A）

A、缓冲区溢出 B、网络监听 C、拒绝服务 D、IP欺骗

17、主要用于加密机制的协议是(D)

A、HTTP B、FTP C、TELNET D、SSL

18、用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？ ( B )

A、缓存溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDOS攻击

19、在以下认证方式中，最常用的认证方式是：(A)

A、基于账户名／口令认证 B、基于摘要算法认证

C、基于PKI认证 D、基于数据库认证

20、下列不属于系统安全的技术是( B )

A、防火墙 ;B、加密狗 ;C、认证 ; D、防病毒

21、抵御电子邮箱入侵措施中，不正确的是（ D ）

A、不用生日做密码 B、不要使用少于5位的密码 C、不要使用纯数字 D、自己做服务器

22、不属于常见的危险密码是（ D ）

A、跟用户名相同的密码 B、使用生日作为密码 C、只有4位数的密码 D、10位的综合型密码

23、不属于计算机病毒防治的策略的是（ D ）

A、确认您手头常备一张真正“干净”的引导盘

B、及时、可靠升级反病毒产品

C、新购置的计算机软件也要进行病毒检测

D、整理磁盘

25、当今IT 的发展与安全投入，安全意识和安全手段之间形成( B )

A、安全风险屏障 B、安全风险缺口

C、管理方式的变革 D、管理方式的缺口

26、我国的计算机年犯罪率的增长是( C )

A、10% B、160% C、60% D、300%

27、信息安全风险缺口是指( A )

A、IT 的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

28、网络攻击与防御处于不对称状态是因为( C )

A、管理的脆弱性 B、应用的脆弱性

C、网络软硬件的复杂性 D、软件的脆弱性

29、网络攻击的种类( A )

A、物理攻击，语法攻击，语义攻击 B、黑客攻击，病毒攻击

C、硬件攻击，软件攻击 D、物理攻击，黑客攻击，病毒攻击

30、语义攻击利用的是( A )

A、信息内容的含义 B、病毒对软件攻击

C、黑客对系统攻击 D、黑客和病毒的攻击

31、计算机网络最早出现在哪个年代? ( B )

A、20世纪50年代 B、20世纪60年代

C、20世纪80年代 D、20世纪90年代

32、最早研究计算机网络的目的是什么？( C )

A、直接的个人通信； B、共享硬盘空间、打印机等设备；

C、共享计算资源； D、大量的数据交换。

33、以下关于DOS攻击的描述，哪句话是正确的？（ C ）

A、不需要侵入受攻击的系统

B、以窃取目标系统上的机密信息为目的

C、导致目标系统无法处理正常用户的请求

D、如果目标系统没有漏洞，远程攻击就不可能成功

34、许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么？（ C ）

A、安装防火墙 B、安装入侵检测系统

C、给系统安装最新的补丁 D、安装防病毒软件

35、以网络为本的知识文明人们所关心的主要安全是（ C ）

A、人身安全 B、社会安全 C、信息安全

47、第一次出现"HACKER"这个词是在（ B ）

A、BELL实验室 B、麻省理工AI实验室 C、AT&T实验室

36、可能给系统造成影响或者破坏的人包括（ A ）

A、所有网络与信息系统使用者 B、只有黑客 C、只有管理员

37、黑客的主要攻击手段包括（ A ）

A、社会工程攻击、蛮力攻击和技术攻击

B、人类工程攻击、武力攻击及技术攻击

C、社会工程攻击、系统攻击及技术攻击

38、从统计的情况看，造成危害最大的黑客攻击是( C )

A、漏洞攻击 B、蠕虫攻击 C、病毒攻击

39、第一个计算机病毒出现在( B )

A、40年代 B、70 年代 C、90年代

40、口令攻击的主要目的是( B )

A、获取口令破坏系统 B、获取口令进入系统 C、仅获取口令没有用途

41、通过口令使用习惯调查发现有大约\_B的人使用的口令长度低于5个字符的

A、50、5% B、51、 5% C、52、5%

42、通常一个三个字符的口令破解需要( B )

A、18毫秒 B、18 秒 C、18分钟

43、邮件炸弹攻击主要是( B )

A、破坏被攻击者邮件服务器 B、添满被攻击者邮箱

C、破坏被攻击者邮件客户端

44、逻辑炸弹通常是通过( B )

A、必须远程控制启动执行，实施破坏

B、指定条件或外来触发启动执行，实施破坏

C、通过管理员控制启动执行，实施破坏

45、扫描工具( C )

A、只能作为攻击工具 B、只能作为防范工具

C、既可作为攻击工具也可以作为防范工具

46、黑客造成的主要安全隐患包括( A )

A、破坏系统、窃取信息及伪造信息

B、攻击系统、获取信息及假冒信息

C、进入系统、损毁信息及谣传信息

47、从统计的资料看，内部攻击是网络攻击的( B )

A、次要攻击 B、最主要攻击 C、不是攻击源

48、一般性的计算机安全事故和计算机违法案件可由\_\_\_\_\_受理（ C ）

A、案发地市级公安机关公共信息网络安全监察部门

B、案发地当地县级（区、市）公安机关治安部门。

C、案发地当地县级（区、市）公安机关公共信息网络安全监察部门

D、案发地当地公安派出所

49、计算机刑事案件可由\_\_\_\_\_受理（ A ）

A、案发地市级公安机关公共信息网络安全监察部门

B、案发地市级公安机关治安部门

C、案发地当地县级（区、市）公安机关公共信息网络安全监察部门

D、案发地当地公安派出所

50、计算机信息系统发生安全事故和案件，应当\_\_\_\_\_\_在内报告当地公安机关公共信息网络安全监察部门（ D ）

A、8小时 B、48小时 C、36小时 D、24小时

51、对计算机安全事故的原因的认定或确定由\_\_\_\_\_作出（ C ）

A、人民法院 B、公安机关 C、发案单位 D、以上都可以

52、对发生计算机安全事故和案件的计算机信息系统，如存在安全隐患的，

B 应当要求限期整改。

A、人民法院 B、公安机关 C、发案单位的主管部门 D、以上都可以

53、传入我国的第一例计算机病毒是( B )

A、大麻病毒 B、小球病毒 C、1575病毒 D、米开朗基罗病毒

54、我国是在＿＿年出现第一例计算机病毒( C )

A、1980 B、1983 C、1988 D、1977

55、计算机病毒是( A )

A、计算机程序 B、数据 C、临时文件 D、应用软件

56、1994年我国颁布的第一个与信息安全有关的法规是( D )

A、国际互联网管理备案规定 B、计算机病毒防治管理办法

C、网吧管理规定 D、中华人民共和国计算机信息系统安全保护条例

57、网页病毒主要通过以下途径传播( C )

A、邮件 B、文件交换 C、网络浏览 D、光盘

58、故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，

后果严重的，将受到\_\_\_\_处罚( A )

A、处五年以下有期徒刑或者拘役 B、拘留 C、罚款 D、警告

59、计算机病毒防治产品根据\_\_\_\_标准进行检验( A )

A、计算机病毒防治产品评级准测 B、计算机病毒防治管理办法

C、基于DOS系统的安全评级准则 D、计算机病毒防治产品检验标准

60、《计算机病毒防治管理办法》是在哪一年颁布的( C )

A、1994 B、1997 C、2000 D、1998

61、VPN是指( A )

A、虚拟的专用网络 B、虚拟的协议网络 C、虚拟的包过滤网络

62、目前的防火墙防范主要是( B )

A、主动防范 B、被动防范 C、不一定

63、IP地址欺骗通常是( A )

A、黑客的攻击手段 B、防火墙的专门技术 C、IP 通讯的一种模式

黑客在攻击中进行端口扫描可以完成（ D ）。

A、 检测黑客自己计算机已开放哪些端口

B、口令破译

C、 获知目标主机开放了哪些端口服务

D、截获网络流量

64、Code Red爆发于2001年7月，利用微软的IIS漏洞在Web服务器之间传播。针对这一漏洞，微软早在2001年三月就发布了相关的补丁。如果今天服务器仍然感染Code Red，那么属于哪个阶段的问题?（C）

A、微软公司软件的设计阶段的失误 B、微软公司软件的实现阶段的失误

C、系统管理员维护阶段的失误 D、最终用户使用阶段的失误

65、木马程序一般是指潜藏在用户电脑中带有恶意性质的 ( A )，利用它可以在用户不知情的情况下窃取用户联网电脑上的重要数据信息。

A、远程控制软件 B、计算机操作系统 C、木头做的马

66、为了防止各种各样的病毒对计算机系统造成危害，可以在计算机上安装防病毒软件，并注意及时 ( B )，以保证能防止和查杀新近出现的病毒。

A、 分析 B、 升级 C、检查

67、局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样，则（ C ）。

A、两台计算机都正常

B、两台计算机都无法通讯

C、一台正常通讯一台无法通讯

68、企业重要数据要及时进行（ C ），以防出现以外情况导致数据丢失。

Ａ、杀毒 Ｂ、加密 Ｃ、备份

69、窃听是一种（ ）攻击，攻击者（ ）将自己的系统插入到发送站和接收站之间。截获是一种（ ）攻击，攻击者（ ）将自己的系统插入到发送站和接受站之间。（A）

A、 被动,无须,主动,必须

B、 主动,必须,被动,无须

C、 主动,无须,被动,必须

D、 被动,必须,主动,无须

70、可以被数据完整性机制防止的攻击方式是（D）。

A、 假冒源地址或用户的地址欺骗攻击

B、 抵赖做过信息的递交行为

C、 数据中途被攻击者窃听获取

D、 数据在途中被攻击者篡改或破坏

71、王某，未经著作权人许可，以私服营运方式，通过信息网络向公众传播他人网络游戏软件，获利14万余元，其行为均构成（ A ）。

A、侵犯著作权罪 B、侵犯商业秘密罪

C、非法侵入计算机信息系统罪 D、非法经营罪

72、任何组织或者个人注册微博客账号，制作、复制、发布、传播信息内容的，应当使用（ A ），不得以虚假、冒用的居民身份信息、企业注册信息、组织机构代码信息进行注册。网站开展微博客服务，应当保证前款规定的注册用户信息真实。

A真实身份信息 B正确的网站信息 C真实的ID D工商注册信息

73、2010年年底，熊某偶尔登录到一个境外的淫秽网站，发现该网站有大量的淫秽图片及视频可以观看，便在该网站上注册成为会员。之后，熊某渐渐沉迷于这些淫秽图片和视频，不能自拔。为获得更大的浏览权限，熊某便陆续发了17篇包含淫秽信息的帖子共被点击查看29410次，以不断提高自身的会员等级。熊某的行为（ B ）

A不构成犯罪 B构成传播淫秽物品罪

C构成非法经营罪 D构成制作、复制、出版、贩卖、传播淫秽物品牟利罪

74、文艺青年张小五写了一部反映社会现实的小说，发表后引起热烈反响，好评如潮。甲网站觉得有利可图，擅自将该小说发布在网络上，供网民在线阅读。该网站侵犯了张小五的哪种著作权？（ B ）

A发表权 B信息网络传播权 C复制权 D发行权

75、著作权行政管理部门对侵犯互联网信息服务活动中的信息网络传播权的行为实施行政处罚，适用（ A ）

A《著作权行政处罚实施办法》

B《互联网著作权行政保护办法》

C民法中关于知识产权的相关规定

D《商标法》

二、判断题

1、VPN的主要特点是通过加密使信息能安全的通过Internet传递。（对）

2、密码保管不善属于操作失误的安全隐患。（错）

3、漏洞是指任何可以造成破坏系统或信息的弱点。（对）

4、安全审计就是日志的记录。（错）

5、计算机病毒是计算机系统中自动产生的。（错）

6、对于一个计算机网络来说,依靠防火墙即可以达到对网络内部和外部的安全防护（错）

7、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（错）

8、最小特权、纵深防御是网络安全原则之一。（对）

9、安全管理从范畴上讲，涉及物理安全策略、访问控制策略、信息加密策略和网络安全管理策略。（对）

10、用户的密码一般应设置为16位以上。（对）

11、开放性是UNIX系统的一大特点。（对）

12、防止主机丢失属于系统管理员的安全管理范畴。（错）

13、我们通常使用SMTP协议用来接收E-MAIL。（错）

14、在堡垒主机上建立内部DNS服务器以供外界访问，可以增强DNS服务器的安全性。（错）

15、为了防御网络监听，最常用的方法是采用物理传输。（错）

16、使用最新版本的网页浏览器软件可以防御黑客攻击。（对）

17、通过使用SOCKS5代理服务器可以隐藏QQ的真实IP。（对）

18、一但中了IE窗口炸弹马上按下主机面板上的Reset键，重起计算机。（错）

19、禁止使用活动脚本可以防范IE执行本地任意程序。（对）

20、只要是类型为TXT的文件都没有危险。（错）

21、不要打开附件为SHS格式的文件。（对）

22、发现木马，首先要在计算机的后台关掉其程序的运行。（对）

23、限制网络用户访问和调用cmd的权限可以防范Unicode漏洞。（对）

24、解决共享文件夹的安全隐患应该卸载Microsoft网络的文件和打印机共享。（对）

25、不要将密码写到纸上。（对）

26、屏幕保护的密码是需要分大小写的。（对）

27、计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒。（对）

28、木马不是病毒。（对）

29．复合型防火墙防火墙是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用，同时也常结合过滤器的功能。（对）

30、非法访问一旦突破数据包过滤型防火墙，即可对主机上的软件和配置漏洞进行攻击。（错）

31、ATM 技术领先于TCP/IP技术，即将取代IP技术，实现语音、视频、数据传输网络的三网合一（错）

32、Internet设计之初，考虑了核战争的威胁，因此充分考虑到了网络安全问（错）

33、我的计算机在网络防火墙之内，所以其他用户不可能对我计算机造成威胁（错）

34、Internet没有一个集中的管理权威（对）

35、统计表明，网络安全威胁主要来自内部网络，而不是Internet（对）

36、只要设置了足够强壮的口令，黑客不可能侵入到计算机中（错）

37、路由器在转发IP分组时，一般不检查IP分组的源地址，因此可以伪造IP分组的源地址进行攻击，使得网络管理员无法追踪。（对）

38、发起大规模的DDoS攻击通常要控制大量的中间网络或系统（对）

39、路由协议如果没有认证功能，就可以伪造路由信息，导致路由表混乱，从而使网络瘫痪（对）

40、目前入侵检测系统可以及时的阻止黑客的攻击。（错）

41、TCSEC是美国的计算机安全评估机构和安全标准制定机构（对）

42、蠕虫、特洛伊木马和病毒其实是一回事（错）

43、只要选择一种最安全的操作系统，整个系统就可以保障安全（错）

44、在计算机系统安全中，人的作用相对于软件，硬件和网络而言，不是很重要（错）

45、在设计系统安全策略时要首先评估可能受到的安全威胁（对）

46、安装系统后应当根据厂商或安全咨询机构的建议对系统进行必要的安全配置（对）

47、系统安全的责任在于IT技术人员，最终用户不需要了解安全问题（错）

48．网络的发展促进了人们的交流，同时带来了相应的安全问题（错）

49．具有政治目的的黑客只对政府的网络与信息资源造成危害（错）

50、病毒攻击是危害最大、影响最广、发展最快的攻击技术（错）

51、黑色星期四"是因有人通过BELL实验室与Internet连接的有漏洞的机器上放置了一个蠕虫程序而引起网络灾难得名的（错）

52、邮件的附件如果是带有.exe、.com、.pif、.pl、.src和.vbs为后缀的文件，应确定其安全后再打开 (对)

53、在信息战中中立国的体现要比非信息战简单（错）

54、信息战的军事目标是指一个国家军队的网络系统、信息系统、数据资源（错）

55、计算机病毒是计算机系统中自动产生的（错）

56、小球病毒属于引导型病毒（对）

57、公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作（对）

58、计算机病毒防治产品实行销售许可证制度（对）

59、计算机病毒防治产品分为三级，其中三级品为最高级（错）

60，删除不必要的网络共享可以提高防范病毒的能力（对）

61、带VPN的防火墙一旦设置了VPN 功能，则所有通过防火墙的数据包都将

62、通过VPN通道进行通讯（错）

63、VPN的所采取的两项关键技术是认证与加密（对）

64、要保证一个公司总部与其分支机构的网络通讯安全只有通过VPN来实现（错）

65、网络安全工程实施的关键是质量，而质量的关键是服务的长期保障能力（对）

66、网络安全服务的开展与网络安全防范是一对矛盾（对）

67、网络安全边界防范的不完备性仅指防外不防内（错）

68、使用最新版本的网页浏览器软件可以防御黑客攻击。（错）

69、不要将密码写到纸上。（对）

70、计算机数据恢复在实际生活当中可以百分百恢复。（错）

71、违反国家法律、法规的行为，危及计算机信息系统安全的事件，称为计算机案件。（对）

72、计算机犯罪是行为人以计算机为工具或以计算机资产为犯罪对象实施的，依照我国刑法应受处罚的，具有社会危害性的行为。（对）

73、 计算机信息系统的安全威胁同时来自内、外两个方面。 （对）

74、外单位人员如可以随意接入奇瑞公司内网。（错）

75、格式化过后的计算机，原来的数据就找不回来了（错）

问答题：

1、今年我国首届国家网络安全宣传周的主题是什么？

答案：共建网络安全，共享网络文明

2、罗定职业技术学院的官方网址是什么？

答案：www.ldpoly.com 和 www.ldptc.cn

3、罗定职业技术学院政务和公益机构域名是什么？

答案：罗定职业技术学院.公益

4、首次使用CRP数字校园、校园一卡通等信息系统时，为了保存自已的信息和财产安全应当怎么做？

答案：进入信息系统修改密码，并将其设置为一个复杂的密码。

5、计算机网络最突出的优点是什么？

答案：共享资源

6、信息安全有哪些常见的威胁？

答案：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。

7、解决互联网安全问题的根本条件是什么？

答案：提高整个社会网民的互联网道德本质。

8、什么是钓鱼网站？

答案：“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的URL地址以及页面内容，或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的HTML代码，以此来骗取用户银行或信用卡账号、密码等私人资料。

9、什么是网络安全？

答案：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续可靠正常地运行，网络服务不被中断。

10、什么是木马？

答案：木马是一种带有恶意性质的远程控制软件。木马一般分为客户端（client）和服务器端（server）。客户端就是本地使用的各种命令的控制台，服务器端则是要给别人运行，只有运行过服务器端的计算机才能够完全受控。木马不会像病毒那样去感染文件。

11、什么是后门？

答案：后门是指一种绕过安全性控制而获取对程序或系统访问权的方法。

12、防范网络黑客防措施有哪些？

答案：①选用安全的口令②口令不得以明文方式存放在系统中③建立帐号锁定机制④实施存取控制⑤确保数据的安全

13、网络病毒的来源有哪些？

答案：邮件附件、E-mail 、Web服务器、文件共享。

14、局域网内部若出现ARP攻击，会出现哪两种两句现象？

答案：1.不断弹出“本机的（错）（错）（错）段地址与网络中的（错）（错）（错）段地址冲突”的对话框。2.计算机不能正常上网，出现网络中断的症状。

15、控制USB接口使用的目的？

答案：1、网络的安全 2、信息的保密

16、什么是IP欺骗？

答案：攻击者可通过伪装成被信任源IP地址等方式来骗取目标主机的信任。

17、电子邮件存在哪些安全性问题？

1、垃圾邮件包括广告邮件、骚扰邮件、连锁邮件、反动邮件等。垃圾邮件会增加网络负荷，影响网络传输速度，占用邮件服务器的空间。2、诈骗邮件通常指那些带有恶意的欺诈性邮件。利用电子邮件的快速、便宜，发信人能迅速让大量受害者上当。3、邮件炸弹指在短时间内向同一信箱发送大量电子邮件的行为，信箱不能承受时就会崩溃。4、通过电子邮件传播的病毒，大多数采用附件的形式夹带在电子邮件中。当收信人打开附件后，病毒会查询他的通讯簿，给其上所有或部分人发信，并将自身放入附件中，以此方式继续传播扩散。

18、什么是网络蠕虫？

答案：网络蠕虫是一种智能化、自动化，综合网络攻击、密码学和计算机病毒技术，无须计算机使用者干预即可运行的攻击程序或代码。

19、网络蠕虫有什么特征？

答案：具有病毒的特征，传染性，隐蔽性，破坏性；不利用文件寄生，可以主动传播，并且通过网络可快速传播，容易造成网络拥塞；具有智能化、自动化和高技术化；

20、防火墙的基本功能有哪些？

答案：1过滤进出网络的数据；2管理进出网络的访问行为；3封堵某些禁止的业务；4记录进出网络的信息和活动；5对网络的攻击进行将侧和报警。

21、因特网电子商务系统必须保证网络安全的四大要素是什么？

答案：1传输数据的保密性；2数据的完整性；3交易各方身份的真实性；

4交易的不可抵赖性；

21、对蠕虫病毒和一般病毒进行比较有什么区别？

答案：存在形式：普通病毒寄存在文件上，蠕虫病毒寄存在独立程序上；

传染机制：普通病毒在宿主程序上运行，蠕虫病毒会主动攻击；

传染目标：普通病毒传染本地文件，蠕虫病毒传染整个网络的计算机。

22、黑客攻击的动机都有哪些？

答案：1.好奇心理2.挑战性。3.报复心理4，经济利益5，政治目的，6.情报获取

23、什么是密码破解，有哪些方法？

答案：通过猜解或者直接破坏原密码的密码验证机制来达到和密码分析一样的最终效果，或者是密码对应的权限。

一般的密码破解大致分为以下几类。

1）使用软件无限次尝试密码。2）绕过密码验证机制。3）如果密码加密，使用替代密码代替原密码

24、后门程序与计算机病毒的差别是什么？

答案：后门程序又称特洛伊木马，其用途是潜伏在用户的计算机中，进行信息搜集或便于黑客进入。后门程序和计算机病毒最大的差别，在于后门程序不一定有自我复制的动作，即后门程序不一定会“感染”其他计算机。

25、黑客技术发展趋势是什么？

答案：（1）网络攻击的自动化程度和攻击速度不断提高（2）攻击工具越来越复杂（3）黑客利用安全漏洞的速度越来越快（4）防火墙被攻击者渗透的情况越来越多（5）安全威胁的不对称性在增加（6）攻击网络基础设施产生的破坏效果越来越大

26、什么是漏洞？

答案：漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

27、网络面临的安全威胁主要有哪些方面？

网络面临的安全威胁可分为两种：一是对网络数据的威胁；二是对网络设备的威胁。概括起来主要威胁包括以下几个方面：1）由自然力造成的非人为的数据丢失、设备失效、线路阻断。2）人为但属于操作人员无意的失误造成的数据丢失。3）来自外部和内部人员的恶意攻击和入侵。

28、IPv6先对IPv4有哪些优势？

IPv6优势：首先，IPv6解决了IP地址数量短缺的问题；其次，IPv6对IPv4协议中诸多不完善之处进行了较大的改进，在网络保密性、完整性方面作了更好的改进，在可控性和抗否认性方面有了新的保证。

29、计算机病毒传染的一般过程是什么？？

答案：1）判断传染目标（文件）是否符合感染条件（是否已经被感染）

2）若目标符合感染条件，则将病毒链接到传染目标的特点位置，并存入磁盘。

3）继续监视系统的运行，寻找新的传染目标

30、网络安全服务包括哪些？

答案：1、对等实体认证服务2、数据源点认证服务3数据保密服务4数据完整性服务5访问控制服务6可用性

1. 1单项选择题（1-605）
2. Chinese Wall 模型的设计宗旨是：（A）。

A、用户只能访问哪些与已经拥有的信息不冲突的信息 B、用户可以访问所有信息

C、用户可以访问所有已经选择的信息 D、用户不可以访问哪些没有选择的信息

1. 安全责任分配的基本原则是：（C）。

A、“三分靠技术，七分靠管理” B、“七分靠技术，三分靠管理”

C、“谁主管，谁负责” D、防火墙技术

1. 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（B）不属于信息运行安全技术的范畴。

A、风险分析 B、审计跟踪技术 C、应急技术 D、防火墙技术

1. 从风险的观点来看，一个具有任务紧急性，核心功能性的计算机应用程序系统的开发和维护项目应该（A）。

A、内部实现 B、外部采购实现 C、合作实现 D、多来源合作实现

1. 从风险分析的观点来看，计算机系统的最主要弱点是（B）。

A、内部计算机处理 B、系统输入输出 C、通讯和网络 D、外部计算机处理

1. 从风险管理的角度，以下哪种方法不可取？（D）

A、接受风险 B、分散风险 C、转移风险 D、拖延风险

1. 当今IT的发展与安全投入，安全意识和安全手段之间形成（B）。

A、安全风险屏障 B、安全风险缺口 C、管理方式的变革 D、管理方式的缺口

1. 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（D）。

A、已买的软件 B、定做的软件 C、硬件 D、数据

1. 当一个应用系统被攻击并受到了破坏后，系统管理员从新安装和配置了此应用系统，在该系统重新上线前管理员不需查看：（C）

A、访问控制列表 B、系统服务配置情况

1. 审计记录 D、用户账户和权限的设置

10、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行（B）。

1. 逻辑隔离 B、物理隔离 C、安装防火墙 D、VLAN 划分

11、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？（D）

A、威胁、脆弱性 B、系统价值、风险

C、信息安全、系统服务安全 D、受侵害的客体、对客体造成侵害的程度业务

12、公司应明确员工的雇佣条件和考察评价的方法与程序，减少因雇佣不当而产生的安全风险。人员考察的内容不包括（B）。

A、身份考验、来自组织和个人的品格鉴定 B、家庭背景情况调查

C、学历和履历的真实性和完整性 D、学术及专业资格

13、计算机信息的实体安全包括环境安全、设备安全、（B）三个方面。

A运行安全 B、媒体安全 C、信息安全 D、人事安全

14、目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（B）

A、公安部 B、国家保密局

C、信息产业部 D、国家密码管理委员会办公室

15、目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（B）

A、GB/T 18336-2001 信息技术安全性评估准则

B、GB 17859-1999 计算机信息系统安全保护等级划分准则

C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构

D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

16、确保信息没有非授权泄密，即确保信息不泄露给非授权的个人、实体或进程，不为其所用，是指（C）。

A、完整性 B、可用性 C、保密性 D、抗抵赖性

17、如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（A）

A、自动软件管理 B、书面化制度 C、书面化方案 D、书面化标准

18、如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？（A）

A、计算风险 B、选择合适的安全措施

C、实现安全措施 D、 接受残余风险

19、软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（A）

A、软件中止和黑客入侵 B、远程监控和远程维护

C、软件中止和远程监控 D、远程维护和黑客入侵

20、 管理审计指（C）

A、保证数据接收方收到的信息与发送方发送的信息完全一致

B、防止因数据被截获而造成的泄密

C、对用户和程序使用资源的情况进行记录和审查

D、保证信息使用者都可

21、为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（A）

A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B、进行离职谈话，禁止员工账号，更改密码

C、让员工签署跨边界协议

D、列出员工在解聘前需要注意的所有责任

22、为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（D）

A、人际关系技能 B、项目管理技能 C、技术技能 D、沟通技能

23、我国的国家秘密分为几级？（A）

A、3 B、4 C、5 D、6

24、系统管理员属于（C）。

A、决策层 B、管理层

C、执行层 D、既可以划为管理层，又可以划为执行层

25、下列哪一个说法是正确的？（C）

A、风险越大，越不需要保护 B、风险越小，越需要保护

C、风险越大，越需要保护 D、越是中等风险，越需要保护

26、下面哪类访问控制模型是基于安全标签实现的？（B）

A、自主访问控制 B、强制访问控制

C、基于规则的访问控制 D、基于身份的访问控制

27、下面哪项能够提供最佳安全认证功能？（B）

A、这个人拥有什么 B、这个人是什么并且知道什么

C、这个人是什么 D、这个人知道什么

28、下面哪一个是国家推荐性标准？（A）

A、GB/T 18020-1999 应用级防火墙安全技术要求

B、SJ/T 30003-93 电子计算机机房施工及验收规范

C、GA243-2000 计算机病毒防治产品评级准则

D、ISO/IEC 15408-1999 信息技术安全性评估准则

29、下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（C）

A、对安全违规的发现和验证是进行惩戒的重要前提

B、惩戒措施的一个重要意义在于它的威慑性

C、处于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训

D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

30、下面哪一项最好地描述了风险分析的目的？（C）

A、识别用于保护资产的责任义务和规章制度

B、识别资产以及保护资产所使用的技术控制措施

C、识别资产、脆落性并计算潜在的风险

D、识别同责任义务有直接关系的威胁

31、下面哪一项最好地描述了组织机构的安全策略？（A）

A、定义了访问控制需求的总体指导方针

B、建议了如何符合标准

C、表明管理意图的高层陈述

D、表明所使用的技术控制措施的高层陈述

32、下面哪一种风险对电子商务系统来说是特殊的？（D）

A、服务中断 B、应用程序系统欺骗

C、未授权的信息泄露 D、确认信息发送错误

33、下面有关我国标准化管理和组织机构的说法错误的是？（C）

A、国家标准化管理委员会是统一管理全国标准化工作的主管机构

B、国家标准化技术委员会承担国家标准的制定和修改工作

C、全国信息安全标准化技术委员负责信息安全技术标准的审查、批准、编号和发布

D、全国信息安全标准化技术委员负责统一协调信息安全国家标准年度技术项目

34、项目管理是信息安全工程师基本理论，以下哪项对项目管理的理解是正确的？（A）

A、项目管理的基本要素是质量，进度和成本

B、项目管理的基本要素是范围，人力和沟通

C、项目管理是从项目的执行开始到项目结束的全过程进行计划、组织

D、项目管理是项目的管理者，在有限的资源约束下，运用系统的观点，方法和理论，对项目涉及的技术工作进行有效地管理

35、信息安全的金三角是（C）。

A、可靠性，保密性和完整性 B、多样性，冗余性和模化性

C、保密性，完整性和可用性 D、多样性，保密性和完整性

36、信息安全风险缺口是指（A）。

A、IT的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

37、信息安全风险应该是以下哪些因素的函数？（A）

A、信息资产的价值、面临的威胁以及自身存在的脆弱性等

B、病毒、黑客、漏洞等

C、保密信息如国家密码、商业秘密等

D、网络、系统、应用的复杂的程度

38、信息安全工程师监理的职责包括？（A）

A、质量控制，进度控制，成本控制，合同管理，信息管理和协调

B、质量控制，进度控制，成本控制，合同管理和协调

C、确定安全要求，认可设计方案，监视安全态势，建立保障证据和协调

D、确定安全要求，认可设计方案，监视安全态势和协调

39、信息安全管理最关注的是？（C）

A、外部恶意攻击 B、病毒对PC的影响

C、内部恶意攻击 D、病毒对网络的影响

40、信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（C）

A、信息的价值 B、信息的时效性

C、信息的存储方式 D、法律法规的规定

41、信息网络安全的第三个时代是（A）

A、主机时代，专网时代，多网合一时代 B、主机时代，PC时代，网络时代

C、PC时代，网络时代，信息时代 D、2001年，2002年，2003年

42、一个公司在制定信息安全体系框架时，下面哪一项是首要考虑和制定的？（A）

A、安全策略 B、安全标准 C、操作规程 D、安全基线

43、以下哪个不属于信息安全的三要素之一？（C）

A、机密性 B、完整性 C、抗抵赖性 D、可用性

44、以下哪一项安全目标在当前计算机系统安全建设中是最重要的？（C）

A、目标应该具体 B、目标应该清晰

C、目标应该是可实现的 D、目标应该进行良好的定义

45、以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（A）

A、制度和措施 B、漏洞分析

C、意外事故处理计划 D、采购计划

46、以下哪一项是对信息系统经常不能满足用户需求的最好解释？（C）

A、没有适当的质量管理工具 B、经常变化的用户需求

C、用户参与需求挖掘不够 D、项目管理能力不强

47、以下哪一种人给公司带来了最大的安全风险？（D）

A、临时工 B、咨询人员 C、以前的员工 D、当前的员工

48、以下哪种安全模型未使用针对主客体的访问控制机制？（C）

A、基于角色模型 B、自主访问控制模型

C、信息流模型 D、强制访问控制模型

49、以下哪种措施既可以起到保护的作用还能起到恢复的作用？（C）

A、对参观者进行登记 B、备份

C、实施业务持续性计划 D、口令

50、以下哪种风险被定义为合理的风险？（B）

A、最小的风险 B、可接受风险

C、残余风险 D、总风险

51、以下人员中，谁负有决定信息分类级别的责任？（B）

A、用户 B、数据所有者 C、审计员 D、安全官

52、有三种基本的鉴别的方式：你知道什么，你有什么,以及（C）。

A、你需要什么 B、你看到什么 C、你是什么 D、你做什么

53、在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（B）

A、自下而上 B、自上而下 C、上下同时开展 D、以上都不正确

54、在风险分析中，下列不属于软件资产的是（D）

A、计算机操作系统 B、网络操作系统

C、应用软件源代码 D、外来恶意代码

55、在国家标准中，属于强制性标准的是：（B）

A、GB/T XXXX-X-200X B、GB XXXX-200X

C、DBXX/T XXX-200X D、QXXX-XXX-200X

56、在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（A）

A、当信息安全事件的负面影响扩展到本组织意外时

B、只要发生了安全事件就应当公告

C、只有公众的什么财产安全受到巨大危害时才公告

D、当信息安全事件平息之后

57、在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？（A）

A、标准（Standard） B、安全策略（Security policy）

C、方针（Guideline） D、流程(Proecdure)

58、在信息安全管理工作中“符合性”的含义不包括哪一项？（C）

A、对法律法规的符合 B、对安全策略和标准的符合

C、对用户预期服务效果的符合 D、通过审计措施来验证符合情况

59、在许多组织机构中，产生总体安全性问题的主要原因是（A）。

A、缺少安全性管理 B、缺少故障管理

C、缺少风险分析 D、缺少技术控制机制

60、职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（D）

A、数据安全管理员 B、数据安全分析员

C、系统审核员 D、系统程序员

61、中国电信的岗位描述中都应明确包含安全职责，并形成正式文件记录在案，对于安全职责的描述应包括（D）。

A、落实安全政策的常规职责 B、执行具体安全程序或活动的特定职责

C、保护具体资产的特定职责 D、以上都对

62、终端安全管理目标：规范支撑系统中终端用户的行为，降低来自支撑系统终端的安全威胁，重点解决以下哪些问题？（A）。

A、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

B、终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

C、终端接入和配置管理；桌面及主机设置管理；终端防病毒管理

D、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理

63、著名的橘皮书指的是（A）。

A、可信计算机系统评估标准(TCSEC) B、信息安全技术评估标准（ITSEC）

C、美国联邦标准（FC） D、通用准则（CC）

64、资产的敏感性通常怎样进行划分？（C）

A、绝密、机密、敏感 B、机密、秘密、敏感和公开

C、绝密、机密、秘密、敏感和公开等五类

D、绝密、高度机密、秘密、敏感和公开等五类

65、重要系统关键操作操作日志保存时间至少保存（C）个月。

A、1 B、2 C、3 D、4

66、安全基线达标管理办法规定：BSS系统口令设置应遵循的内控要求是（C）

A、数字+字母 B、数字+字母+符号

C、数字+字母+字母大小写 D、数字+符号

67、不属于安全策略所涉及的方面是（D）。

A、物理安全策略 B、访问控制策略

C、信息加密策略 D、防火墙策略

68、“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（C）。

A、“普密”、“商密”两个级别 B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别

D、“一密”、“二密”，“三密”、“四密”四个级别

69、对MBOSS系统所有资产每年至少进行（A）次安全漏洞自评估。

A、1 B、2 C、3 D、4

70、下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（A）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

71、中国电信各省级公司争取在1-3年内实现CTG-MBOSS 系统安全基线“达标”（C）级以上。

A、A级 B、B级 C、C级 D、D级

72、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

73、获取支付结算、证劵交易、期货交易等网络金融服务的身份认证信息（B）组以上的可以被《中华人民共和国刑法》认为是非法获取计算机信息系统系统认定的“情节严重”。

A、5 B、10 C、-15 D、20

74、基准达标项满（B）分作为安全基线达标合格的必要条件。

A、50 B、60 C、70 D、80

75、《国家保密法》对违法人员的量刑标准是（A）。

A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑

B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑

C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑

D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

76、$HOME/.netrc文件包含下列哪种命令的自动登录信息？（C）

A、rsh B、ssh C、ftp D、rlogin

77、/etc/ftpuser文件中出现的账户的意义表示（A）。

A、该账户不可登录ftp B、该账户可以登录ftp C、没有关系 D、缺少

78、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

79、Linux系统/etc目录从功能上看相当于Windows的哪个目录？（B）

A、program files B、Windows C、system volume information D、TEMP

80、Linux系统格式化分区用哪个命令？（A）

A、fdisk B、mv C、mount D、df

81、在Unix系统中，当用ls命令列出文件属性时，如果显示-rwxrwxrwx,意思是（A）。

A、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示其他用户的访问权限

B、前三位rwx表示文件同组用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

C、前三位rwx表示文件同域用户的访问权限；中间三位rwx表示文件属主的访问权限；后三位rwx表示其他用户的访问权限

D、前三位rwx表示文件属主的访问权限；中间三位rwx表示文件同组用户的访问权限；后三位rwx表示同域用户的访问权限

82、Linux系统通过（C）命令给其他用户发消息。

A、less B、mesg C、write D、echo to

83、Linux中，向系统中某个特定用户发送信息，用什么命令？（B）

A、wall B、write C、mesg D、net send

84、防止系统对ping请求做出回应，正确的命令是：（C）。

A、echo 0>/proc/sys/net/ipv4/icmp\_ehco\_ignore\_all

B、echo 0>/proc/sys/net/ipv4/tcp\_syncookies

C、echo 1>/proc/sys/net/ipv4/icmp\_echo\_ignore\_all

D、echo 1>/proc/sys/net/ipv4/tcp\_syncookies

85、NT/2K模型符合哪个安全级别？（B）

A、B2 B、C2 C、B1 D、C1

86、Red Flag Linux指定域名服务器位置的文件是（C）。

A、etc/hosts B、etc/networks C、etc/rosolv.conf D、/.profile

87、Solaris操作系统下，下面哪个命令可以修改/n2kuser/.profile文件的属性为所有用户可读、科协、可执行？（D）

A、chmod 744 /n2kuser/.profile B、 chmod 755 /n2kuser/.profile

C、 chmod 766 /n2kuser/.profile D、 chmod 777 /n2kuser/.profile

88、如何配置，使得用户从服务器A访问服务器B而无需输入密码？（D）

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhost文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/etc/hosts.equiv文件

89、Solaris系统使用什么命令查看已有补丁列表？（C）

A、uname –an B、showrev C、oslevel –r D、swlist –l product ‘PH??’

90、Unix系统中存放每个用户信息的文件是（D）。

A、/sys/passwd B、/sys/password C、/etc/password D、/etc/passwd

91、Unix系统中的账号文件是（A）。

A、/etc/passwd B、/etc/shadow C、/etc/group D、/etc/gshadow

92、Unix系统中如何禁止按Control-Alt-Delete关闭计算机？（B）

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

93、Unix中。可以使用下面哪一个代替Telnet，因为它能完成同样的事情并且更安全？（）

A、S-TELNET B、SSH C、FTP D、RLGON

94、Unix中，默认的共享文件系统在哪个位置？（C）

A、/sbin/ B、/usr/local/ C、/export/ D、/usr/

95、Unix中，哪个目录下运行系统工具，例如sh,cp等？（A）

A、/bin/ B、/lib/ C、/etc/ D、/

96、U盘病毒依赖于哪个文件打到自我运行的目的？（A）

A、autoron.inf B、autoexec.bat C、config.sys D、system.ini

97、Windows nt/2k中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

98、Windows 2000目录服务的基本管理单位是（D）。

A、用户 B、计算机 C、用户组 D、域

99、Windows 2000系统中哪个文件可以查看端口与服务的对应？（D）

A、c:\winnt\system\drivers\etc\services B、c:\winnt\system32\services

C、c:\winnt\system32\config\services D、c:\winnt\system32\drivers\etc\services

100、Windows NT/2000 SAM存放在（D）。

A、WINNT B、WINNT/SYSTEM32

C、WINNT/SYSTEM D、WINNT/SYSTEM32/config

101、 Windows NT/2000中的.pwl文件是？（B）

A、路径文件 B、口令文件 C、打印文件 D、列表文件

102、Windows NT的安全标识（SID）串是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是什么？（C）

A、击键速度 B、用户网络地址 C、处理当前用户模式线程所花费CPU的时间 D、PING的响应时间

103、Windows NT和Windows 2000系统能设置为在几次无效登录后锁定账号，可以防止：（B）。

A、木马 B、暴力破解 C、IP欺骗 D、缓冲区溢出攻击

104、Windows主机推荐使用（A）格式。

A、NTFS B、FAT32 C、FAT D、Linux

105、XP当前的最新补丁是（C）。

A、SP1 B、SP2 C、SP3 D、SP4

106、按TCSEC标准，WinNT的安全级别是（A）。

A、C2 B、B2 C、C3 D、B1

107、当你感觉到你的Win2003运行速度明显减慢，当打开任务管理器后发现CPU使用率达到了100%，你认为你最有可能受到了（D）攻击。

A、缓冲区溢出攻击 B、木马攻击 C、暗门攻击 D、DOS攻击

108、档案权限755，对档案拥有者而言，是什么含义？（A）

A、可读，可执行，可写入 B、可读

C、可读，可执行 D、可写入

109、如何配置，使得用户从服务器A访问服务器B而无需输入密码（D）。

A、利用NIS同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhosts文件

C、在两台服务器上创建并配置$HOME/.netrc文件

D、在两台服务器上创建并配置/et/hosts.equiv文件

110、要求关机后不重新启动，shutdown后面参数应该跟（C）。

A、–k B、–r C、-h D、 –c

111、一般来说，通过web运行http服务的子进程时，我们会选择（D）的用户用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

112、以下哪项技术不属于预防病毒技术的范畴？（A）

A、加密可执行程序 B、引导区保护

C、系统监控与读写控制 D、校验文件

113、用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？（B）

A、缓冲区溢出攻击 B、钓鱼攻击 C、暗门攻击 D、DDos攻击

114、与另一台机器建立IPC$会话连接的命令是（D）。

A、net user [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

B、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$) user:Administrator / passwd:aaa

C、net user \192.168.0.1IPC$ D、net use [\\192.168.0.1\IPC$](file:///\\192.168.0.1\IPC$)

115、在NT中，如果config.pol已经禁止了对注册表的访问，那么黑客能够绕过这个限制吗？怎样实现？（B）

A、不可以 B、可以通过时间服务来启动注册表编辑器

C、可以通过在本地计算机删除config.pol文件 D、可以通过poledit命令

116、在NT中，怎样使用注册表编辑器来严格限制对注册表的访问？（C）

A、HKEY\_CURRENT\_CONFIG,连接网络注册、登录密码、插入用户ID

B、HKEY\_CURRENT\_MACHINE,浏览用户的轮廓目录，选择NTUser.dat

C、HKEY\_USERS,浏览用户的轮廓目录，选择NTUser.dat

D、HKEY\_USERS,连接网络注册，登录密码，插入用户ID

117、在Solaris 8下，对于/etc/shadow文件中的一行内容如下“root:3vd4NTwk5UnLC:9038::::::”,以下说法正确的是：（E）。

A、这里的3vd4NTwk5UnLC是可逆的加密后的密码

B、这里的9038是指从1970年1月1日到现在的天数

C、这里的9038是指从1980年1月1日到现在的天数

D、这里的9038是指从1980年1月1日到最后一次修改密码的天数

E-以上都不正确

118、在Solaris 8下，对于/etc/shadow文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（A）。

A、是/etc/passwd文件格式 B、是/etc/shadow文件格式

C、既不是/etc/passwd也不是/etc/shadow文件格式

D、这个root用户没有SHELL，不可登录

E、这个用户不可登录，并不是因为没有SHELL

119、在Solaris系统中，终端会话的失败登录尝试记录在下列哪个文件里面?(D)

A、-/etc/default/login B、/etc/nologin

C、/etc/shadow D、var/adm/loginlog

120、在Windows 2000中，以下哪个进程不是基本的系统进程:(D)

A、smss. exe B、csrss. Exe C、winlogon. exe D、-conime.exe

121、在Windows 2000中可以察看开放端口情况的是:(D)。

A、nbtstat B、net C、net show D、netstat

122.、在Windows 2003下netstat的哪个参数可以看到打开该端口的PID?(C)（格式到此）

A、a B、n C、o D 、p

123.、在使用影子口令文件(shadowedpasswords)的Linux系统中，/etc/passwd文件和/etc/shadow文件的正确权限分别是(C)。

A、rw-r-----,-r-------- B、rw-r--r--,-r--r--r—

C、rw-r--r--,-r-------- Drw-r--rw-,-r-----r--

124.、制定数据备份方案时，需要重要考虑的两个因素为适合的备份时间和(B)。

A、备份介质 B、备份的存储位置

C、备份数据量 D、恢复备份的最大允许时间

125.、周期性行为，如扫描，会产生哪种处理器负荷?(A)

A、Idle Ioad B、Usage Ioad C、Traffic load D、以上都不对

126、主要由于(D)原因，使Unix易于移植

A、Unix是由机器指令书写的 B、Unix大部分由汇编少部分用C语言编写

C、Unix是用汇编语言编写的 D、Unix小部分由汇编大部分用C语言编写

127.、HP-UX系统中，使用(A)命令查看系统版本、硬件配置等信息。

A、uname -a B、ifconfig C、netstat D、ps -ef

128.、Linux文件权限一共10位长度，分成四段，第三段表示的内容是(C)。

A、文件类型 B、文件所有者的权限

C、文件所有者所在组的权限 D、其他用户的权限

129、在云计算虚拟化应用中，VXLAN技术处于OS工网络模型中2-3层间，它综合了2层交换的简单性与3层路由的跨域连接性。它是通过在UDP/IP上封装Mac地址而实现这一点的。在简单应用场合，vxLAN可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?(C)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

130.、Linux中，什么命令可以控制口令的存活时间了(A)。

A、chage B、passwd C、chmod D、umask

131.、Qfabric技术是使用市场上现成的计算和存储网元并利用行业标准的网络接口将它们连接后组建大规模的数据中心，以满足未来云计算的要求。该技术概念是哪个厂家主推的概念?(B)

A、惠普 B、uniper C、Cisco与Vmware D、博科Brocade

132、为了检测Windows系统是否有木马入侵，可以先通过()命令来查看当前的活动连接端口。

A、ipconfig B、netstat -rn C、tracert –d D、netstat -an

133、网络营业厅提供相关服务的可用性应不低于（A）。

A、99.99% B、99.9% C、99% D、98.9%

134.、IRF(Intelligent Resilient Framework)是在该厂家所有数据中心交换机中实现的私有技术，是应用在网络设备控制平面的多虚拟技术。该技术属于哪个厂家?(A)

A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade

135.、Windows NT的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:(D)。

A、击键速度 B、当前用户名

C、用户网络地址 D、处理当前用户模式线程所花费CPU的时间

136、脆弱性扫描，可由系统管理员自行进行检查，原则上应不少于(B)。

A、每周一次 B、每月一次 C、每季度一次 D、每半年一次

137、下面哪一个情景属于身份验证(Authentication)过程?(A)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

138、下面哪一个情景属于授权(Authorization)过程?(B)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

139、下列哪一条与操作系统安全配置的原则不符合?(D)

A、关闭没必要的服务 B、不安装多余的组件

C、安装最新的补丁程序 D、开放更多的服务

140、关于DDoS技术，下列哪一项描述是错误的(D)。

A、一些DDoS攻击是利用系统的漏洞进行攻击的

B、黑客攻击前对目标网络进行扫描是发功DDoS攻击的一项主要攻击信息来源

C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的DDoS攻击入侵

D、DDoS攻击不对系统或网络造成任何影响

141、关于PPP协议下列说法正确的是:(C)。

A、PPP协议是物理层协议

B、PPP协议是在HDLC协议的基础上发展起来的

C、PPP协议支持的物理层可以是同步电路或异步电路

D、PPP主要由两类协议组成:链路控制协议族CLCP)和网络安全方面的验证协议族(PAP和CHAP)

142、接口被绑定在2层的zone，这个接口的接口模式是（C）。

A、NAT mode B、Route mode

C、-Transparent mode D、NAT或Route mode

143、接入控制方面，路由器对于接口的要求包括：（D）。

A、串口接入 B、局域网方式接入 C、Internet方式接入 D、VPN接入

144、局域网络标准对应OSI模型的哪几层？（C）。

A、上三层 B、只对应网络层 C、下三层 D、只对应物理层

145、拒绝服务不包括以下哪一项？（D）。

A、DDoS B、畸形报文攻击 C、Land攻击 D、ARP攻击

146、抗DDoS防护设备提供的基本安全防护功能不包括（A）。

A、对主机系统漏洞的补丁升级 B、检测DDoS攻击

C、DDoS攻击警告 D、DDoS攻击防护

147、路由器产品提供完备的安全架构以及相应的安全模块，在软、硬件层面设置重重过滤，保护路由器业务安全。其中不对的说法是：（C）。--》缺少D选项

A、路由器产品支持URPF，可以过滤大多数虚假IP泛洪攻击

B、路由器产品支持CAR功能，可以有效限制泛洪攻击

C、路由器产品不支持ACL配置功能，不能定制过滤规则

D、

148、路由器对于接入权限控制，包括：（D）。

A、根据用户账号划分使用权限 B、根据用户接口划分使用权限

C、禁止使用匿名账号 D、以上都是

149、路由器启动时默认开启了一些服务，有些服务在当前局点里并没有作用，对于这些服务：（C）。缺少D选项

A、就让他开着，也耗费不了多少资源 B、就让他开着，不会有业务去访问

C、必须关闭，防止可能的安全隐患 D、

150、设置Cisco设备的管理员账号时，应（C）。

A、多人共用一个账号 B、多人共用多个账号

C、一人对应单独账号 D、一人对应多个账号

151、什么命令关闭路由器的finger服务？（C）

A、disable finger B、no finger C、no finger service D、no service finger

152、什么是IDS？（A）

A、入侵检测系统 B、入侵防御系统 C、网络审计系统 D、主机扫描系统

153、实现资源内的细粒度授权，边界权限定义为：（B）。

A、账户 B、角色 C、权限 D、操作

154、使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）

A、拒绝服务 B、文件共享 C、BIND漏洞 D、远程过程调用

155、使用TCP 79端口的服务是：（D）。

A、telnet B、SSH C、Web D、Finger

156、使用一对一或者多对多方式的NAT转换，当所有外部IP地址均被使用后，后续的内网用户如需上网，NAT转换设备会执行什么样的动作？（C）

A、挤掉前一个用户，强制进行NAT转换 B、直接进行路由转发

C、不做NAT转换 D、将报文转移到其他NAT转换设备进行地址转换

157、私网地址用于配置本地网络、下列地址中属于私网地址的是？（C）

A、100.0.0.0 B、172.15.0.0 C、192.168.0.0 D、244.0.0.0

158、随着Internet发展的势头和防火墙的更新，防火墙的哪些功能将被取代。（D）

A、使用IP加密技术 B、日志分析工作

C、攻击检测和报警 D、对访问行为实施静态、固定的控制

159、随着安全要求的提高、技术的演进，（D）应逐步实现物理隔离，或者通过采用相当于物理隔离的技术（如MPLSVPN）实现隔离。

A、局域网 B、广域网及局域网 C、终端 D、广域网

160、通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出现崩溃，请问这种攻击属于何种攻击？（D）

A、拒绝服务（DoS）攻击 B、扫描窥探攻击

C、系统漏洞攻击 D、畸形报文攻击

161、通信领域一般要求3面隔离，即转发面、控制面、用户面实现物理隔离，或者是逻辑隔离，主要目的是在某一面受到攻击的时候，不能影响其他面。路由器的安全架构在实现上就支持：（D）

A、转发面和控制面物理隔离 B、控制面和用户面逻辑隔离

C、转发面和用户面逻辑隔离 D、以上都支持

162、网管人员常用的各种网络工具包括telnet、ftp、ssh等，分别使用的TCP端口号是（B）。

A、21、22、23 B、23、21、22 C、23、22、21 D、21、23、22

163、网络安全工作的目标包括：（D）。

A、信息机密性 B、信息完整性 C、服务可用性 D、以上都是

164、网络安全在多网合一时代的脆弱性体现在（C）。

A、网络的脆弱性 B、软件的脆弱性 C、管理的脆弱性 D、应用的脆弱性

165、应限制Juniper路由器的SSH（A），以防护通过SSH端口的DoS攻击。

A、并发连接数和1分钟内的尝试连接数 B、并发连接数

C、1分钟内的尝试连接数 D、并发连接数和3分钟内的尝试连接数

166、应用网关防火墙的逻辑位置处在OSI中的哪一层？（C）

A、传输层 B、链路层 C、应用层 D、物理层

167、应用网关防火墙在物理形式上表现为？（B）

A、网关 B、堡垒主机 C、路由 D、交换机

168、用来追踪DDoS流量的命令式：（C）

A、ip source-route B、ip cef C、ip source-track D、ip finger

169、用于保护整个网络IPS系统通常不会部署在什么位置？（D）

A、网络边界 B、网络核心 C、边界防火墙内 D、业务终端上

170、用于实现交换机端口镜像的交换机功能是：（D）

A、PERMIT LIST B、PVLAN C、VTP D、SPAN

171、有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（D）。

A、L2TP是由PPTV协议和Cisco公司的L2F组合而成

B、L2TP可用于基于Internet的远程拨号访问

C、为PPP协议的客户建立拨号连接的VPN连接

D、L2TP只能通过TCP/IP连接

172、有关PPTP（Point-to-Point Tunnel Protocol）说法正确的是（C）。

A、PPTP是Netscape提出的 B、微软从NT3.5以后对PPTP开始支持

C、PPTP可用在微软的路由和远程访问服务上 D、它是传输层上的协议

173、有一些应用，如微软Out look或MSN。它们的外观会在转化为基于Web界面的过程中丢失，此时要用到以下哪项技术：（B）

A、Web代理 B、端口转发 C、文件共享 D、网络扩展

174、预防信息篡改的主要方法不包括以下哪一项？（A）

A、使用VPN技术 B、明文加密 C、数据摘要 D、数字签名

175、域名服务系统（DNS）的功能是（A）。

A、完成域名和IP地址之间的转换 B、完成域名和网卡地址之间的转换

C、完成主机名和IP地址之间的转换 D、完成域名和电子邮件地址之间的转换

176、源IP为100.1.1.1，目的IP为100.1.1.255，这个报文属于什么攻击？（B）（假设该网段掩码为255.255.255.0）

A、LAND攻击 B、SMURF攻击 C、FRAGGLE攻击 D、WINNUKE攻击

177、在AH安全协议隧道模式中，新IP头内哪个字段无需进行数据完整性校验？（A）

A、TTL B、源IP地址 C、目的IP地址 D、源IP地址+目的IP地址

178、在C/S环境中，以下哪个是建立一个完整TCP连接的正确顺序？（D）

A、SYN，SYN/ACK，ACK B、Passive Open,Active Open,ACK,ACK

C、SYN,ACK/SYN,ACK D、Active Open/Passive Open,ACK,ACK

179、在L2TP应用场景中，用户的私有地址分配是由以下哪个组建完成？（B）

A、LAC B、LNS C、VPN Client D、用户自行配置

180、在OSI模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（A）

A、应用层 B、物理层 C、会话层 D、网络层

181、在OSI参考模型中有7个层次，提供了相应的安全服务来加强信息系统的安全性。以下哪一层提供了抗抵赖性？（B）

A、表示层 B、应用层 C、传输层 D、数据链路层

182、在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（B）

A、产生日志的数量 B、攻击减少的速度

C、较低的价格 D、假阳性的减少量

183、在安全审计的风险评估阶段，通常是按什么顺序来进行的？（A）

A、侦查阶段、渗透阶段、控制阶段 B、渗透阶段、侦查阶段、控制阶段

C、控制阶段、侦查阶段、渗透阶段 D、侦查阶段、控制阶段、渗透阶段

184、在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（D）

A、IETF 因特网工程工作小组 B、ISO 国际标准组织

C、IANA 因特网地址指派机构 D、OSI 开放系统互联

185、在传输模式IPSec应用情况中，以下哪个区域数据报文可受到加密安全保护？（D）

A、整个数据报文 B、原IP头 C、新IP头 D、传输层及上层数据报文

186、在点到点链路中，OSPF的Hello包发往以下哪个地址？（B）

A、127.0.0.1 B、224.0.0.5 C、233.0.0.1 D、255.255.255.255

187、在建立堡垒主机时，（A）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

188、在进行Sniffer监听时，系统将本地网络接口卡设置成何种侦听模式？（D）

A、unicast单播模式 B、Broadcast广播模式

C、Multicast组播模式 D、Promiscuous混杂模式

189、在零传输（Zone transfers）中DNS服务使用哪个端口？（A）

A、TCP 53 B、UDP 53 C、UDP 23 D、TCP23

190、在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（C）

A、入网访问控制 B、权限控制 C、网络检测控制 D、防火墙控制

191、在思科设备上，若要查看所有访问表的内容，可以使用的命令式（B）

A、show all access-lists B、show access-lists

C、show ip interface D、show interface

192、在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的这是对（A）。

A、可用性的攻击 B、保密性的攻击 C、完整性的攻击 D、真实性的攻击

193、在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（C）

A、报文服务拒绝 B、假冒 C、数据流分析 D、报文服务更改

194、在以下OSI七层模型中，synflooding攻击发生在哪层？（C）

A、数据链路层 B、网络层 C、传输层 D、应用层

195、在以下哪类场景中，移动用户不需要安装额外功能（L2TP）的VPDN软件？（B）

A、基于用户发起的L2TP VPN B、基于NAS发起的L2TP VPN

C、基于LNS发起的L2TP VPN D、以上都是

196、账户口令管理中4A的认证管理的英文单词为：（B）

A、Account B、Authentication C、Authorization D、Audit

197、只具有（A）和FIN标志集的数据包是公认的恶意行为迹象。

A、SYN B、date C、head D、标志位

198、主从账户在4A系统的对应关系包含：（D）

A、1 -N B、1 -1 C、N -1 D、以上全是

199、主动方式FTP服务器要使用的端口包括（A）。

A、TCP 21 TCP 20 B、TCP21 TCP大于1024的端口

C、TCP 20、TCP 大于1024端口 D、都不对

200、下列（D）因素不是影响IP电话语音质量的技术因素。

A、时延 B、抖动 C、回波 D、GK性能

201、下列安全协议中使用包括过滤技术，适合用于可信的LAN到LAN之间的VPN（内部VPN）的是（D）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

202、下列不是抵御DDoS攻击的方法有（D）。

A、加强骨干网设备监控 B、关闭不必要的服务

C、限制同时打开的Syn半连接数目 D、延长Syn半连接的time out时间

203、下列措施不能增强DNS安全的是（C）。

A、使用最新的BIND工具 B、双反向查找

C、更改DNS的端口号 D、不要让HINFO记录被外界看到

204、下列各种安全协议中使用包过滤技术，适合用于可信的LAN到LAN之间的VPN，即内部网VPN的是（）。

A、PPTP B、L2TP C、SOCKS v5 D、IPSec

205、下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适？（D）

A、回应的比例 B、被动的防御 C、主动的防御 D、都不对

206、下列哪项是私有IP地址？（A）

A、10.5.42.5 B、172.76.42.5 C、172.90.42.5 D、241.16.42.5

207、下列哪一项能够提高网络的可用性？（B）

A、数据冗余 B、链路冗余 C、软件冗余 D、电源冗余

208、下列哪一种攻击方式不属于拒绝服务攻击：（A）。

A、LOphtCrack B、Synflood C、Smurf D、Ping of Death

209、下列哪一项是arp协议的基本功能？（A）

A、通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行

B、对局域网内的其他机器广播路由地址

C、过滤信息，将信息传递个数据链路层 D、将信息传递给网络层

210、最早的计算机网络与传统的通信网络最大的区别是什么？（A）

A、计算机网络采用了分组交换技术 B、计算机网络采用了电路交换技术

C、计算机网络的可靠性大大提高 D、计算机网络带宽和速度大大提高

211、以下哪个属于IPS的功能？（A）

A、检测网络攻击 B、网络流量检测 C、实时异常告警 D、以上都是

212、以下说法错误的是（C）。

A、安全是一个可用性与安全性之间的平衡过程 B、安全的三要素中包含完整性

C、可以做到绝对的安全 D、网络安全是信息安全的子集

213、以下属于4A策略管理模块可以管理的为（C）。

A、访问控制策略 B、信息加密策略 C、密码策略 D、防火墙策略

214、最早研究计算机网络的目的是什么？（B）

A、共享硬盘空间、打印机等设备 B、共享计算资源

C、直接的个人通信 D、大量的数据交换

215、防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为（C）。

A、内容过滤 B、地址转换 C、透明代理 D、内容中转

216、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）。

A、防火墙 B、CA中心 C、加密机 D、防病毒产品

217、网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（D）。

A、多重安全网关 B、防火墙 C、Vlan隔离 D、物理隔离

218、下列哪项不是Tacacs+协议的特性。（A）

A、扩展记账 B、加密整个数据包 C、使用TCP D、支持多协议

219、一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（A）

A、最小特权 B、阻塞点 C、失效保护状态 D、防御多样化

220、包过滤防火墙工作的好坏关键在于？（C）

A、防火墙的质量 B、防火墙的功能 C、防火墙的过滤规则设计 D、防火墙的日志

221、对于日常维护工作，连接路由器的协议通常使用：（B）。缺少D选项

A、TELNET，简单，容易配置 B、SSH &SSHv2 加密算法强劲，安全性好

C、TELNET配置16位长的密码，加密传输，十分安全 D、

222、BOTNET是（C）。

A、普通病毒 B、木马程序 C、僵尸网络 D、蠕虫病毒

223、监听的可能性比较低的是（B）数据链路。

A、Ethernet B、电话线 C、有线电视频道 D、无线电

224、当IPS遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（B）。

A、pass B、bypass C、watchdog D、HA

225、网络环境下的security是指（A）。

A、防黑客入侵，防病毒，窃取和敌对势力攻击

B、网络具有可靠性，可防病毒，窃密和敌对势力攻击

C、网络具有可靠性，容灾性，鲁棒性

D、网络的具有防止敌对势力攻击的能力

226、某一案例中，使用者已将无线AP的SSID广播设置为禁止，并修改了默认SSID值，但仍有未经授权的客户端接入该无线网络，这是因为（D）

A、禁止SSID广播仅在点对点的无线网络中有效

B、未经授权客户端使用了默认SSID接入

C、无线AP开启了DHCP服务

D、封装了SSID的数据包仍然会在无线AP与客户端之间传递

227、为了保护DNS的区域传送（zone transfer），应该配置防火墙以阻止（B）。

1.UDP

2.TCP

3.53

4.52

A、1,3 B、2,3 C、1,4 D、2,4

228、以下不属于代理服务技术优点的是（D）。

A、可以实现身份认证 B、内部地址的屏蔽盒转换功能

C、可以实现访问控制 D、可以防范数据驱动侵袭

229、应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（C）。

A、60% B、70% C、80% D、90%

230、TCP协议与UDP协议相比，TCP是（B），UDP是（）。

A、设置起来麻烦；很好设置 B、容易；困难

C、面向连接的；非连接的 D、不可靠的；可靠的

231、交换机转发以太网的数据基于：（B）。

A、交换机端口号 B、MAC地址 C、IP地址 D、数据类别

232、HTTP，FTP，SMTP建立在OSI模型的哪一层？（D）

A、2层-数据链路层 B、3层-网络层 C、4层-传输层 D、7层-应用层

233、网络安全的基本属性是（D）。

A、机密性 B、可用性 C、完整性 D、以上都是

234、网络安全的主要目的是保护一个组织的信息资产的（A）。

A、机密性、完整性、可用性 B、参照性、可用性、机密性、

C、可用性、完整性、参照性 D、完整性、机密性、参照性

235、DBS是采用了数据库技术的计算机系统。DBS是一个集合体，包含数据库、计算机硬件、软件和（C）。

A、系统分析员 B、程序员 C、数据库管理员 D、操作员

236、MySQL -h host -u user -p password命令的含义如下，哪些事正确的？（D）

A、-h后为host为对方主机名或IP地址 B、-u后为数据库用户名

C、-p后为密码 D、以上都对

237、Oracle当连接远程数据库或其它服务时，可以指定网络服务名，Oracle9i支持5中命名方法，请选择错误的选项。（D）

A、本地命名和目录命名 B、Oracle名称（Oracle Names）

C、主机命名和外部命名 D、DNS和内部命名

238、Oracle的数据库监听器（LISTENER）的默认通讯端口是？（A）

A、TCP 1521 B、TCP 1025 C、TCP 1251 D、TCP 1433

239、Oracle默认的用户名密码为（A）。

A、Scote/tiger B、root C、null D、rootroot

240、Oracle数据库中，物理磁盘资源包括哪些（D）。

A、控制文件 B、重做日志文件 C、数据文件 D、以上都是

241、Oracle中启用审计后，查看审计信息的语句是下面哪一个？（C）

A、select \* from SYS.AUDIT$ B、select \* from syslogins

C、select \* from SYS.AUD$ D、AUDIT SESSION

242、SMTP的端口？（A）

A、25 B、23 C、22 D、21

243、SQL Server的登录账户信息保存在哪个数据库中？（C）

A、model B、msdb C、master D、tempdb

244、SQL Sever的默认DBA账号是什么？（B）

A、administrator B、sa C、root D、SYSTEM

245、SQL Sever的默认通讯端口有哪些？（B）

A、TCP 1025 B、TCP 1433 C、UDP 1434 D、TCP 14333 E、TCP 445

246、SQL Sever中可以使用哪个存储过程调用操作系统命令，添加系统账号？（B）

A、xp\_dirtree B、xp\_cmdshell C、xp\_cmdshell D、xpdeletekey

247、SQL Sever中下面哪个存储过程可以执行系统命令？（C）

A、xp\_regread B、xp\_command C、xp\_cmdshell D、sp\_password

248、SQL的全局约束是指基于元祖的检查子句和（C）。

A、非空值约束 B、域约束子句 C、断言 D、外键子句

249、SQL数据库使用以下哪种组件来保存真实的数据？（C）

A、Schemas B、Subschemas C、Tables D、Views

250、SQL语句中，彻底删除一个表的命令是（B）。

A、delete B、drop C、clear D、remore

251、SQL语言可以（B）在宿主语言中使用，也可以独立地交互式使用。

A、-极速 B、-嵌入 C、-混合 D、-并行

252、SSL安全套接字协议所用的端口是（B）。

A、80 B、443 C、1433 D、3389

253、不属于数据库加密方式的是（D）。

A、库外加密 B、库内加密 C、硬件/软件加密 D、专用加密中间件

254、测试数据库一个月程序主要应对的风险是（B）。

A、非授权用户执行“ROLLBACK”命令 B、非授权用户执行“COMMIT”命令

C、非授权用户执行“ROLLRORWARD”命令 D、非授权用户修改数据库中的行

**255、查看Oracle 8i及更高版本数据库的版本信息的命令是（C）。----缺少CD选项**

**A、cd $Oracle\_HOME/orainst B、C-cd $Oracle\_HIME/orainst C、 D、**

256、从安全的角度来看，运行哪一项起到第一道防线的作用？（C）

A、远端服务器 B、WEB服务器 C、防火墙 D、使用安全shell程序

257、从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（B）。

A、每个分割区G有g=|G|记录，其中g=0或g>=n，且g为偶数，

B、记录必须成对地加入G或从G中删除

C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从m各分割区G1，G2，… …Gm中每一个分割区而来的，则统计信息g（G1VG2V… …VGm）是允许发布

D、记录必须不对地加入G或从G中删除

258、单个用户使用的数据库视图的描述为（A）。

A、外模式 B、概念模式 C、内模式 D、存储模式

259、对于IIS日志记录，推荐使用什么文件格式？（D）

A、Microsoft IIS日志文件格式 B、NCSA公用日志文件格式

C、ODBC日志记录格式 D、W3C扩展日志文件格式

**260、对于IIS日志文件的存放目录，下列哪项设置是最好的？（D）----缺少D选型**

**A、%WinDir%\System32\LogFiles B、C:\Inetpub\wwwroot\LogFiles**

**C、C:\LogFiles..)-F:\LogFiles D、**

261、对于IIS日志文件的访问权限，下列哪些设置是正确的？（D）

A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）

B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）

C、SYSTEM（完全控制）Administrator（完全控制）Inernet来宾账户（读取和运行） D、SYSTEM（完全控制）Administrator（完全控制）

262、对于数据库的描述一下哪项说法是正确的？（A）

A、数据和一系列规则的集合 B、一种存储数据的软件

C、一种存储数据的硬件 D、是存放人量数据的软件

263、攻击者可能利用不必要的extproc外部程序调用功能获取对系统的控制权，威胁系统安全。关闭Extproc功能需要修改TNSNAMES.ORA和LISTENER.ORA文件删除一下条目，其中有一个错误的请选择出来（A）。

A、sys\_ertproc B、icache\_extproc

C、PLSExtproc D、extproc

264、关系数据库中，实现实体之间的联系是通过表与表之间的（D）。

A、公共索引 B、公共存储

C、公共元组 D、公共属性

265、关系型数据库技术的特征由一下哪些元素确定的？（A）

A、行和列 B、节点和分支

C、Blocks和Arrows D、父类和子类

266、关于WEB应用软件系统安全，说法正确的是（D）？

A、Web应用软件的安全性仅仅与WEB应用软件本身的开发有关

B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C、黑客的攻击主要是利用黑客本身发现的新漏洞

D、以任何违反安全规定的方式使用系统都属于入侵

267、目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（D）？

A、数据库系统庞大会提供管理成本 B、数据库系统庞大会降低管理效率

C、数据的集中会降低风险的可控性 D、数据的集中会造成风险的集中

268、哪一个是PKI体系中用以对证书进行访问的协议（B）？

A、SSL B、LDAP C、CA D、IKE

269、如果一个SQL Server数据库维护人员，需要具有建立测试性的数据库的权限，那么应该指派给他哪个权限（A）？

A、Database Creators B、System Administrators

C、Server Administrators D、Security Adiministrators

270、如果以Apache 为WWW服务器，（C）是最重要的配置文件。

A、access.conf B、srm.cong C、httpd.conf D、mime.types

271、若有多个Oracle数据需要进行集中管理，那么对sysdba的管理最好选择哪种认证方式（B）？

A、系统认证 B、password文件认证方式 C、域认证方式 D、以上三种都可

272、数据库管理系统DBMS主要由哪两种部分组成？（A）

A、文件管理器和查询处理器 B、事务处理器和存储管理器

C、存储管理器和查询处理器 D、文件管理器和存储管理器

273、数据库系统与文件系统的最主要区别是（B）。

A、数据库系统复杂，而文件系统简单

B、文件系统不能解决数据冗余和数据独立性问题，而数据库系统可以解决

C、文件系统只能管理程序文件，而数据库系统能够管理各宗类型的文件

D、文件系统管理的数据量较少，而数据库系统可以管理庞大的数据量

274、为了防止电子邮件中的恶意代码，应该由（A）方式阅读电子邮件。

A、纯文本 B、网页 C、程序 D、会话

275、为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机（D）？

A、SMTP身份认证 B、逆向名字解析 C、黑名单过滤 D、内容过滤

276、为什么要对数据库进行“非规范化”处理（B）？

A、确保数据完整性 B、增加处理效率 C、防止数据重复 D、节省存储空间

277、下列不属于WEB安全性测试的范畴的是（A）？

A、数据库内容安全性 B、客户端内容安全性

C、服务器端内容安全性 D、日志功能

278、下列操作中，哪个不是SQL Server服务管理器功能（A）？

A、执行SQL查询命令 B、停止SQL Server 服务

C、暂停SQL Server服务 D、启动SQL Server服务

279、下列关于IIS的安全配置，哪些是不正确的（C）？

A、将网站内容移动到非系统驱动程序 B、重命名IUSR账户

C、禁用所有WEB服务扩展 D、创建应用程序池

280、下列哪些不是广泛使用http服务器？（D）

A、W3C B、Apache C、IIS D、IE

281、下列哪些属于WEB脚本程序编写不当造成的（C）？

A、IIS5.0 Webdav Ntdll.dll远程缓冲区一处漏洞

B、apache可以通过../../../../../../../etc/passwd方位系统文件

C、登陆页面可以用password=’a’or’a’=’a’绕过

D、数据库中的口令信息明文存放

282、下列哪种方法不能有效的防范SQL进入攻击（C）？

A、对来自客户端的输入进行完备的输入检查

B、把SQL语句替换为存储过程、预编译语句或者使用ADO命令对象

C、使用SiteKey技术

D、关掉数据库服务器或者不使用数据库

283、下列哪种工具不是WEB服务器漏洞扫描工具（B）？

A、Nikto B、Web Dumper C、paros Proxy D、Nessus

284、下列哪种攻击不是针对统计数据库的（D）？

A、小查询集合大查询集攻击 B、中值攻击 C、跟踪攻击 D、资源解析攻击

285、下列哪项中是数据库中涉及安全保密的主要问题（A）？

A、访问控制问题 B、数据的准确性问题

C、数据库的完整性问题 D、数据库的安全性问题

286、下列应用服务器中，不遵循J2EE规范的是（C）？

A、MTS B、WebLogic C、Oracle 9iApplication Server D、WebSpere

287、下面关于IIS报错信息含义的描述正确的是（B）？

A、401-找不到文件 B、403-禁止访问 C、404-权限问题 D、500-系统错误

288、下面关于Oracle进程的描述，哪项是错误的（B）？

A、运行在Windows平台上的Oracle能让每个用户组程序化地打开新的进程，这是一个安全隐患

B、在Windows平台，除了Oracle.exe进程外还有其他的独立进程

C、unix平台上有多个独立运行的进程，包括数据写进程、日志写进程、存档进程、系统监控进程、进程监控进程

D、有一个特殊的内存区域被映射为\*nix平台上的所有进程，此区域时系统全局去

289、下面哪一项是与数据库管理员（DBA）职责不相容的（C）？

A、数据管理 B、信息系统管理 C、系统安全 D、信息系统规划

290、下面选型中不属于数据库安全控制的有（D）。

A、信息流控制 B、推论控制 C、访问控制 D、隐通道控制

291、下面选型中不属于数据库安全模型的是（D）。

A、自主型安全模型 B、强制型安全模型 C、基于角色的模型 D、访问控制矩阵

292、一般来说，通过WEB运行http服务的子进程时，我们会选择（D）的用户权限方式，这样可以保证系统的安全。

A、root B、httpd C、guest D、nobody

293、一下不是数据库的加密技术的是（D）。

A、库外加密 B、库内加密 C、硬件加密 D、固件加密

294、一下对于Oracle文件系统描述错误的是（B）？

A、\*nix下Oracle的可执行文件在$Oracle\_HOME/bin/Oracle,$Oracle\_HOME/bin也应该包含在路径环境变量内

B、Windows下Oracle的可执行文件在%Oracle\_HOME%\bin\Oracle.exe,其他

C、硬件加密 D、固件加密

295、以下几种功能中，哪个是DBMS的控制功能（A）？

A、数据定义 B、数据恢复 C、数据修改 D、数据查询

296、以下哪个安全特征和机制是SQL数据库所特有的（B）？

A、标识和鉴别 B、数据恢复 C、数据修改 D、数据查询

297、以下哪个是数据库管理员（DBA）可以行使的职责（A）？

A、系统容量规划 B、交易管理 C、审计 D、故障承受机制

298、以下哪条命令能利用“SQL注入”漏洞动用XP\_cmdshell存储过程，获得某个子目的清单？（A）

A、http://localhost/script?’:EXEC+master..XP\_cmdshell+’dir’:--

B、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’:--

C、http://localhost/script?0’:EXEC+master..XP\_cmdshell+’ dir’:--

D、http://localhost/script?1’:EXEC+master..XP\_cmdshell+’ dir’--

299、以下哪条命令能利用“SQL”漏洞动用XP\_cmdshell存储过程，启动或停止某项服务？（B）

A、http://localhost/script?’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;-

B、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ;--

C、http://localhost/script?1’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ ; --

D、http://localhost/script?0’:EXEC+master..XP\_servicecontrol+’start’ ,+’Server’ --

300、以下哪项不属于访问控制策略的实施方式？（D）

A、子模式法 B、修改查询法 C、集合法 D、验证法

301、以下哪一项是和电子邮件系统无关的？（）

A、PEM(Privacy enhanced mail) B、PGP(Pretty good privacy)

C、X.500 D、X.400

302、以下哪种方法可以用于对付数据库的统计推论？（C）

A、信息流控制 B、共享资源矩阵 C、查询控制 D、间接存取

303、以下是对层次数据库结构的描述，请选择错误描述的选项。（C）

A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来

B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据

C、它的优点是用户不需要十分熟悉数据库结构

D、层次数据库模型的结构就像是一棵倒转的树

304、以下是对单用户数据库系统的描述，请选择错误描述的选项（C）。

A、单用户数据库系统是一种早期的最简单的数据库系统

B、在单用户系统中，整个数据库系统，包括应用程序、DBMS、数据，都装在一台计算机之间不能共享数据

C、在单用户系统中，由多个用户共用，不同计算机之间能共享数据

D、单用户数据库系统已经不适用于现在的使用，被逐步淘汰了

305、以下是对分布式结构数据库系统的描述，请选择错误描述的选项。（D）

A、分布式结构的数据库系统的数据在逻辑上是一个整体，但物理地分布在计算机网络的不同节点上，每个节点上的主机又带有多个终端用户

B、网络中的每个节点都可以独立的处理数据库中的数据，执行全局应用

C、分布式结构的数据库系统的数据分布存放给数据的处理、管理和维护带来困难

D、分布式结构的数据库系统的数据只在存放在服务器端，其他节点只进行处理和执行

306、以下是对关系数据库结构的描述，请选择错误描述的选项。（D）

A、数据存储的主要载体是表，或相关数据组

B、有一对一、一对多、多对多三种表关系

C、表关联是通过引用完整性定义的，这是通过主码和外码（主键或外键约束条件实现的）

D、缺点是不支持SQL语言

307、以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（A）

A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力

B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行DBMS功能又执行应用程序

C、在网络中把某些节点的计算机专门用于执行DBMS核心功能，这台计算机就成为数据库服务器

D、其他节点上的计算机安装DBMS外围应用开发工具和应用程序，支持用户的应用，称为客户机

308、以下是对面向对象数据库结构的描述，请选择错误描述的选项。（C）

A、它允许用对象的概念来定义与关系数据库交互

B、面向对象数据库中有两个基本的结构：对象和字面量

C、优点是程序员需要掌握与面向对象概念以及关系数据库有关的存储

D、缺点是用户必须理解面向对象概念，目前还没有统一的标准，稳定性还是一个值得关注的焦点

309、以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（D）

A、主从式结构是指一个主机带多个终端的多用户结构

B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上

C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源

D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈

311、在GRUB的配置文件grub.conf中，“timeout=-1”的含义是（C）。

A、不等待用户选择，直接启动默认的系统

B、在10秒钟内，等待用户选择要启动的系统

C、一直等待用户选择要启动的系统

D、无效

312、在Oracle中，quota可以限制用户在某个表空间上最多可使用多少字节，如果要限制data\_ts表500K，以下哪个是正确的命令？（B）

A、quo 500k in data\_ts B、quota 500K on data\_ts

C、quota data\_ts ,imit 500K D、quota data\_ts on 500K

313、在Oracle中，建表约束包括引用完整性约束、check完整性约束，还有以下三项是正确的，请排除一个错误选项。（D）

A、非空完整性约束 B、唯一完整性约束

C、主码完整性约束 D、数据角色性约束

314、在Oracle中，将scott的缺省表空间改为data2\_ts，下列哪个是正确的？（A）

A、ALTER USER scott DEFAULT TABLESPACE data2\_ts

B、ALTER DEFAULT TABLESPACE data2\_ts USER scott

C、ALTER USER scott TABLESPACE DEFAULT data2\_ts D、ALTER scott USER DEFAULT TABLESPACE data2\_ts

315、在Oracle中，将scott的资源文件改为otherprofile，下列哪个是正确的？（C）

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

316、在Oracle中，将当前系统所有角色都授予scott，除Payroll外，下列哪个是正确的？（D）

A、ALTER DEFAULT ROLLE USER　　scott ALL EXCEPT Payroll

B、ALTER USER DEFAULT ROLLE ALL EXCEPT Payroll

C、ALTER DEFAULT ROLLE ALL EXCEPT USER scott

D、ALTER USER scott DEFAULT ROLLE ALL EXCEPT Payroll

317、在Oracle中，用ALTER将scott的口令改为hello，下列哪个是正确的？（A）

A、ALTER USER scott IDENTIFIED BY hello

B、ALTER scott USER IDENTIFIED BY hello

C、ALTER USER scott IDENTIFIED AS hello

D、ALTER USER hello IDENTIFIED BY scott

318、在WEB应用软件的基本结构中，客户端的基础是（A）。

A、HTML文档 B、客户端程序

C、HTML协议 D、浏览器

319、在WEB应用软件的系统测试技术中，下面不属于安全性测试内容的是（C）。

A、客户端的内容安全性 B、服务器的内容安全性

C、数据库的内容安全性 D、Cookie安全性

320、在典型的WEB应用站点的层次结构中，“中间件”是在哪里运行的？（C）

A、浏览器客户端 B、web服务器

C、应用服务器 D、数据库服务器

321、在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（C）

A、对话管理服务 B、事务管理服务

C、资源管理服务 D、控制管理服务

322、主要用于加密机制的协议时（D）。

A、HTTP B、FTP C、TELNETD D、SSL

323、分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？（D）

A、自主性 B、可靠性 C、灵活性 D、数据备份

324、下面对Oracle的密码规则描述，哪个是错误的？（D）

A、Oracle密码必须由英文字母，数值，#，下划线(\_)，美元字符（$）构成，密码的最大长度为30字符，并不能以“$”，“#”，“\_”或任何数字卡头；密码不能包含像“SELECT”，“DELETE”，“CREATE”这类的ORACLE/SQL关键字

B、Oracle的若算法加密机制（）两个相同的用户名和密码在两台不同的ORACLE数据库机器中，将具有相同的哈希值。这些哈希值存储在SYS.USER表中，可以通过像DBA\_USE这类的试图来访问

C、Oracle默认配置下，每个中户如果有10此的失败登录，此账户将会被锁定

D、SYS账户在Oracle数据库中有最高权限，能够做任何事情，包括启动/关闭Oracle数据库，如果SYS被锁定，将不能访问数据库

325、无论是哪一种Web服务器，都会受到HTTP协议本身安全问题的困扰，这样的信息系统安全漏洞属于（C）。

A、设计型漏洞 B、开发型漏洞 C、运行型漏洞 D、以上都不是

326、SSL加密的过程包括以下步骤：（1）通过验证以后，所有数据通过密钥进行加密，使用DEC和RC4加密进行加密；（2）随后客户端随机生成一个对称密钥；（3）信息通过HASH加密，或者一次性加密（MD5SHA）进行完整性确认；（4）客户端和服务器协商建立加密通道的特定算法。正确的顺序的是（D）

A、（4）（3）（1）（2） B、（4）（1）（3）（2） C、（4）（2）（3）（1） D、（4）（2）（3）（1）

327、影响WEB系统安全的因素，不包括？（C）

A、复杂应用系统代码量大、开发人员多、难免出现疏忽

B、系统屡次升级、人员频繁变更，导致代码不一致

C、历史遗留系统、试运行系统等对个WEB系统运行于不同的服务器上

D、开发人员未经安全编码培训

328、Oracle通过修改用户密码策略可提高密码强度，以下哪个密码策略参数中文描述是错误的？（A）

A、PASSWORD\_MAX 登录超过有效次数锁定时间

B、FAILED\_LOGIN\_ATTEMPTS 最大错误登录次数

C、PASSWORD\_GRACE\_TIME 密码失效后锁定时间

D、PASSWORD\_LIFE\_TIME 口令有效时间

329、SQL Server服务有一个启动账号，默认账号是属于administrators组，现在为了安全需要创建一个新的服务启动账号，它需要哪些权限既能兼顾安全又能保证启动数据库成功，请排除一个错误的。（D）

A、数据库本地目录的读写权限 B、启动本地服务的权限

C、读取注册表的权限 D、通过API访问Windows Resource

330、作为一台运行IIS 在Internet发布站点的Windows Web服务器，下面哪项服务不是必需的？（B）

A、IIS Admin B、Net Logon

C、Performance Logs and Alerts D、World Wide Web Publishing

331、数据库中超级账户不能被锁定，其中Oracle的是（），mysql的是（），SQLServer的是（C）。

A、sa，root，sys B、admin，root，sa

C、sys，root，sa D、sys，admin，sa

332，Oracle的安全机制，是由（A）、实体权限和角色权限这三级体系结构组成的。

A、系统权限 B、索引权限 C、操作权限 D、命令控制

333、对SQL数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（B）

A、-- B、- C、-= D、-+

334、在Web页面中增加验证码功能后，下面说法正确的是（A）。

A、可以增加账号破解等自动化软件的攻击难度 B、可以防止文件包含漏洞 C、可以防止缓冲溢出 D、可以防止 浏览

335、以下破解Oracle密码哈希值的步棸，其中哪个描述是错误的？（B）

A、用Sqlplus直接登录到Oracle数据库，使用select username，password form dba\_users命令查看数据库中的用户名和密码，此时看到的密码是哈希值

B、在Cain的Cracker菜单点击导入用户名和哈希值，可直接显示用户密码明文

C、在Cain的Cracker菜单点解导入用户名和哈希值，只能通过字典破解 D、在Cain的Rainbow生成的表会占用大量的硬盘空间和内存，可是破解速度和效率很高

336、在数据库向因特网开放前，哪个步棸是可以忽略的？（B）

A、安全安装和配置操作系统和数据库系统

B、应用系统应该在内网试运行3个月

C、对应用软件如Web也没、ASP脚本等进行安全性检查

D、网络安全策略已经生效

337、如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf文件，查看是否包含如下设置，选出一个正确的（D）。

A、audit=filename B、sys=filename C、event=filename D、log=filename

338、针对一台对外提供Web服务的Windows服务器，下列关于账户权限控制，哪些项是不合理的？（C）

A、限制匿名账户对Web内容的目录写权限

B、从Everyone组中删除“从网络访问此计算机” 用户权限

C、禁用IUSR-MACHE和IWAN\_MACHINE账户

D、本地登录时必须使用Administrators账户

339、网上营业中间件如果启用了SSl，应采用不低于（C）版本的SSL，采用经国家密码管理局认可的密码算法。

A、2.0 B、2.5 C、3.0 D、3.1

340、SQL Server默认的具有DBA权限的账号是什么？（C）

A、root B、admin C、sa D、system

341、（A）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

342、（C）是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。

A、电磁兼容性 B、传导干扰 C、电磁干扰 D、辐射干扰

343、《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（B）。

A、GA 163-1997 B、GA 267-2000

C、GA 243-2000 D、GB 17859-1999

344、安装了合格防雷保安器的计算机信息系统，还必须在（C）雷雨季节前对防雷保安器、保护接地装置进行一次年度检查，发现不合格时，应及时修复或更换。

A、第三年 B、第二年 C、每年 D、当年

345、使用IIalon灭火的工作原理是什么？（C）

A、降低温度 B、隔绝氧气和可燃物

C、破坏氧气和可燃物之间的化学反应 D、减少氧气

346、白炽灯、高压汞灯与可燃物、可燃结构之间的距离不应小于（C）cm。

A、30 B、40 C、50 D、60

347、被电击的人能否获救，关键在于（D）。

A、触电的方式 B、人体电阻的大小

C、触电电压的高底 D、能否尽快脱离电源和施行紧急救护

348、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）。

A、可以随意弯折 B、转弯是，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

349、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

350、长期在高频电磁场作用下，操作者会有什么不良反应？（B）

A、呼吸困难 B、神经失常 C、疲劳无力

351、触电事故中，绝大部分是由于（A）导致人身伤亡的。

A、人体接受电流遭到电击 B、烧伤 C、触电休克

352、从业人员发现直接危及人身安全的紧急情况时，例如气体灭火系统开始开启时，应（A）。

A、停止作业，立即撤离危险现场 B、继续作业

C、向上级汇报，等待上级指令

353、从业人员既是安全生产的保护对象，又是实现安全生产的（C）。

A、关键 B、保证 C、基本要素

354、低压验电笔一般适用于交、直流电压未（C）伏以下。

A、220 B、380 C、500

355、电流为（B）毫安是，称为致命电流。

A、50 B、100 C、120 D、150

356、电器的保险丝只能装在（B）上。

A、零线 B、火线 C、底线

357、电器着火是不能用（C）灭火。

A、四氧化碳或1211灭火 B、沙土 C、水

358、对不符合防雷标准、规范防雷工程专业设计方案，以下（B）应当按照审核结论进行修改并重新报批。

A、建设单位 B、防雷工程专业设计单位 C、工程施工单位

359、发现人员触电时，应（B），使之脱离电源。

A、立即用手拉开触电人员 B、用绝缘物体拨开电源或触电者 C、用铁棍拨开电源线

360、凡设在年平均雷电日大于（C）的地区的计算机信息系统，原则上均应装设计算机信息系统防雷保安器，以防止雷电电磁脉冲过电压和过电流侵入计算机信息系统设备。

A、40 B、45 C、5 D、15

361、废电池随处丢弃会造成（B）的污染。

A、白色污染 B、重金属污染 C、酸雨

362、干粉灭火器多长时间检查一次？（A）

A、半年 B、一年 C、三个月 D、两年

363、根据国家相关规定，电压（D）以下不必考虑防止电击的安全？

A、48伏 B、36伏 C、65伏 D、25伏

364、根据作业环境的不同，安全帽的颜色也不同，如在爆炸性作业场所工作宜戴（A）安全帽。

A、红色 B、黄色 C、白色

365、关于空气的正向压力，下面哪项描述是正确的？（B）

A、当门打开时，空气向内流动 B、当门打开，空气向外流动

C、当发生火灾，系统自动切断电源 D、当发生火灾，烟雾向另外一间房间流动

366、国家颁布的《安全色》标准中，表示警告、主要的颜色为（C）。

A、红色 B、蓝色 C、黄色

367、火灾中对人员威胁最大的是（B）。

A、火 B、烟气 C、可燃物

368、机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（B）m。

A、0.1 B、0.6 C、1.2 D、0.3

369、计算机电源系统的所有节点均应镀铅锡处理（B）连接。

A、热压 B、冷压 C、焊锡 D、直接

370、计算机系统接地应采用（A）。

A、专用底线 B、和大楼的钢筋专用网相连

C、大楼的各种金属管道相连 D、没必要

371、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法 B、隔离灭火法 C、冷却灭火法

372、计算机系统应选用（A）电缆。

A、铜芯 B、铅芯

C、铁芯 D、没有要求

373、进行腐蚀品的装卸作业应戴（B）手套。

A、帆布 B、橡胶 C、棉布

374、人体在电磁场作用下，由于（C）将使人体受到不同程度的伤害。

A、电流 B、电压 C、棉布

375、身上着火后，下列哪种灭火方法是错误的（C）。

A、就地打滚 B、用厚重衣物覆盖压灭火苗 C、迎风快跑

376、生产经营单位必须为从业人员提供符合国家标准或（C）标准的劳动防护用品。

A、当地 B、本单位 C、行业

377、使用新设备，必须了解、掌握其安全技术特征，采取有效的安全防护措施，并对从业人员进行专门的安全生产。（B）

A、当地 B、本单位 C、行业

378.实验地点相对湿度大于75%时，则此实验环境属于易触电的环境：（A）

A、危险 B、特别危险 C、一般

379、通过人身的安全交流电流规定在(A)以下。

A、10mA B、30mA C、50mA

380、下列不属于对物理层信息窃取的是(D)

A、对存储介质的盗取 B、对监视器的窃听

C、对网络线路的窃听 D、对设备屏蔽电磁干扰

381、新、改、扩建项目的安全设施投资应当纳入(C)。

A、企业成本 B、安措经费 C、建设项目概算

382、液体表面的蒸汽与空气形成可燃气体，遇到点火源时，发生一闪即灭的现象称为(C)

A、爆炸 B、蒸发 C、闪燃

383、防雷保安器：防止(B)破坏计算机信息系统的保安装置，可分为两大类：电源

线防雷保安器（简称电源防雷保安器）和信号传输线防雷保安器（简称通道防雷保安器）。

A、直击雷 B、感应雷 C、雷暴 D、雷电电磁脉冲

384、EMC标准是为了保证(D)正常工作而制走的。

A、网络 B、媒体 C、信息 D、系统和设备

385、以下不符合防静电要求的是(B)。

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

386、以下哪些属于系统的物理故障？(A)

A、硬件故障与软件故障 B、计算机病毒

C、人为的失误 D、网络故障和设备环境故障

387、用灭火器灭火时，灭火器的喷射口应该对准火焰的(C)。

A、上部 B、中部 C、根部

388、运输、携带、邮寄计算机信息媒体进出靖的，应当如实向(A)申报。

A、海关 B、工商

C、税务 D、边防

389、在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ (B)

A、产生静电 B、计算机部件腐蚀

C、有污染物 D、B+A

390、在空气不流通的狭小地方使用二氧化碳灭火器可能造成的危险是(B)。

A中毒 B缺氧 C爆炸

391、在雷雨天不要走近高压电杆、铁塔、避雷针、远离至少(C)米以外。

A、IO米 B、15米 C、20米

392、在易燃易爆场所穿(C)最危险。

A、布鞋 B、胶鞋 C、带钉鞋

393、在遇到高压电线断落地面时，导线断落点(B)m内，禁止人员进入。

A、IO B、20 C、30

394、数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？(C)

A、30%-40% B、40%-50% C、45%-60% D、50%-70%

395、计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所

以防雷保安器必须有合理的(B)。

A、屏蔽配置 B、接地配置

C、分流配置 D、均压配置

396、计算站场地宜采用(A)蓄电池。

A、封闭式 B、半封闭式

C、开启式 D、普通任意的

397、多层的楼房中，最适合做数据中心的位置是(D)。

A、楼 B、地下室

C、顶楼 D、除以上外的任何楼层

398、计算机机房是安装计算机信息系统主体的关键场所，是(A)工作的重点，所以

对计算机机房要加强安全管理。

A、实体安全保护 B、人员管理

C、媒体安全保护 D、设备安全保护

399、区域安全，首先应考虑（B），用来识别来访问的用户的身份，并对其合法性进行验证，主要通过特殊标示符、口令、指纹等来实现。

A、来访者所持物 B、物理访问控制 C、来访者所具有的特征 D、来访者所知信息

400、在计算机房出入口处或值班室，应设置（D）和应急断电装置。

A、 电视 B、电扇 C、报警器 D、应急电话

401、下列（A）灭火器是扑救精密仪器火灾的最佳选择。

A、二氧化碳灭火剂 B、干粉灭火剂 C、泡沫灭火剂

402、电气安全主要包括人身安全、（B）安全。

A、照明 B、设备 C、电器 D、空调

403、（C）基于IDEA算法。

A、S/MIME B、SET C、PGP D、SSL

404、(C）类型的加密，使得不同的文档和信息进行运算以后得到一个唯一的128位编码。

A、对称加密 B、非对称加密 C、哈希加密 D、强壮加密

405、(C)是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

406、(D)是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。

A、认证机构 B、密码 C、票据 D、数字证书

407、（D）协议主要用于加密机制。

A、HTTP B、FTP C、TELNET D、SSL

408、（A）原则保证只有发送方与接收方能访问消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

409、（D）原则允许某些用户进行特定访问。

A、保密性 B、鉴别 C、完整性 D、访问控制

410、（B）增加明文冗余度。

A、混淆 B、扩散 C、混淆与扩散 D、都不是

411、3DES加密算法的密钥长度是：（A）。

A、168 B、128 C、56 D、256

412、AES密钥长度不能是（D）。

A、128位 B、192位 C、256位 D、512位

413、AES算法是哪种算法？（A）。

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

414、AES属于哪种加密方式？（B）。

A、流加密 B、分组加密 C、异或加密 D、认证加密

415、CA指的是（A）。

A、证书授权 B、加密认证 C、虚拟专用网 D、安全套接层

416、DES经过（A）轮运算后，左右两部分合在一起经过一个末置换，输出一个64位的密文。（A）

A、16 B、8 C、32 D、4

417、DES算法是哪种算法？（A）

A、对称密钥加密 B、非对称密钥加密 C、哈希算法 D、流加密

418、DES属于哪种加密方式？（B）

A、流加密 B、块加密 C、异或加密 D、认证加密

419、DNSSec中并未采用（C）。

A、数字签名技术 B、公钥加密技术 C、地址绑定技术 D、报文摘要技术

420、ECB指的是（D）。

A、密文链接模式 B、密文反馈模式 C、输出反馈模式 D、电码本模式

421、EC-DSA复杂性的程度是（D）。

A、简单 B、最简单 C、困难 D、最困难

422、EFS可以用在什么文件系统下（C）。

A、FAT16 B、FAT32 C、NTFS D、以上都可以

423、IDEA的密钥长度是多少bit？（D）。

A、56 B、64 C、96 D、128

424、Kerberos是80年代中期，麻省理工学院为Athena项目开发的一个认证服务系统，其目标是把认证、记账和（B）的功能扩展到网络环境。

A、访问控制 B、审计 C、授权 D、监控

425、Kerberos是为TCP/IP网络设计的基于（B）的可信第三方鉴别协议，负责在网络上进行仲裁及会话密钥的分配。

A、非对称密钥体系 B、对称密钥体系 C、公钥体系 D、私钥体系

426、Kerberos是一种网络认证协议。它采用的加密算法是（C）。

A、RSA B、PGP C、DES D、MD5

427、Kerberos算法是一个（B）。

A、面向访问的保护系统 B、面向票据的保护系统

C、面向列表的保护系统 D、面向门与锁的保护系统

428、Kerberos提供的最重要的安全服务是？（A）。

A、鉴别 B、机密性 C、完整性 D、可用性

429、MD5产生的散列值是多少位？（C）。

A、56 B、64 C、128 D、160

430、MD5是按每组512位为一组来处理输入的信息，经过一系列变换后，生成一个（B）为散列值。

A、64 B、128 C、256 D、512

431、MD5是以512位分组来处理输入的信息，每一分组又被划分为（A）32位子分组。

A、16个 B、32个 C、64个 D、128个

432、MD5算法将输入信息M按顺序每组（D）长度分组，即：M1，M2，...，Mn-1，Mn。

A、64位 B、128位 C、256位 D、512位

433、PKI（公共密钥基础结构）中应用的加密方式为（B）。

A、对称加密 B、非对称加密 C、HASH加密 D、单向加密

434、PKI的全称是（D）。

A、Private Key Intrusion B、Public Key Intrusion

C、Private Key Infrastructure D、Public Key Infrastructure

435、PKI无法实现（D）。

A、身份认证 B、数据的完整性 C、数据的机密性 D、权限分配

436、RC4是由RIVEST在1987年开发的一种流式的密文，就是实时地把信息加密成一个整体，它在美国一般密钥长度是128位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）。

A、64位 B、56位 C、40位 D、32位

437、RSA公钥加密系统中，他想给她发送一份邮件，并让她知道是他发出，应选用的加密秘钥是（C）。

A、他的公钥 B、她的公钥 C、他的私钥 D、她的私钥

438、RSA使用不方便的最大问题是（A）。

A、产生密钥需要强大的计算能力 B、算法中需要大数

C、算法中需要素数 D、被攻击过很多次

439、RSA算法建立的理论基础是（C）。

A、DES B、替代想组合 C、大数分解和素数检测 D、哈希函数

440、SHA-1产生的散列值是多少位？（D）。

A、56 B、64 C、128 D、160

441、按密钥的使用个数，密码系统可以分为（C）。

A、置换密码系统和易位密码系统 B、分组密码系统和序列密码系统

C、对称密码系统和非对称密码系统 D、密码系统和密码分析系统

442、充分发挥了DES和RSA两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是：（C）。

A、数字签名 B、数字指纹 C、数字信封 D、数字时间戳

443、从技术角度上看数据安全的技术特征主要包含哪几个方面？（B）。

A、数据完整性、数据的方便性、数据的可用性 B、数据的完整性、数据的保密性、数据的可用性 C、数据的稳定性、数据的保密性、数据的可用性 D、数据的方便性、数据的稳定性、数据的完整性

444、单项散列函数的安全性来自于他的（A）。

A、单向性 B、算法复杂性 C、算法的保密性 D、离散性

445、电路网关防火墙工作在OSI协议的哪一层？（A）。

A、传输层 B、链路层 C、应用层 D、物理层

446、电子邮件的机密性与真实性是通过下列哪一项实现的？（A）

A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密

B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密

C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密

D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

447、端对端加密只需要保证消息都在哪里进行加密？（A）

A、源点和目的地节点 B、经过的每一个节点

C、源点和中间经过的每一个节点 D、所有节点

448、对明文字母重新排列，并不隐藏他们的加密方法属于（C）。

A、置换密码 B、分组密码 C、易位密码 D、序列密码

449、对网络中两个相邻节点之间传输的数据进行加密保护的是（A）。

A、节点加密 B、链路加密 C、端到端加密 D、DES加密

450、发送消息和用发送方私钥加密哈希加密信息将确保消息的：（A）。

A、真实性和完整性 B、真实性和隐私 C、隐私和不可否认性 D。隐私和不可否性

451、高级加密标准AES算法中，加密回合数不可能是（D）。

A、10 B、12 C、14 D、16

452、公钥机制利用一对互相匹配的（B）进行加密，解密。

A、私钥 B、密钥 C、数字签名 D、数字证书

453、公钥加密体制中，没有公开的是（A）。

A、明文 B、密文 C、公钥 D、算法

454、公钥证书提供了一种系统的、可扩展的、统一的（A）。

A、公钥分发方案 B、实现不可否认方案

C、对称密钥分发方案 D、保证数据完整性方案

455、关于CA和数字证书的关系，以下说法不正确的是（B）。

A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由CA签发

B、数字证书一般依靠CA中心的对称密钥机制来实现

C、在电子交易中，数字证书可以用于表明参与方的身份

D、数字证书能以一种不能被假冒的方式证明证书持有人身份

456、关于数字签名说法正确的是（A）。

A、数字签名的加密方法以目前的计算机的运算能力来破解是不现实的

B、采用数字签名，不能够保证信息自签发后到收到为止没有做过任何修改（能保证信息收到后没做个任何修改）

C、采用数字签名，能够保证信息是有签名者自己签名发送的，但由于不是真实的签名，签名者容易否认（签名不容易否认）

D、用户可以采用公钥对信息加以处理，形成数字签名（需使用私钥对信息加以处理）

457、基于私有密钥体制的信息认证方法采用的算法是（D）。

A、素数检测 B、非对称算法 C、RSA算法 D、对称加密算法

458、加密技术不能实现（D）。

A、数据信息的完整性 B、基于密码技术的身份认证 C、机密文件加密 D基于IP头信息的包过滤

459、加密技术不能提供以下哪种安全服务？（D）。

A、鉴别 B、机密性 C、完整性 D可用性

460、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）。

A、对称密钥加密 B、非对称密钥加密 C、 D

461、假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（A）。

A、对称加密技术 B、分组加密技术 C、公钥加密技术 D、单项函数密码技术

462、就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。（C）

A、公开密钥体制 B、对称加密体制 C、PKI（公开密钥基础设施） D、数字签名

463、利用非对称密钥体制实现加密通信时，若A要向B发送加密信息，则该加密信息应该使用（B）。

A、A的公钥加密 B、B的公钥加密 C、A的私钥加密 D、B的私钥加密

464、利用物理设备将各类型的无法预测的输入集中起来生成随机数的设备是（A）。

A、随机数生成器 B、伪随机数生成器 C、中央处理 D、非易失存储

465、链路加密要求必须先对链路两端的加密设备进行（C）。

A、异步 B、重传 C、同步 D、备份

466、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？（C）

A、对称的公钥算法 B、非对称私钥算法 C、对称密钥算法 D、非对称密钥算法

467、密码分析的目的是什么？（A）

A、确定加密算法的强度 B、增加加密算法的代替功能

C、减少加密算法的换为功能 D、确定所使用的换位

468、请从下列各项中选出不是HASH函数算法的一项。（D）

A、MD5 B、SHA C、HMAC D、MMAC

469、如今，DES加密算法面临的问题是（A）。

A、密钥太短，已经能被现代计算机暴力破解 B、加密算法有漏洞，在数学上已被破解 C、留有后门，可能泄露部分信息 D、算法过于陈旧，已经有更好的替代方案

470、若单项散列函数的输入串有很小的变化，则输出串（A）。

A、可能有很大的变化 B、一定有很大的变化 C、可能有很小的变化 D、一定有很小的变化

471、散列算法可以做哪些事？（C）。

A、碰撞约束 B、入侵检测 C、组合散列 D、随机数生成器

472、身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（B）。

A、可信性 B、访问控制 C、完整性 D、保密性

473、数字签名常用的算法有（B）。

A、DES算法 B、RSA算法 C、Hash函数 D、AES算法

474、数字签名和随机数挑战不能防范以下哪种攻击或恶意行为？（D）。

A、伪装欺骗 B、重放攻击 C、抵赖 D、DOS攻击

475、数字签名可以解决（D）。

A、数据被泄露 B、数据被篡改 C、未经授权擅自访问 D、冒名发送数据或发送后抵赖

476、数字签名通常使用（B）方式。

A、公钥密码体系中的私钥 B、公钥密码系统中的私钥对数字摘要进行加密

C、密钥密码体系 D、公钥密码体系中公钥对数字摘要进行加密

477、数字信封是用来解决（C）。

A、公钥分发问题 B、私钥分发问题 C、对称密钥分发问题 D、数据完整性问题

478、数字证书不包括（B）。

A、签名算法 B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号 D、颁发数字证书单位的数字签名

479、数字证书的应用阶段不包括（D）。

A、证书检索 B、证书验证 C、密钥恢复 D、证书撤销

480、下列说法中错误的是（D）。

A、非对称算法也叫公开密钥算法 B、非对称算法的加密密钥和解密密钥是分离的 C、非对称算法不需要对密钥通信进行保密 D、非对称算法典型的有RSA算法、AES算法等

481、下列算法中，哪种不是对称加密算法？（C）

A、AES B、DES C、RSA D、RC5

482、下列算法中属于Hash算法的是（C）。

A、DES B、IDEA C、SHA D、RSA

483、以下对于链路加密哪项是正确的？（B）

A、消息只在源点加密，目的节点解密 B、消息在源点加密，在每一个经过的节点解密并加密 C、消息在所有经过的节点中都是加密的，但只在目的节点解密 D、消息以明文形式在节点之间传输

484、以下各种加密算法中属于单钥制加密算法的是（A）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密算法

485、以下各种加密算法中属于双钥制加密算法的是（D）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密486、以下各种算法中属于古典加密算法的是（B）。

A、DES加密算法 B、Caesar替代法 C、Vigenere算法 D、Diffie-Hellman加密487、以下关于CA认证中心说法正确的是（C）。

A、CA认证时使用对称密钥机制的认证方法 B、CA认证中心支负责签名，不负责证书的产生 C、CA认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份 D、CA认证中心不用保持中立，可以随便找一个用户来作为CA认证中心

488、以下关于VPN说法正确的是（B）。

A、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B、VPN指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接

C、VPN不能做到信息认证和身份认证 D、VPN只能提供身份认证、不能提供加密数据的功能

489、以下关于数字签名说法正确的是（D）。

A、数字签名是在所传输的数据后附上一段和传输数据毫无关系的数字信息

B、数字签名能够解决数据的加密传输，即安全传输问题

C、数字签名一般采用对称加密机制 D、数字签名能够解决篡改、伪造等安全性问题

490、以下密码使用方法中正确的是（D）。

A、将密码记录在日记本上以避免忘记 B、任何情况下均不得使用临时性密码

C、密码中的字母不得重复 D、不要使用全部由字母组成的密码

491、以下哪个不包含在证书中？（C）

A、密钥采取的算法 B、公钥及其参数 C、私钥及其参数 D、签发证书的CA名称

492、以下哪个选项不会破坏数据库的完整性？（A）

A、对数据库中的数据执行删除操作 B、用户操作过程中出错

C、操作系统的应用程序错误 D、DBMS或操作系统程序出错

493、以下哪项不属于数据库系统实体安全？（B）

A、环境安全 B、线路安全 C、设备安全 D、媒体安全

494、以下哪一种算法产生最长的密钥？（D）

A、Diffe-Hellman B、DES C、IDEA D、RSA

495、以下认证方式中，最为安全的是（D）。

A、用户名+密码 B、卡+密码 C、用户名+密码+验证码 D、卡+指纹

496、远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（B）

A、知道什么 B、拥有什么 C、是谁 D、双因素认证

497、在3DES算法中，密钥最高可达到多少位？（C）

A、96 B、128 C、168 D、200

498、在IPSec中，（C）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的IPSec协议、密码算法、密钥等信息。

A、ESP B、SPI C、SA D、SP

499、在IPSec中，IKE提供（B）方法供两台计算机建立。

A、解释域 B、安全关联 C、安全关系 D、选择关系

500、在RIP的MD5认证报文中，经过加密的密钥是放在哪里的？（B）

A、保温的第一个表项里 B、报文的最后一个表项里

C、报文的第二个表项里 D、报文头里

501、在非对称加密算法中，涉及到的密钥个数是？（B）

A、一个 B、两个 C、三个 D、三个以上

502、在高级加密标准AES算法中，区块大小为（A）。

A、128位 B、192位 C、256位 D、512位

503、在给定的密钥体制中，密钥与密码算法可以看成是（A）。

A、前者是可变的，后者是固定的 B、前者是固定的，后者是可变的

C、两者都是可变的 D、两者都是固定的

504、在公钥体制中，不公开的是（B）。

A、公钥 B、私钥 C、公钥和私钥 D、私钥和加密算法

505、在密码学中，需要被交换的原消息被称为什么？（D）

A、密文 B、算法 C、密码 D、明文

506、一般证书采用哪个标准？（D）

A、ISO/IEC 15408 B、ISO/IEC 17799 C、BS 7799 D、X. 509V3

507、一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（D）

A、信息的数据和时间戳 B、识别发信的计算机

C、对信息内容进行加密 D、对发送者的身份进行识别

508、在数据库中，下列哪些数据不能加密？（A）

A、索引字段 B、存放日期字段

C、存放密码的 D、存放名称字段

509、在一个网络节点中，链路加密仅在以下哪项中提供安全性？（D）

A、数据链路层 B、物理层

C、通信层 D、通信链路

510、在以下隧道协议中，属于三层隧道协议的是（D）。

A、L2F B、PPTP C、L2TP D、IPSec

511、以下哪一项是基于一个大的整数很难分解成两个素数因数？（B）

A、ECC B、RSA C、DES D、D-H

512、以下哪种数据加密技术可以在基础架构层面进行？（A）

A、IPSec B、Secure Sockets Layer

C、Transport Layer Securit D、RSA

513、目前最安全的身份认证机制是（A）。

A、一次口令机制 B、双因素法

C、基于智能卡的用户身价认证 D、身价认证的单因素法

514、当数据库由于各种原因而使其完整性遭到破坏时，必须采取以下哪项措施来恢复数据库？（C）

A、重新安装数据库 B、换一种数据库

C、使用数据库备份 D、将数据库中的数据利用工具导出，并保存

515、PGP加密算法是混合使用（B）算法和IDEA算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES B、RSA C、IDEA D、AES

516、以下哪些软件是用于加密的软件？（A）

A、PGP B、SHA C、EFS D、DES

517、如果消息接受方要确定发送方身价，则要使用（B）原则。

A、保密性 B、鉴别 C、完整性 D、访问控制

518、对于现代密码破解，（D）是最常的方法。

A、攻破算法 B、监听截获 C、信息猜测 D、暴力破解

519、非对称密码技术的缺点有哪些？（B）

A、密钥持有量减少 B、加/解密速度慢 C、耗用资源较少 D、以上都是

520、CA不能提供下列哪种证书？（D）

A、个人数字证书 B、SSL服务器证书

C、安全电子邮件证书 D、SET服务器证书

521、以下关于混合加密方式说法正确的是（B）。

A、采用公开密钥体制进行通信过程中的加解密处理

B、采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C、采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D、采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密

处理速度快的双重优点

522.、果要保证（C）原则，则不能在中途修改消息内容。

A、保密性 B、鉴别 C、完整性 D、访问控制

523、口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（D）

A、长期没有修改的口令 B、过短的口令

C、两个人共用的口令 D、设备供应商提供的默认的口令

524.非对称密钥的密码技术具有很多优点，其中不包括：（B）。

A、可提供数字签名、零知识证明等额外服务

B、加密/解密速度快，不需占用较多资源

C、通信双方事先不需要通过保密信道交换密钥

D、密钥持有量大大减少

525．DES是一种block（块）密文的加密算法，是把数据加密成多大的块？（B）

A、32位 B、64位 C、128位 D、256位

526．CA数字证书中不包含的信息有（C）。

A、CA的数字签名 B、证书申请者的个人信息

C、证书申请者的私钥 D、证书申请者的公钥信息

527．以下关于对称密钥加密说法正确的是（C）。

A、加密方和解密可以使用不同的算法 B、加密密钥和解密密钥可以是不同的

C、加密密钥和解密密钥必须是相同的 D、密钥的管理非常简单

528、在为计算机设置使用密码时，下面（D）密码是最安全的。

A、12345678 B、66666666

C、20061001 D、72aB@#41

529、（C）的攻击者发生在Web应用层？

A、25% B、50%

C、75% D、90%

530、“U盘破坏者”病毒（Worm.vhy）采用（B）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。

A、网上邻居 B、我的电脑

C、我的文档 D、收藏夹

531、“冲击波”病毒运行时会将自身复制到Windows目录下，并命名为（C）

A、Gsrss.exe B、msbast.exe

C、msblast.exe D、lsass.exe

532、Code Red 爆发于2001年7月，利用微软的IIS漏洞在Web服务器之间传播。针对这一漏洞，微软早在2001年三月就发布了相关的补丁。如果今天服务器仍然感染Code Red，那么属于哪个阶段的问题？（A）

A、系统管理员维护阶段的失误 B、微软公司软件的设计阶段的失误

C、最终用户使用阶段的失误 D、微软公司软件的实现阶段的失误

533、病毒的传播机制主要有哪些？（D）

A、移动存储 B、电子邮件 C、网络共享 D、以上均是

534、病毒的反静态反汇编技术都有（D）。

A、数据压缩 B、数据加密 C、感染代码 D、以上均是

535、病毒在感染计算机系统时，一般（B）感染系统的。

A、病毒程序都会在屏幕上提示，待操作者确认（允许）后

B、实在操作者不觉察的情况下

C、病毒程序会要求操作者制定存储的磁盘和文件夹后

D、在操作者为病毒制定存储的文件名以后

536、杀毒软件时提示“重新启动计算机后删除文件”其主要原因是（A）

A、文件插入了系统关键进程，杀毒时无法处理

B、文件是病毒文件，无法处理

C、由于病毒的加壳形式不同，杀毒时无法正确处理

D、文件正在运行且无法安全的结束，需要其他处理方法

537、蠕虫的目标选择算法有（D）。

A、随机性扫描 B、基于目标列表的扫描

C、顺序扫描 D、以上均是

538、网络钓鱼是指（A）

A、通过大量发送声来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息。

B、网上进行钓鱼活动

C、通过网络组织钓鱼活动，从而获得利益 D、以上都不是

539、不属于常见把入侵主机的信息发送给攻击者的方法是（D）。

A、E-MAIL B、UDP C、ICMP D、连接入侵主机

540、不属于黑客被动攻击的是（A）

A、缓冲区溢出 B、运行恶意软件 C、浏览恶意代码网页 D、打开病毒附件

541、不属于黑客前期收集信息的工具是（D）

A、Nmap B、Xscan C、Nslookup D、LC

542、常见Web攻击方法，不包括？（D）

A、利用服务器配置漏洞 B、恶意代码上传下载

C、构造恶意输入（SQL注入攻击、命令注入攻击、跨站脚本攻击）

D、业务测试

543、常用的抓包软件有（A）。

A、ethereal B、MS office C、fluxay D、netscan

544.网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（A）

A、密码加密后，不会被窃听 B、Cookie字段可以被窃听

C、报文和帧可以窃听 D、高级窃听者还可以进行ARPSpoof，中间人攻击

545、除了在代码设计开发阶段预防SQL注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（C）

A、禁止将任何高权限账号（例如sa,dba等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户

B、拒绝用户访问敏感的系统存储过程

C、禁止用户访问的数据库表 D、限制用户所能够访问的数据库表

546、防止用户被冒名所欺骗的方法是（A）。

A、对信息源发放进行身份验证 B、进行数据加密

C、对访问网络的流量进行过滤和保护 D、采用防火墙

547、给电脑设置多道口令，其中进入电脑的第一道口令是（B）。

A、系统口令 B、CMOS口令

C、文件夹口令 D、文档密码

548、攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息重新发往B称为（D）。

A、中间人攻击 B、口令猜测器和字典攻击

C、强力攻击 D、回放攻击

549、故意制作、传播计算机病毒，造成计算机信息系统不能正常运行，但如果后果不严重就无罪，可以原谅，这种说法（C）。

A、不对，对这种蓄意破坏行为不能原谅 B、即使不是故意的，后果也不很严重

C、对。我国实行成文法，根据《中华人民共和国刑法》第286条的规定，只有造成严重后果者才有罪

D、无法断定

550、关于80年代Mirros蠕虫危害的描述，哪句话是错误的？（B）

A、占用了大量的计算机处理器的时间，导致拒绝股务

B、窃取用户的机密信息，破坏计算机数据文件

C、该蠕虫利用Unix系统上的漏洞传播

D、大量的流量堵塞了网络，导致网络瘫痪

551、关于黑客注入攻击说法错误的是： (D)

A、它的主要原因是程序对用户的输入缺乏过滤

B、一般情况下防火墙对它无法防范

C、对它进行防范时要关注操作系统的版本和安全补丁

D、注入成功后可以获取部分权限

552、基于主机评估报告对主机进行加固时，第一步是（B）。

A、账号、口令策略修改 B、补丁安装

C、文件系统加固 D、日志审核增强

553、计算机病毒会对下列计算机服务造成威胁，除了（C）。

A、完整性 B、有效性

C、保密性 D、可用性

554、计算机病毒是一段可运行的程序，它一般（C）保存在磁盘中。

A、作为一个文件 B、作为一段数据

C、不作为单独文件 D、作为一段资料

555、什么方式能够从远程绕过防火墙去入侵一个网络？(D)

A、IP services\_ B、Active ports

C、Identified network topology D、Modem banks

556、输入法漏洞通过（D）端口实现的。

A、21 B、23 C、445 D、3389

557、特洛伊木马攻击的威胁类型属于（B）。

A、授权侵犯威胁 B、植入威胁

C、渗入威胁 D、旁路控制威胁

558、通常黑客扫描目标机的445端口是为了(B)。

A、利用NETBIOS SMB服务发起DOS攻击

B、发现并获得目标机上的文件及打印机共享

C、利用SMB服务确认Windows系统版本

D、利用NETBIOS服务确认Windows系统版本

559、网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？(A)

A、残余风险评估阶段 B、检查阶段

C、入侵检测系统监控阶段 D、网络异常流量临控阶段

560、网络病毒预防范阶段的主要措施是什么？(A)

A、强制补丁、网络异常流量的发现 B、强制补丁、入侵检测系统监控

C、网络异常流量的发现、入侵检测系统的监控阶段 D、缺少D选项

561、下列除了(B)以外，都是防范计算机病毒侵害的有效方法。

A、使用防病毒软件 B、机房保持卫生，经常进行消毒

C、避免外来的磁盘接触系统 D、网络使用防病毒网关设备

562、下列除了(A)以外，都是计算机病毒传

A、通过操作员接触传播 B、通过U盘接触传播

C、通过网络传播 D、通过电子播的途径邮件传播

563、下列措施中，(C)不是减少病毒的传染

和造成的损失的好办法。

A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B、外来的文件要经过病毒检测才能使用，不要使用盗版软件

C、不与外界进行任何交流，所有软件都自行开发

D、定期用抗病毒软件对系统进行查毒、杀毒

564、下列哪项是跨站脚本Cross Site Scripting攻击具体事例？（B）

A、搜索用户 B、发帖子，发消息 C、上传附件 D、下载文件

565、下列哪项为信息泄露与错误处理不当Information Leakage and Improper

Error Handlina攻击具体实例？(D)

A、不明邮件中隐藏的html链接 B、发帖子，发消息

C、上传附件 D、错误信息揭示路径

566、下面哪一项是黑客用来实施DDoS攻击的工具？(D)

A、LC5 B、Rootkit C、Icesword D、Trinoo

567、以下哪个工具可以抹去所有NT/2K配置，并将其还原到初始状态？(A)

A、Rollback. exe B、Recover. exe C、Zap. exe D、Reset. exe

568、以下哪个工具通常是系统自带任务管理器的替代？(D)

A、Regmon B、Filemon C、Autoruns D、Process explorer

569、以下哪个针对访问控制的安全措施是最容易使用和管理的？(C)

A、密码 B、加密标志 C、硬件加密 D、加密数据文件

570、以下哪项不是分布式拒绝服务攻击常用的工具？(D)

A、Trinoo B、Trinoo C、TFN D、synkill

571、以下哪项不属于针对数据库的攻击？(D)

A、特权提升 B、强力破解弱口令或默认的用户名及口令

C、SQL注入 D、利用xss漏洞攻击

572、以下哪项工具不适合用来做网络监听？(B)

A、sniffer B、Webscan C、 Windump D、 D-Iris

573、以下哪项是SYN变种攻击经常用到的工具？(B)

A、sessionIE B、synkill C、TFN D、Webscan

574、以下哪一项不是流氓软件的特征？(D)

A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装

B、通常添加驱动保护使用户难以卸载

C、通常会启动无用的程序浪费计算机的资源

D、通常会显示下流的言论

575、一个数据仓库中发生了安全性破坏。以下哪一项有助于安全调查的进行？(B)

A、访问路径 B、时戳 C、数据定义 D、数据分类

576、以下哪一项不属于恶意代码？(C)

A、病毒 B、蠕虫 C、宏 D、特洛伊木马

577、以下哪一项不属于计算机病毒的防治策略？(D)

A、防毒能力 B、查毒能力 C、杀毒能力 D、禁毒能力

578、以下哪一项是常见Web站点脆弱性扫描工具？(A)

A、Appscan B、Nmap C、Sniffer D、LC

579、以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？(A)

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将臀陆信息写入记事本

580、以下哪种符号在SQL注入攻击中经常用到？(D)

A、$\_ B、1 C、@ D、;

581、以下哪种工具能从网络上检测出网络监听软件(A)

A、sniffdet, , B、purify, , C、Dsniff D、WireShark

582、以下哪种攻击可能导致某些系统在重组IP分片的过程中宕机或者重新启动？(B)

A、分布式拒绝服务攻击 B、Ping of Death

C、NFS攻击 D、DNS缓存毒化攻击

583、下面哪部分不属于入侵的过程？(B)

A、数据采集 B、数据存储 C、数据检测 D、数据分析

584、以下对木马阐述不正确的是(A)。

A、木马可以自我复制和传播

B、有些木马可以查看目标主机的屏幕

C、有些木马可以对目标主机上的文件进行任意揉作

D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。

585、由于攻击者可以借助某种手段，避开DBMS以及应用程序而直接进入系统访问

数据，我们通常采取以下哪种方式来防范？(A)

A、数据库加密

B、修改数据库用户的密码，将之改得更为复杂

C、使用修改查询法，使用户在查询数据库时需要满足更多的条件

D、使用集合法

586、在大多数情况下，病毒侵入计算机系统以后，(D)。

A、病毒程序将立即破坏整个计算机软件系统

B、计算机系统将立即不能执行我们的各项任务

C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

587、在确定威胁的可能性时，可以不考虑以下哪项？(D)

A、威胁源 B、潜在弱点

C、现有控制措施 D、攻击所产生的负面影响

588、在以下人为的恶意攻击行为中，属于主动攻击的是(A)。

A、身份假冒 B、数据GG C、数据流分析 D、非法访问

589、下面哪一种攻击方式最常用于破解口 令？(B)

A、哄骗( spoofing) B、字典攻击(dictionary attack)

C、拒绝服务(DoS) D、WinNuk

590、针对DNS服务器发起的查询DoS攻击，属于下列哪种攻击类型？(C)

A、syn flood B、ack flood C、 udpflood D、Connection flood

591、下列哪项不是安全编码中输入验证的控制项？(D)

A、数字型的输入必须是合法的数字

B、字符型的输入中对’进行特殊处理

C、验证所有的输入点，包括Get，Post，Cookie以及其他HTTP头

D、正确使用静态查询语句，如PreDaredStatement

592、以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？(C)

A、早期的SMTP协议没有发件人认证的功能

B、网络上存在大量开放式的邮件中转服务器，导致垃圾邮件的来源难于追查

C、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因

D、Internet分布式管理的性质，导致很难控制和管理

593、以下哪种方法是防止便携式计算机机密信息泄露的最有效方法？（A）

A、用所有者的公钥对硬盘进行加密处理 B、激活引导口令（硬件设置口令）

C、利用生物识别设备 D、利用双因子识别技术将登录信息写入记事本

594、以下哪种攻击属于DDoS类攻击？（A）

A、SYN变种攻击 B、smurf攻击 C、arp攻击 D、Fraggle攻击

595、URL访问控制不当不包括（D）

A、Web应用对页面权限控制不严 B、缺乏统一规范的权限控制框架

C、部分页面可以直接从URL中访问 D、使用分散登录认证

596、Web应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（A）

A、静态密码 B、短信挑战 C、指纹认证 D、图片认证

597、Web应用漏洞按类别进行排名，由多到少正确的顺序为？（A）

A、跨站脚本、注入、恶意代码、引用不当

B、注入、跨站脚本、恶意代码、引用不当

C、恶意代码、跨站脚本、注入、引用不当

D、引用不当、跨站脚本、注入、恶意代码

598、从技术角度，以下不是漏洞来源的是（D）

A、软件或协议设计时候的瑕疵 B、软件或协议实现中的弱点

C、软件本身的瑕疵 D、显示卡内存容量过低

599、（C）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A、身份假冒 B、数据篡改 C、信息窃取 D、越权访问

600、有关密码学分支的定义，下列说法中错误的是（D）

A、密码学是研究信息系统安全保密的科学，由两个相互对立、相互斗争、而且又相辅相成、相互渗透的分支科学所组成的、分别称为密码编码学和密码分析学

B、密码编码学是对密码体制、密码体制的输入输出关系进行分析、以便推出机密变量、包括明文在内的敏感数据

C、密码分析学主要研究加密信息的破译或信息的伪造

D、密码编码学主要研究对信息进行编码，实现信息的隐藏

601、与RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（C）

A、数字签名 B、鉴别机制 C、加密机制 D、数据完整性

602、以下哪项是数据库加密方法中的库外加密的缺点？（A）

A、即使访问一条数据也要对整个数据库解密 B、密钥管理比较复杂

C、加密之后不能完整的查询数据 D、密钥过于简单，容易被破解

603、以下哪项数据中涉及安全保密的最主要问题？（A）

A、访问控制问题 B、数据完整性 C、数据正确性 D、数据安全性

604、以下哪一个最好的描述了数字证书？（A）

A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，它使得黑客不能得知用户的身份

C、网站要求用户使用用户名和密码登陆的安全机制

D、伴随在线交易证明购买的收据

605、TCP SYN Flood网络攻击时利用了TCP建立连接过程需要（C）次握手的特点而完成对目标进行攻击的。

A、1 B、2 C、3 D、6

二、多项选择题（606-789）

606、COBIT度量过程的三个纬度分别是（ABC）。

A、能力 B、绩效 C、控制度 D、能力成熟度

607、IT系统内网与互联网连接检查手段有哪些？（BCD）

A、工具扫描 B、人员访谈 C、人工检查 D、文档检查

608、公司应该采取以下措施，对第三方访问进行控制。（ABCD）

A、公司应于第三发公司法人签署保密协议，并要求其第三方个人签署保密承诺，此项工作应在第三方获得网络与信息资产的访问权限之前完成

B、实行访问授权管理，未经授权，第三方不得进行任何形式的访问

C、公司应加强第三方访问的过程控制，监督其活动及操作，对其进行适当的安全宣传与培训

D、第三方人员应佩戴易于识别的标志，并在访问公司重要场所时有专人陪同

609、计算机信息系统安全的三个相辅相成，互补互通的有机组成部分是（ABD）

A、安全策略 B、安全法规 C、安全技术 D、安全管理

610、劳动合同中应包含网络与信息安全条款，这些条款规定（ACD）。

A、员工的安全责任和违约罚则

B、安全责任不可延伸至公司场所以外和正常工作时间以外

C、安全责任可延伸至公司场所以外和正常工作时间以外

D、如必要，一些安全责任应在雇佣结束后延续一段特定的时间

611、审核是网络安全工作的核心，下列应用属于主动审核的是：（CD）

A、Windows事件日志记录 B、数据库的事务日志记录

C、防火墙对访问站点的过滤 D、系统对非法链接的拒绝

612、通用准则CC实现的目标有（ABC）

A、成为统一的国际通用安全产品、系统的安全标准

B、在不同国家达成协议，相互承认产品安全等级评估

C、概述IT产品的国际通用性 D、都不是

613、系统用户账号登记表应包括（ABCD）。

A、使用者姓名、部门、职务、联系电话 B、账号权限

C、批准人、开通人 D、开通时间、到期日

614、下列情况哪些是对公司经营管理的影响为“一般”级别的互联网网络安全事件？（ABD）

A、发生未到达“预警”的一般性安全事件

B、出现新的漏洞，尚未发现利用方法或利用迹象

C、有来自境外的网络性能明显下降的报警，并且其技术原因普遍适用于我国互联网 D、出现新的蠕虫/病毒或其它恶意代码，尚未证明可能造成严重危害

615、信息安全的主要原则有（BCD）

A、认证性 B、保密性 C、可用性 D、完整性

**616、针对支撑系统，除业务关联性、对业务网络的影响，资产价值主要体现在（ACD）几个方面。 缺少D选项**

**A、业务收益的影响 B、设备购买成本 C、面向客户的重要程度 D、**

617、IT系统病毒泛滥的主要原因有哪些？（ABCD）

A、主机和终端防病毒软件缺乏统一管理

B、主机和终端防病毒软件没有设置为自动更新或更新周期较长

C、防病毒服务器没有及时更新放病毒库

D、缺乏防病毒应急处理流程和方案

618、IT系统病毒防护评估检查对象包括哪些内容？（ABCD）

A、防病毒服务器 B、重要应用Windows主机

C、Windows终端 D、主机管理员

619、互联网连接防火墙设备的安全策略配置要求包括哪几点（ABCD）。

A、远程登录是否禁止telnet方式 B、最后一条策略是否是拒绝一切流量

C、是否存在允许any to any的策略

D、是否设置了管理IP，设备只能从管理IP登录维护

620、《安全基线标准》在安全管理层面主要围绕哪几部分考评安全基线？（ABC）

A、组织架构管理 B、人员安全管理 C、运维安全管理 D、制度安全管理

621、IT系统维护人员权限原则包括（ACD）。

A、工作相关 B、最大授权 C、最小授权 D、权限制约

622、安全系统加固手册中关于造成系统异常中断的各方面因素，主要包括哪三方面（ABD）

A、人为原因 B、环境原因 C、生产原因 D、设备原因

623、IT系统维护人员权限原则包括（ACD）

A、工作相关 B、最大授权 C、最小授权 D、权限制约

624、计算当前Linux系统中所有用户的数量，可以使用（ABC）命令

A、wc -l /etc/passwd B、wc -l</etc/passwd

C、cat/etc/passwd|wc -l D、cat/etc/passwd>wc -l

625、Solarid系统中，攻击者在系统中增加账户会改变哪些文件？（AB）

A、shadow B、passwd C、inetd,conf D、hosts

626、Syn Flood攻击的现象有以下哪些？（ABC）

A、大量连接处于SYN\_RCVD状态 B、正常网络访问受阻

C、系统资源使用率高

627、UNIX安全审计的主要技术手段有哪些？（ABCDEF）

A、文件完整性审计 B、用户、弱口令审计 C、安全补丁审计

D、端口审计 E、进程审计 F、系统日志审计

628、Unix系统提供备份工具有（ABCD）

A、cp：可以完成把某一目录内容拷贝到另一目录

B、tar：可以创建、把文件添加到或从一个tar档案中解开文件

C、cpio：把文件拷贝进或拷贝出一个cpio档案或tar档案

D、dump：用来恢复整个文件系统或提取单个文件

629、操作系统应利用安全工具提供以下哪些访问控制功能？（ABC）

A、验证用户身份，必要的话，还应进行终端或物理地点识别

B、记录所有系统访问日志

C、必要时，应能限制用户连接时间 D、都不对

630、从哪些地方可以看到遗留痕迹？（ABCD）

A、回收站 B、最近使用过的文件 C、注册表 D、文件最后更改的时间戳631、

632、关于Windows活动目录说法正确的是（ABD）。

A、活动目录是采用分层结构来存储网络对象信息的一种网络管理体系

B、活动目录可以提供存储目录数据和网络用户级管理员使用这些数据的方法

C、利用活动目录来实现域内计算机的分布式管理

D、活动目录与域紧密结合构成与目录林和域目录树，使大型网络中庞大、复杂的网络管理、控制、访问变得简单，使网络管理效率更高

633、建立堡垒主机的一般原则是（AC）。

A、最简化原则 B、复杂化原则 C、预防原则 D、网络隔离原则

634、逻辑空间主要包括哪些部分？（ABDE）

A、TABLESPACES B、SEGMENTS C、DATAFILE

D、EXTENTS E、BLOCK

635、哪些属于Windows日志？（ABCD）

A、AppEvent.Evt B、SecEvent.Evt C、SysEvent.Evt D、W3C扩展日志

636、如何设置listener口令？（ACDE）

A、以Oracle用户运行lsnrctl命令 B、set log\_file

C、change\_password D、set password E、save\_config

637、审计启动其日志有哪两种存放方式？（BD）

A、NONE B、OS C、TRUE D、SYS.AUD$

638、生产服务器通常都是UNIX平台，资产价值最高，不直接连接外部网络，主要的安全需求是（ABD）

A、访问控制 B、账号口令 C、数据过滤 D、权限管理和补丁管理

639、使用md5sum工具对文件签名，以下说法正确的是？（ADE）

A、md5sum对任何签名结果是定长的16字节

B、md5sum对文件签名具有不可抵赖性

C、md5sum是对文件进行加密运算得出签名，不同文件结果几乎不相同

D、md5sum是对文件进行哈希运算得出签名，不同文件结果几乎不相同

E、md5sum对文件签名时，与文件的日期和时间无关

640、为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有（ABCD）

A、口令/账号加密 B、定期更换口令

C、限制对口令文件的访问 D、设置复杂的、具有一定位数的口令

641、文件系统是构成Linux基础，Linux中常用文件系统有（ABD）？

A、ext3 B、ext2 C、hfs D、reiserfs

642、下列关于UNIX下日志说法正确的是（AC）

A、wtmp记录每一次用户登录和注销的历史信息

B、acct记录每个用户使用过的命令

C、sulog记录su命令的使用情况

D、acct记录当前登录的每个用户

643、下列哪些操作可以看到自启动项目？（ABD）

A、注册表 B、开始菜单 C、任务管理器 D、msconfig

644、下列哪些命令行可用于查看当前进程？（ABC）

A、Ps -ef B、Strings -f/proc/[0-9]\*/cmdline

C、Ls -al /proc/[0-9]\*/exe D、Cat/etc/inetd.conf

645、下面操作系统中，哪些是UNIX操作系统？（CD）

A、Red-hat Linux B、Novell Netware C、Free BSD D、SCO Unix

646、严格的口令策略应当包含哪些要素（ABC）

A、满足一定的长度，比如8位以上 B、同时包含数字，字母和特殊字符

C、系统强制要求定期更改口令 D、用户可以设置空口令

647、在Solaris 8 下，使用ps -ef命令列出进程中有一行如下“root 1331 0 00:01:00? 0:00 /usr/sbin/inetd -s -t”，以下说法正确的是（ABE）

A、参数-t是trace，记录包括IP和PORT等信息

B、参数-t对于UDP服务无效 C、进程启动的时间不能确定

D、进程已经运行了1分钟 E、进程的父进程号是1

648、在Solaris 8 下，以下说法正确的是：（AB）

A、/etc/rc2.d里S开头的文件在系统缺省安装的缺省级别会自动运行

B、/etc/rc3.d里S开头的文件在系统缺省安装的缺省级别会自动运行

C、/etc/init.d里的文件在系统启动任何级别时会自动运行

D、init 0是进入单用户级别 E、init 6命令会运行所有级别的rc目录下以S开头的文件

649、在Solaris 8 下，以下说法正确的是：（BC）

A、PATH环境变量最后带有“.”，会使当前目录的命令比其他目录的命令有限执行

B、可以修改/etc/inittab里ttymon的参数，使得登录的SHELL在无输入时自动退出

C、在使用/bin/ksh时，可以设置TMOUT值，使得登录的SHELL在无输入时自动退出

D、在/etc/login中，可以设置TIMEOUT值，使得登录的SHELL在无输入时自动退出

E、tar xvf命令的意思是以tar格式解开输入，并且保持文件属性等参数不变

650、在配置Apache访问控制时，Allow和Deny指令可以允许或拒绝来自特定主机名或主机名地址的访问。那么下列哪些配置是不正确的？（AD）

A、Order allow,deny Allow from 192.101.205

B、B、Order deny,allow Deny from all Allow from example

C、C、Order deny,allow Deny from 192.101.205

D、D、Order allow,deny Deny from 192.101.205 Allow from all

651、造成操作系统安全漏洞的原因是（ABC）。

A、不安全的编程语言 B、不安全的编程习惯

C、考虑不周的架构设计 D、人为的恶意破坏

652、针对Linux主机，一般的加固手段包括（ABC）。

A、打补丁 B、关闭不必要的服务 C、限制访问主机 D、切断网络

653、做系统快照，查看端口信息的方式有（AD）。

A、netstat -an B、net share C、net use D、用taskinfo来查看连接情况

654、网厅安全解决方案主要从哪几个方面对网厅安全进行建议和指导？（ABCD）

A、安全管理 B、安全防护 C、安全运维 D、灾备/恢复

655、IT系统软件设计中应当考虑并执行安全审计功能，详细记录访问信息的活动，包括（ABCD）。

A、记录的活动以是否有数据的修改、应用程序的异常关闭、异常删除触发

B、应用系统应当配置单独的审计数据库，审计记录应单独存放，并设置严格的边界访问控制，只有安全管理人员才能够看到审计记录

C、信息系统的审计功能包括：事件日期、时间、发起者信息、类型、描述和结果

D、应用系统的审计进程为后台处理，与应用系统运行同步进行，并且对于审计进程应当涉及相应的守护进程，一旦出现异常停止系统可重新启动审计进程，从而保障审计的“完整性”

656、IPSec的配置步骤包括：（ABCD）

A、防火墙基本配置 B、定义保护数据流和域间规则

C、配置IPSec安全提议 D、配置IKEPeer

657、Juniper路由器在配置SSH访问时应注意如下（ABCD）细节。

A、建立允许访问的SSH-ADDRESSES过滤器

B、确保只允许来自内部接口的授权用户访问

C、针对SSH进行限速以保护路由引擎

D、过滤器应用在loopback接口

658、对于使用RPF反向地址验证，以下说法错误的是：（BCD）。

A、对称路由可以使用 B、非对称路由可以使用

C、有些情况不可以使用，但与对称或非对称路由无关

D、在任何情况下都可以使用

659、防病毒服务升级检查包括如下几项内容？（ABC）

A、检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决

B、在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本

C、对重要的服务器，定期抽查防病毒客户端的病毒库升级情况

660、防范DOS攻击的方法主要有（ABCD）。

A、安装Dos检测系统 B、对黑洞路由表里的地址进行过滤

C、及时打好补丁 D、正确配置TCP/IP参数

661、防火墙trust域中的客户机通过nat访问untrust中的服务器的ftp服务，已经允许客户机访问服务器的tcp21端口，但只能登陆到服务器，却无法下载文件，以下解决办法中可能的是：（ABC）

A、修改trust untrust域间双向的默认访问策略为允许

B、FTP工作方式为port模式时，修改untrust trust域间in方向的默认访问策略为允许 C、在trust untrust域间配置中启用detect ftp

D、FTP工作方式为passive模式时，修改untrust trust域间in方向的默认访问策略为允许

662、防火墙不能防止以下哪些攻击？（ABD）

A、内部网络用户的攻击 B、传送已感染病毒的软件和文件

C、外部网络用户的IP地址欺骗 D、数据驱动型的攻击

663、防火墙常见的集中工作模式有（ABC）。

A、路由 B、NAT C、透明 D、旁路

664、防火墙的缺陷主要有（ABCD）。

A、限制有用的网络服务 B、无法防护内部网络用户的攻击

C、不能防备新的网络安全问题 D、不能完全防止传送已感染病毒的软件或文件

665、防火墙的日志管理应遵循如下原则：（BC）

A、本地保存日志 B、本地保存日志并把日志保存到日志服务器上

C、保持时钟的同步 D、在日志服务器保存日志

666、防火墙的特征是（ABCD）。

A、保护脆弱和有缺陷的网络服务 B、加强对网络系统的访问控制

C、加强隐私，隐藏内部网络结构 D、对网络存取和访问进行监控审计

667、防火墙的主要功能有哪些？（ABCD）

A、过滤进、出网络的数据 B、管理进、出网络的访问行为

C、封堵某些禁止的业务，对网络攻击进行检测和报警

D、记录通过防火墙的信息内容和活动

668、防火墙的作用主要有（ABCD）。

A、实现一个公司的安全策略 B、创建一个阻塞点

C、记录Internet活动 D、限制网络暴露

669、防火墙技术，涉及到（ABCD）。

A、计算机网络技术 B、密码技术 C、软件技术 D、安全操作系统

670、防火墙可以部署在下列位置：（ABCD）。

A、安全域边界 B、服务器区域边界

C、可信网络区域和不可信网络区域之间 D、根据网络特点设计方案

671、防火墙配置时应确保（ABCD）服务不开放。

A、Rlogin B、NNTP C、Finger D、NFS

672、启用Cisco设备的访问控制列表，可以起到如下作用（ABC）。

A、过滤恶意和垃圾路由信息 B、控制网络的垃圾信息流

C、控制未授权的远程访问 D、防止DDoS攻击

673、如果Cisco设备的VTY需要远程访问，则需要配置（ABCD）。

A、至少8位含数字、大小写、特写字符的密码 B、远程连接的并发数目

C、访问控制列表 D、超市退出

674、如果需要配置Cisco路由器禁止从网络启动和自动从网络下载初始配置文件，配置命令包括（AB）。

A、no boot network B、no service config C、no boot config D、no service network

675、入侵检测的内容主要包括：（BC）。

A、独占资源、恶意使用 B、试图闯入或成功闯入、冒充其他用户

C、安全审计 D、违反安全策略、合法用户的泄露

676、入侵检测系统包括以下哪些类型？（AC）

A、主机入侵检测系统 B、链路状态入侵检测系统

C、网络入侵检测系统 D、数据包过滤入侵检测系统

677、随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器（sniffer）来监听整个子网的办法不再可行。可选择解决的办法有（ABCD）。

A、使用交换机的核心芯片上的一个调试的端口

B、把入侵检测系统放在交换机内部或防火墙等数据流的关键入口

C、采用分解器（tap）

D、使用以透明网桥模式接入的入侵检测系统

678、通常要求把路由器的日志存储在专用日志服务器上，假设把Cisco路由器日志存储在192.168.0.100的syslog服务器上，需要在路由器侧配置的操作时：（ABCD）。

A、使用Router(config)# logging on启用日志：使用Router(config)# logging trap information将记录日志级别设定为“information”

B、使用Routee(config)# logging192.168.0.100将记录日志类型设定为“local6”

C、使用(config)# logging facility local6将日志发送到192.168.0.100

D、使用(config)# logging sourceinterface loopback0设定日志发送源loopback0

679、通过SSL VPN接入企业内部的应用，其优势体现在哪些方面：（ABCD）。

A、应用代理 B、穿越NAT和防火墙设备

C、完善的资源访问控制 D、抵御外部攻击

680、网络地址端口转换（NAPT）与普通地址转换有什么区别？（AD）

A、经过NAPT转换后，对于外网用户，所有报文都来自于同一个IP地址

B、NAT只支持应用层的协议地址转换

C、NAPT只支持网络层的协议地址转换

D、NAT支持网络层的协议地址转换

681、网络攻击的类型包括以下哪几种？（ABCD）

A、窃取口令 B、系统漏洞和后门 C、协议缺陷 D、拒绝服务

682、网络面临的典型威胁包括（ABCD）。

A、未经授权的访问 B、信息在传送过程中被截获、篡改

C、黑客攻击 D、滥用和误用

683、网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，该类病毒程序大规模爆发后，会对相关网络造成拒绝服务攻击，为了防止受到网络蠕虫的侵害，应当注意对（ACD）及时进行升级更新。

A、计算机操作系统 B、计算机硬件 C、文字处理软件 D、应用软件

684、下列关于NAT地址转换的说法中哪些事正确的：（ABCD）。

A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

B、地址转换可以按照用户的需要，在局域网内向外提供FTP、WWW、Telnet等服务

C、有些应用层协议在数据中携带IP地址信息，对它们作NAT时还要修改上层数据中的IP地址信息

D、对于某些非TCP、UDP的协议（如ICMP、PPTP），作上层NAT时，会对它们的特征参数（如ICMP的id参数）进行转换。

685、下列哪两项正确描述了由WPA定义的无线安全标准？（BC）

A、使用公开密钥的认证方法 B、当客户端连接的时候都要进行动态密钥交换

C、包含PSK认证 D、定制了一个经常更换的静态的加密密钥来增强安全性

686、下列配置中，可以增强无线AP（access point）安全性的有（ABCD）。

A、禁止SSID广播 B、禁用DHCP服务

C、采用WPA2-PSK加密认证 D、启用MAC地址接入过滤

687、下面可以攻击状态检测的防火墙方法有：（ABD）

A、协议隧道攻击 B、利用FTP-pasv绕过防火墙认证的攻击

C、ip欺骗攻击 D、反弹木马攻击

688、下面什么路由协议不可以为HSRP的扩充：（ABC）

A、SNMP B、CDP C、HTTP D、VRRP

689、下面什么协议有MD5认证：（ABC）

A、BGP B、OSPF C、EIGER D、RIPversion 1

690、下面是网络安全技术的有：（ABC）

A、防火墙 B、防病毒 C、PKI D、UPS

691、选购一个防火墙时应该考虑的因素有：（ABCD）

A、网络受威胁的程度 B、可能受到的潜在损失

C、站点是否有经验丰富的管理员 D、未来扩展的需要

692、一台路由器的安全快照需要保存如下哪些信息？（AB）

A、当前的配置--running-config B、当前的开放端口列表

C、当前的路由表 D、当前的CPU状态

693、以下对于包过滤防火墙的描述正确的有（ACD）。

A、难以防范黑客攻击 B、处理速度非常慢

C、不支持应用层协议 D、不能处理新的安全威胁

694、以下对于代理防火墙的描述正确的有（ABCD）。

A、能够理解应用层上的协议 B、时延较高，吞吐量低

C、能做复杂一些的访问控制，并做精细的认证和审核 D、可伸缩性较差

695、以下关于L2TP VPN配置注意事项的说法中正确的有：（ABC）

A、L2TP的LNS端必须配置虚拟接口模板（Virtual-Template）的IP地址，该虚拟接口模板需要加入域

B、防火墙缺省需要进行隧道的认证。如果不配置认证，需要undo tunnel authentication命令

C、为了使L2TP拨号上来的用户分配的地址不能喝内网用户的地址在同一个网段

D、LNS端不允许配置多个L2TP-Group

1. 以下哪几项关于安全审计和安全审计系统的描述是正确的？（CD）

A、对入侵和攻击行为只能起到威慑作用

B、安全审计不能有助于提高系统的抗抵赖性

C、安全审计是对系统记录和活动的独立审查和检验

D、安全审计系统可提供侦破辅助和取证功能

697、以下哪些属于网络欺骗方式？（ABCD）

A、IP欺骗 B、ARP欺骗 C、DNS欺骗 D、Web欺骗

698、以下哪些是防火墙规范管理需要的？（ABCD）

A、需要配置两个防火墙管理员 B、物理访问防火墙必须严密地控制

C、系统软件、配置数据文件在更改后必须进行备份

D、通过厂商指导发布的硬件和软件的bug和防火墙软件升级版

699、以下硬件安装维护重要安全提示正确的有：（ABCD）

A、不要在雷雨天气进行故障处理 B、保持故障处理区域的干净、干燥

C、上防静电手套或防静电腕带再执行安装和更换操作

D、在使用和操作设备时，需要按照正确的操作流程来操作

700、以下属于DTE(Data Terminal Equipment)数据终端设备的有（AB）

A、路由器 B、PC C、交换机 D、HUB

701、在防火墙的“访问控制”应用中，内网、外网、DMZ三者的访问关系为：（ABD）

A、内网可以访问外网 B、内网可以访问DMZ区

C、DMZ区可以访问内网 D、外网可以访问DMZ区

702、关于GRE校验和验证技术，当本端配置了校验和而对端没有配置校验和时，以下叙述正确的有（BC）。

A、本端对接收报文检查校验和 B、对端对接收报文检查校验和

C、本端对发送报文计算校验和 D、对端对发送报文计算校验和

703、配置PPP链路层协议时，链路层协议状态始终不能转为Up状态的处理建议：（ABCD）

A、PPP链路两端的接口上配置的参数和验证方式都必须一致，LCP检查才能成功

B、如果LCP协商失败，请检查LCP配置协商参数

C、请检查验证方式配置是否正确。因为LCP协商中，包含验证方式的协商。因为LCP协商中，包含验证方式的协商。验证方式协商失败也会导致LCP协商失败

D、接口试图下先执行shutdown命令将接口关闭，再执行undo shutdown命令重启接口

704、对DNSSEC的描述正确的有（AC）。

A、为DNS数据提供来源验证，即保证数据来自正确的名称服务器

B、DNSSEC可防御DNS Query Flood攻击

C、为域名数据提供完整性验证，即保证数据在传输的过程中没有被篡改

D、实施DNSSEC后，只需升级软件系统，对网络、服务器等硬件设备不需考虑

705、MySQL安装程序会给出三种选择，用户可以根据自身的需要选择一种适合的安装方式，以下哪些是正确的？（ABD）

A、Typical（典型安装） B、Compact(最小安装)

C、Full(全部安装) D、Custom(选择安装)

706、MySQL中用DROP语句可删除数据库和数据表，以下哪句是正确的语法？（ABCD）

A、DROP TABLE table\_name1 B、DROP TABLE table\_name1,table\_name2

C、DROP TABLE IF EXISTS table\_name1 D、DROP DATABASE DB name1

707、Oracle 7.2之前的数据库连接用户名和密码在网络传输时是不进行加密的，为了要和旧版本兼容Oracle数据库9.02存在DBLINK\_ENCRYPT\_LOGIN参数用来调节数据库连接时用户名和密码的加密特性，以下说法正确的是：（ACD）。

A、DBLINK\_ENCRYPT\_LOGIN为TRUE时，数据库连接加密用户名和密码

B、DBLINK\_ENCRYPT\_LOGIN时，数据库连接不加密用户名和密码

C、DBLINK\_ENCRYPT\_LOGIN为FALSE时，如果加密的数据库连接失败，会尝试不加密的连接

D、DBLINK\_ENCRYPT\_LOGIN为TRUE时，加密的数据库连接失败，也不会尝试不加密的连接

708、Oracle实例主要由哪两部分组成：（AC）

A、内存 B、Share pool buffer C、后台进程 D、pmon和smon

709、Oracle中如何设置audit trail审计，正确的说法是：（ABD）

A、在init.ora文件中设置“audit\_trail = true”或者“audit\_trail = db”

B、以SYSDBA身份使用AUDIT ALL ON SYS.AUD$ BY ACCESS，语句对audit trail审计

C、Oracle不支持对audit trail的审计

D、在设置audit trail审计前，要保证已经打开Oracle的审计机制

710、SQL Server的登录认证种类有以下哪些？（ACD）

A、Windows认证模式 B、双因子认证模式

C、混合认证模式 D、SQL Server认证

711、SQL Server的取消权限的操作有以下哪些？（ABC）

A、在“详细信息”窗格中右击要授予/拒绝/取消其权限的用户定义的角色

B、单击“属性”命令在“名称”下单击“权限”单击列出全部对象

C、选择在每个对象上授予拒绝或废除的权限，选中标志表示授予权限，X表示拒绝权限，空框表示废除权限，只列出适用于该对象的权限

D、回到“数据库用户属性”对话框中，再点击“确定”按钮，所有的设置就完成了

712、SQL Server中ALTER DATABASE可以提供以下哪些功能选项？（ABCD）

A、更改数据库名称 B、文件组名称 C、数据文件 D、日志文件的逻辑名称

713、SQL Server中关于实例的描述，请选择正确的答案。（ABD）

A、如果安装选择“默认”的实例名称。这时本SQL Server的名称将和Windows 2000服务器的名称相同

B、SQL Server可以在同一台服务器上安装多个实例

C、SQL Server只能在一台服务器上安装一个实例

D、实例各有一套不为其他实例共享的系统及用户数据库，所以各实例的运行是独立的。

714、SQL Server中使用企业管理器从数据库中删除数据或日志文件的步骤如下，正确的步骤是？（ABCD）

A、展开服务器组，然后展开服务器

B、展开“数据库”文件夹，右击要从中删除数据或日志文件的数据库，然后单击“属性”命令

C、若要删除数据文件，单击“常规”选项卡。若要删除日志文件，单击“事务日志”选项卡

D、在“文件名”列户，单击要删除的文件名旁边的箭头，再点DELETE键，文件名旁出现十字光标，表明将删除此文件

715、参数REMOTE\_LOGIN\_PASSWORDFILE在Oracle数据库实例的初始化参数文件中，此参数控制着密码文件的使用及其状态，以下说法正确的是：（ABCD）

A、NONE：只是Oracle系统不使用密码文件，不允许远程管理数据库

B、EXCLUSIVE：指示只有一个数据库实例可以使用密码文件

C、SHARED：指示可有多个数据库实例可以使用密码文件

D、以上说法都正确

716、关于SQL Server 2000中的SQL账号、角色，下面说法正确的是：（ABC）

A、PUBLIC,guest为缺省的账号 B、guest不能从master数据库清除

C、可以通过删除guest账号的角色，从而消弱guest可能带来的安全隐患

D、SQL Server角色的权限是不可以修改的

717、连接MySQL后选择需要的数据库DB\_NAME？以下哪些方法是对的（AC）

A、连接后用USE DB\_NAME选择数据库

B、连接后用SET DB\_NAME选择数据库

C、用mysql -h host -u user -p DB\_NAME连接数据库

D、用mysql -h host -u user -p -T DB\_NAME连接数据库

718、如果数据库不需要远程访问，可以禁止远程tcp/ip连接，以增强安全性。可选择的有效方法：（AC）

A、用防火墙封堵数据库侦听端口避免远程连接 B、禁止tcp/ip协议的使用

C、在mysqld服务器中参数中添加 --skip-networking启动参数来使mysql

D、在/etc/my.cnf下添加remoteConnnect=disable

719、以下哪些MySQL中GRANT语句的权限指定符？（ABCDEF）

A、ALTER B、CREATE C、DELETE

D、UPLOAD E、DROP F、INSERT

720、用THC组织的Oracle的工具，通过sniffer方式抓取数据库的认证信息可有效破解Oracle密码，以下哪些数据是必须获取的？（ABC）

A、AUTH\_SESSKEY B、AUTH\_PASSWORD C、用户名 D、实例名

721、在Oracle 9数据库可以通过配置$Oracle\_HOME\network\admin\sqlnet.ora文件实现数据库层次的基于TCP协议和地址的访问控制。下面说法正确的是：（ABCD）

A、首先需要配置TCP,VALIDNODE\_CHECKING=yes启用节点检查功能

B、其次配置TCP.INVITED\_NODES=192.168.0.12，192.168.0.33将会允许地址是192.168.0网段的12和33的主机访问

C、然后配置TCP.EXCLUDED\_NONES=192.168.0.123将会禁止地址是192.168.0网段的123的主机访问

D、要以上配置生效必须重启lsnrctl监听器

722、在SQL Server 2000中，如果想查询当前数据库服务器软件的版本，可以使用下面哪些方式（ABCD）

A、在查询分析器中通过如下语句查询SELECT ServerPROPERTY(‘productversion’),ServerPROPERTY(‘productlevel’),ServerPROPERTY(‘edition’)

B、在命令行下，用SQL Server自带的管理工具osql连接进入数据库，输入select@@version

C、企业管理器查看服务器属性 D、在SQL Server服务管理器里面查看“关于”

723、在SQL Server 2000中一些无用的存储过程，这些存储过程极容易被攻击者利用，攻击数据库系统。下面的存储过程哪些可以用来执行执行系统命令或修改注册表？（ABC）

A、xp\_cmdshell B、xp\_regwrite C、xp\_regdeletekey D、select \* from master

724、在SQL Server中创建数据库，如下哪些描述是正确的？（ABCD）

A、创建数据库的权限默认授权sysadmin和dbcreator固定服务器角色的成员，但是它仍可以授予其他用户

B、创建数据库的用户将成为该数据库的所有者

C、在一个服务器上，最多可以创建32,767个数据库

D、数据库名称必须遵循标示符规则

725、在对SQL Server 2000的相关文件、目录进行安全配置时，下面可以采用的措施是：（ABCD）

A、删除缺省安装时的例子样本库

B、将存放数据的库文件，配置权限为administrators组、system和启动SQL Server服务的用户账号及DBA组具有完全控制权限

C、对SQL Server安装目录，去除everyone的所有控制权限

D、将数据库数据相关的文件，保存在非系统盘的NTFS独立分区

726、sybase数据库文件系统需要哪些裸设备？（ABCD）

A、master B、proce C、data D、log

727、Oracle支持哪些加密方式？（ABCD）

A、DES B、RC4\_256 C、RC4\_40 D、DES40

728、SQL Server用事件探测器可以帮助排除故障和解决问题，创建跟踪的步骤如下哪些是正确的？（ABCD）

A、从“模板名称”下拉菜单为你创建跟踪选择一个模板

B、“事件探查器”主界面打开后，从“文件”菜单选择“新跟踪”

C、在“跟踪名称”文本框中输入你想要为这个跟踪创建的跟踪名称

D、修改这些默认的选项设置。通过点击“显示全部事件”和“显示全部列”复选框来查看其他的选项。

729、最重要的电磁场干扰源是：（BCD）

A、电源周波干扰 B、雷电电磁脉冲LEMP

C、电网操作过电压SEMP D、静电放电ESD

730、雷电侵入计算机信息系统的途径主要有：（ABD）

A、信息传输通道线侵入 B、电源馈线侵入 C、建筑物 D、地电位反击

731、电信生产其机房作业，是由专门的值机员、机务员来完成，作业内容是：固定电话、无线电话、电报、载波、短波、微波、卫星和电力等电信通信设备，使设备出去良好状态，保证其正常运行。（ABCD）

A、安装 B、值守 C、维护 D、检修

732、对计算机系统有影响的腐蚀性气体大体有如下几种：（ABCD）

A、二氧化硫 B、氢化硫 C、臭氧 D、一氧化碳

733、防火工作的基本措施有：（ABCD）

A、加强对人员的教育管理 B、加强对可燃物的管理

C、加强对物的管理 D、加强对火源、电源的管理

734、会导致电磁泄漏的有（ABCDE）

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

E、信号处理电

735、火灾自动报警、自动灭火系统部署应注意（ABCD）。

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、具有自动和手动两种触发装置

736、计算机场地安全测试包括（ABCD）。

A、温度，湿度，尘埃 B、照度，噪声，电磁场干扰环境场强

C、接地电阻，电压、频率 D、波形失真率，腐蚀性气体的分析方法

737、计算机信息系统设备处于不同雷电活动地区，其雷电电磁场强度有很大差异，根据这一差异，将被防护空间分为下列哪些防护区？（ABCD）

A、直击雷非防护区（LPZOA） B、直击雷防护区（LPZOB）

C、第一防护区（LPZI） D、后续防护区（LPZ2,3...等）

738、静电的危害有（ABCD）。

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

739、灭火的基本方法有（ABCD）。

A、冷却法 B、隔离法 C、窒息法 D、抑制

740、实体安全技术包括（ABD）。

A、环境安全 B、设备安全 C、人员安全 D、媒体安全

741、使用配有计算机的仪器设备时，不应该做的有：（ABCD）

A、更改登机密码和系统设置

B、自行安装软件

C、玩各种电脑游戏

D、将获得的图像、数据等资料存储在未予指定的硬盘分区上

742、硬件设备的使用管理包括（ABCD）。

A、严格按硬件设备的操作使用规程进行操作

B、建立设备使用情况日志，并登记使用过程

C、建立硬件设备故障情况登记表

D、坚持对设备进行例行维护和保养

743、预防静电的措施有（ABCD）。

A、接地 B、不使用或安装产生静电的设备

C、不在产生静电场所穿脱工作服 D、作业人员穿防静电鞋

744、在实验室中引起火灾的通常原因包括：（ABCD）

A、明火 B、电器保养不良

C、仪器设备在不使用时未关闭电源 D、使用易燃物品时粗心大意

745、直击雷：直接击在（ABCD）并产生电效应、热效应和机械力的雷电放电。

A、建筑物 B、构建物 C、地面突进物 D、大地或设备

746、员工区域安全守则包括：（ABCD）

A、非工作时间，员工进入或离开办公区域，应在值班人员处登记

B、外来人员进入办公区域或机房，相关员工必须全程陪同

C、将物品带入/带出公司，要遵守公司相关的规定及流程

D、参加会议时遵守会前、会中、会后的保密流程

747、机房出入控制措施包括：（ABCD）

A、机房接待前台须核查弄清业务系统安全区域的来访者的身份，并记录其进入和离开安全区域的日期与时间

B、机房须告知进入安全区的来访者，该区域的安全要求和紧急情况下的行动步骤

C、可采用强制性控制措施，对来访者的访问行为进行授权和验证

D、要求所有进出机房人员佩带易于辨识的标识

748、为了减小雷电损失，可以采取的措施有（ACD）

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

749、安全要求可以分解为（ABCDE）。

A、可控性 B、保密性 C、可用性 D、完整性 E、不可否认性

750、HASH加密使用复杂的数字算法来实现有效的加密，其算法包括（ABC）

A、MD2 B、MD4 C、MD5 D、Cost256

751、利用密码技术，可以实现网络安全所要求的。（ABCD）

A、数据保密性 B、数据完整性 C、数据可用性 D、身份验证

752、一个密码体系一般分为以下哪几个部分？（ABCD）

A、明文 B、加密密钥和解密密钥

C、密文 D、加密算法和解密算法

753、公钥密码体质的应用主要在于。（AC）

A、数字签名 B、加密 C、密钥管理 D、哈希函数

754、目前基于对称密钥体制的算法主要有。（BC）

A、RSA B、DES C、AES D、DSA

755、使用esp协议时，可以使用的加密运算是。（ABC）

A、DES B、3DES C、AES D、RSA

756、数字签名的作用是。（ACD）

A、确定一个人的身份 B、保密性

C、肯定是该人自己的签字 D、使该人与文件内容发生关系

757、以下属于对称加密算法的是：（ABD）

A、DES B、3DES C、SHA-1 D、RC4 E、MD5

758、在加密过程中，必须用到的三个主要元素是（ABC）

A、所传输的信息（明文） B、加密 钥匙（Encryption Key）

C、加密函数 D、传输信道

759、账号口令管理办法适用于所有和DSMP系统、智能网系统、彩铃平台相关的（ACD）

A、系统管理员 B、操作系统

C、操作维护人员 D、所有上述系统中存在的账号和口令

760、为保证密码安全，我们应采取的正确措施有（ABC）

A、不使用生日做密码 B、不使用少于5为的密码

C、不适应纯数字密码 D、将密码设的非常复杂并保证20位以上

761、公司在使用数据签名技术时，除充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名外，还应注意（ABCD）

A、采取保护公钥完整性的安全措施，例如使用公约证书

B、确定签名算法的类型、属性以及所用密钥长度

C、用于数字签名的密钥应不同于用来加密内容的密钥

D、符合有关数字签名的法律法规，必要时，应在合同或协议中规定使用数字签名的相 关事宜

762、相对于对称加密算法，非对称密钥加密算法（ACD）

A、加密数据的速率较低

B、更适合于现有网络中对所传输数据（明文）的加解密处理

C、安全性更好 D、加密和解密的密钥不同

763、一个典型的PKI应用系统包括（ABCD）实体

A、认证机构CA B、册机构RA C、证书及CRL目录库 D、用户端软件

764、加密的强度主要取决于（ABD）

A、算法的强度 B、密钥的保密性 C、明文的长度 D、密钥的强度

765、一下对于对称密钥加密说法正确的是（BCD）

A、对称加密算法的密钥易于管理 B、加解密双方使用同样的密钥

C、DES算法属于对称加密算法 D、相对于非对称加密算法，加解密处理速度比较快

766、在通信过程中，只采用数字签名可以解决（ABC）等问题

A、数据完整性 B、数据的抵抗赖性 C、数据的篡改 D、数据的保密性

767、对称密钥算法体系包括：（ABCDE）

A、明文(plaintext)：原始消息或数据，作为算法的输入

B、加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换

C、秘密密钥(secret key)：秘密密钥也是算法输入，算法进行的具体替换和转换取决于 这个密钥

D、密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对 于一个给定的消息，两个不同的密钥会产生两个不同的密文

、.解密算法(decryption algorithm)：本质上是加密算法的执行。它使用密文和统一密钥 产生原始明文

768、一下对于混合加密方式说法正确的是。（BCD）

A、 使用公开密钥密码体制对要传输的信息（明文）进行加解密处理

B、使用对称加密算法对要传输的信息（明文）进行加解密处理

C、使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信

D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的

769、电信的网页防篡改技术有（ABC）

A、外挂轮询技术 B、核心内嵌技术

C、时间触发技术 D、安装防病毒软件

770、病毒发展的趋势是？（ABC）

A、 范围更广 B、度更快 C、方式更多

771、病毒自启动方式一般有（ABC）

A、 修改注册表 B、将自身添加为服务

C、将自身添加到启动文件夹 D、修改系统配置文件

772、常见Web攻击方法有一下哪种？（ABCD）

A、SQL Injection B、Cookie欺骗 C、跨站脚本攻击

D、信息泄露漏洞 E、文件腹泻脚本存在的安全隐患

F、 GOOGLE HACKING

773、宏病毒感染一下哪些类型的文件？（ABCDEF）

A.、DOC B、EXE C、XLS D、DOT

774、木马传播包括一下哪些途径：（ACD）

A.、通过电子邮件的附件传播 B、通过下载文件传播

C、通过网页传播 D、通过聊天工具传播

775、目前最好的防病毒软件能做到的是（ABCD）

A.、检查计算机是否感染病毒，消除已感染的任何病毒

B、杜绝病毒对计算的侵害

C、查出计算机已感染的已知病毒，消除其中的一部分

D、检查计算机是否染有已知病毒，并作相应处理

776、通用的DoS攻击手段有哪些？（CD）

A、 SYN Attack B、ICMP Flood C、UDP Flood

D、Ping of Death E、Tear Drop F、Ip Spoofing

777、以下关于蠕虫的描述正确的有：（ABCDEF）

A、 蠕虫具有自动利用网络传播的特点，在传播的同时，造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪

B、 隐藏式蠕虫的基本特征，通过在主机上隐藏，使得用户不容易发现它的存在

C、蠕虫需要传播受感染的宿主文件来进行复制

D、蠕虫的传染能力主要是针对计算机内的文件系统。

778、以下哪几种扫描检测技术属于被动式的检测技术？（AB）

A、 基于应用的检测技术 B、基于主动的检测技术

C、基于目标的漏洞检测技术 D、基于网络的检测技术

779、以下是检查磁盘与文件是否被病毒感染的有效方法：（BC）

A、 检查磁盘目录中是否有病毒文件 B、用抗病毒软件检查磁盘的各个文件

C、用放大镜检查磁盘编码是否有霉变现象 D、检查文件的长度是否无故变化

780、造成计算机不安全的因素有（BD）等多种。

A、 技术原因 B、自然原因 C、认为原因 D、管理原因

781、嗅探技术有哪些特点？（ABCD）

A、间接性 B、.直接性 C、隐蔽性 D、开放性

782、一个恶意的攻击者必须具备哪几点？（ABC）

A、 方法 B、机会 C、动机 D、运气

783、对于DOS网络攻击，可以采用以下哪些措施来缓解主机系统被攻击进程。（ACD）

A.、缩短SYN Timeout时间和设置SYN Cookie B、增加网络带宽

C、在系统之前增加负载均衡设备 D、在防火墙上设置ACL或黑客路由

784、利用Bind/DNS漏洞攻击的分类主要有（ACD）

A、 拒绝服务 B、匿名登录 C、.缓冲区溢出

D、DNS缓存中毒 E、病毒或后门攻击

785、常见Web攻击方法有一下哪种？（ABCD）

A、 SQL Injection B、 Cookie欺骗 C、 跨站脚本攻击 D、信息泄露漏洞

786、黑客所使用的入侵技术主要包括（ABCDE）

A.、协议漏洞渗透 B、密码分析还原 C、应用漏洞分析与渗透

D、拒绝服务攻击 E、病毒或后门攻击

787、主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有（ABC）

A、针对入侵者采取措施 B、修正系统

C、收集更详细的信息 D、入侵追踪

788、下面哪些漏洞属于网络服务类安全漏洞：（BC）

A.、Windows 2000中文版输入法漏洞 B、IS Web服务存在的IDQ远程溢出漏洞

C、RPC DCOM服务漏洞 D、Web服务asp脚本漏洞

789、系统感染病毒后的现象有哪些？（ABCD）

A、系统错误或系统崩溃 B、系统反应慢，网络拥塞

C、陌生的进程或服务 D、陌生的自启动

**三、判断题：（790-1000）**

790、TCSEC将信息安全风机防护等级一共分为7个安全等级：D、C1、C2、B1、B2、B3、 A。(A)

A、正确 B、错误

791、通用标准v2版（CC）的安全等级是以EAL来表示的。（A）

A、正确 B、错误

792、一个企业的信息安全组织能否顺利开展工作（定期安全评估、日志安全巡检、定期安全审核、应急演练等），主要取决于公司领导对信息安全工作的认识程度和支持力度。（A）

A、正确 B、错误

793、在信息安全领域，CIA通常是指：保密性、完整性和可用性。（A）

A、正确 B、错误

794、信息安全是永远是相对的，并且需要不断持续关注和改进，永远没有一劳永逸的安全

防护措施。（A）

A、正确 B、错误

795、在信息安全领域，CIA通常是指：保密性、完整性和非抵赖性。（B）

A、正确 B、错误

796、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

797、信息安全的威胁主体包括内部人员、准内部人员、外部人员、系统自身等方面。（B）

A、正确 B、错误误

798、互联网网络安全事件根据危害和紧急程度分为一般、预警、报警、紧急、重大五种。 （B）

A、正确 B、错误

799、安全审计是从管理和技术两个方面检查公司的安全策略和控制措施的执行情况，发现安全隐患的过程。（A）

A、正确 B、错误

800、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确 B、错误

801、计算机系统安全是指应用系统具备访问控制机制，数据不被泄露、丢失、篡改等。（B）

A、正确 B、错误

802、主机加固完成后，一般可以有效保证主机的安全性增强。（A）

A、正确 B、错误

803、黑客在进行信息收集时，通常利用Windows的IPC漏洞可以获得系统用户的列表的信 息。（A）

A、正确 B、错误

804、Solaris系统中一般需要确认ROOT账号只能本地登录，这样有助于安全增强。（A）

A、正确 B、错误

805、HP-UX系统加固中在设置ROOT环境变量不能有相对路径设置。（A）

A、正确 B、错误

806、屏幕保护的木马是需要分大小写。（B）

A、正确 B、错误

807、安全审计就是日志的记录。（B）

A、正确 B、错误误

808、HP-UX系统加固中在设置通用用户环境变量不能有相对路径设置。（A）

A、正确 B、错误

809、AIX系统加固时，对系统配置一般需要自编脚本完成。（A）

A、正确 B、错误

810、Windows NT中用户登录域的口令是以明文方式传输的。（B）

A、正确 B、错误

811、操作系统普通用户账号审批记录应编号、留档。（A）

A、正确 B、错误

812、计算机病毒是计算机系统中自动产生的。（B）

A、正确 B、错误

813、主机系统加固时根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。（A）

A、正确 B、错误

814、4A系统的建设能够减轻账户管理员的维护工作。（A）

A、正确 B、错误

815、4A系统的接入管理可以管理到用户无力访问的接入。（B）

A、正确 B、错误

816、Cisco路由器可以使用enable password命令为特权模式的进入设置强壮的密码。（B）

A、正确 B、错误

817、Cisco设备的AUX端口默认是启用的。（A）

A、正确 B、错误

818、DHCP可以向终端提供IP地址、网关、DNS服务器地址等参数。（A）

A、正确 B、错误误

819、Inbound方向的NAT使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际IP地址。（B）

A、正确 B、错误

820、IPS设备即使不出现故障，它仍然是一个潜在的网络瓶颈，需要强大的网络结构来配合。（A）

A、正确 B、错误

821、IPS的过滤器规则不能自由定义。（B）

A、正确 B、错误

822、IPS的某些功能和防火墙类似。（A）

A、正确 B、错误

823、IPS和IDS都是主动防御系统。（B）

A、正确 B、错误

824、NAT是一种网络地址翻译的技术，它能是的多台没有合法地址的计算机共享一个合法的IP地址访问Internet。（A）

A、正确 B、错误

825、Netscreen的ROOT管理员具有的最高权限，为了避免ROOT管理员密码被窃取后造成威胁，应该限制ROOT只能通过CONSOLE接口访问设备，而不能远程登录。(A)

A、正确 B、错误

826、Netscreen防火墙的外网口应禁止PING测试，内网口可以不限制。（B）

A、正确 B、错误

827、OSI是开放的信息安全的缩写。（B）

A、正确 B、错误

828、OSI七层模型中，传输层数据成为段（Segment），主要是用来建立主机端到端连接，包括TCP和UDP连接。（A）

A、正确 B、错误

829、OSI中会话层不提供机密性服务。（A）

A、正确 B、错误

830、SSH使用TCP 79端口的服务。（B）

A、正确 B、错误

831、TCP/IP模型从下至上分为四层：物理层，数据链路层，网络层和应用层。（B）

A、正确 B、错误

832、TCP/IP模型与OSI参考模型的不同点在于TCP/IP把表示层和会话层都归于应用层，所以TCP/IP模型从下至上分为五层：物理层，数据链路层，网络层，传输层和应用层。 （A）

A、正确 B、错误

833、TCP/IP协议体系结构中，IP层对应OSI/RM模型的网络层。（A）

A、正确 B、错误

834、默认情况下需要关闭Cisco设备的Small TCP/UDP服务。（A）

A、正确 B、错误

835、缺省情况下，防火墙工作模式为路由模式，切换工作模式后可直接进行进一步配置。（B）

A、正确 B、错误

836、入侵检测具有对操作系统的校验管理，判断是否有破坏安全的用户活动。（A）

A、正确 B、错误

837、入侵检测可以处理数据包级的攻击。（B）

A、正确 B、错误

838、入侵检测系统不能弥补由于系统提供信息的质量或完整性的问题。（A）

A、正确 B、错误

839、入侵检测系统能够检测到用户的对主机、数据库的网络操作行为。（B）

A、正确 B、错误

840、入侵检测系统是一种对计算机系统或网络事件进行检测并分析这个入侵事件特征的过程。（A）

A、正确 B、错误

841、统计分析的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。（B）

A、正确 B、错误

842、统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。（A）

A、正确 B、错误

843、透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决IP地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的IP的地址。（A）

A、正确 B、错误

844、完整性分析的缺点是一般以批处理方式实现，不用于实时响应。（A）

A、正确 B、错误

845、网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（B）

A、正确 B、错误

846、网络边界的Cisco路由器应关闭CDP服务。（A）

A、正确 B、错误

847、网络边界Cisco设备的CDP协议可以开放。（B）

A、正确 B、错误

848、网络层的防护手段（防火墙，SSL，IDS，加固）可以组织或检测到应用层攻击。（B）

A、正确 B、错误

849、针对不同的攻击行为，IPS只需要一个过滤器就足够了。（B）

A、正确 B、错误

850、主机型IDS其数据采集部分当然位于其所检测的网络上。（B）

A、正确 B、错误

851、状态检测防火墙检测每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。（B）

A、正确 B、错误

852、IPS虽然能主动防御，但是不能坚挺网络流量。（B）

A、正确 B、错误

853、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。（B）

A、正确 B、错误

854、审计系统进行关联分析时不需要关注日志时间。（B）

A、正确 B、错误

855、垃圾邮件一般包括商业广告、政治邮件、病毒邮件、而已欺诈邮件（网络钓鱼）等几个方面。（A）

A、正确 B、错误

856、防止网络窃听最好的方法就是给网上的信息加密，是的侦听程序无法识别这些信息模式。（A）

A、正确 B、错误

857、侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。（A）

A、正确 B、错误

858、模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。（A）

A、正确 B、错误

859、入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。（A）

A、正确 B、错误

860、VPN的主要特点是通过加密是信息安全的通过Internet传递。（A）

A、正确 B、错误

861、传输层协议使用端口号（Port）来标示和区分上层应用程序，如：Telnet协议用的是23号端口、DNS协议使用69号端口。（B）

A、正确 B、错误

862、如果Web应用对URL访问控制不当，可能造成用户直接在浏览器中输入URL，访问不该访问的页面。（A）

A、正确 B、错误

863、如果Web应用没有对攻击者的输入进行适当的编码和过滤，就用于构造数据库查询或操作系统命令时，可能导致注入漏洞。（A）

A、正确 B、错误

864、HTTP协议定义了Web浏览器向Web服务器发生Web页面请求的格式及Web页面在Internet上传输的方式。（A）

A、正确 B、错误

865、HTTP协议是文本协议，可利用回车换行做边界干扰。（A）

A、正确 B、错误

866、Init<sid>.ora文件是Oracle启动文件，任何参数的配置错误都会造成Oracle不能启动，任何参数的不合理配置都可能造成系统故障。（A）

A、正确 B、错误

867、Mysqldump是采用SQL级别的备份机制，它将数据表导成SQL脚本文件，在不同的MySQL版本之间升级时相对比较合适，这也是最常见的备份方法。（A）

A、正确 B、错误

868、Orabrute是进行远程破解Oracle密码的工具，要猜解的密码可以在password.txt中设置。（A）

A、正确 B、错误

869、Oracle的SYS账户在数据库中具有最高权限，能够做任何事情，包括启动/关闭Oracle数据库。即使SYS被锁定，也已然能够访问数据库。（A）

A、正确 B、错误

870、Oracle的若算法加密机制：两个相同的用户名和密码在两个不同的Oracle数据库机器中，将具有相同的哈希值。（A）

A、正确 B、错误

871、Oracle密码允许包含像“SELECT”，“DELETE”，“CREATE”这类的Oracle/SQL关键字。（B）

A、正确 B、错误

872、Oracle的HTTP的基本验证可选择SYS破解，因为它始终存在和有效。（A）

A、正确 B、错误

873、Oracle默认情况下，口令的传输方式是加密。（B）

A、正确 B、错误

874、Oracle数据库的归档日志不是在线日志的备份。（B）

A、正确 B、错误

875、OSI网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。（A）

A、正确 B、错误

876、OSI网络安全体系结构的五类安全服务是鉴别、访问控制、保密性、完整性、抗否认。（A）

A、正确 B、错误

877、SMTP没有对邮件加密的功能是导致垃圾邮件泛滥的主要原因。（A）

A、正确 B、错误

878、SQL Server如果设置了不恰当的数据库文件权限，可能导致敏感文件被非法删除或读取，威胁系统安全。（A）

A、正确 B、错误

879、SQL Server数据库应禁止使用除tcp/ip以外的协议，保护数据库通信安全。（A）

A、正确 B、错误

880、SQL Server应该社会自日志审核无法追踪回溯安全事件。（A）

A、正确 B、错误

881、Web服务器一般省缺不允许攻击者访问Web根目录以外的内容，内容资源不可以任意访问。(A)

882、Web攻击面不仅仅是浏览器中可见的内容。（A）

A、正确 B、错误

883、Web应用对网络通讯中包含的敏感信息进行加密，就不会被窃听。（B）

A、正确 B、错误

884、暴力猜解不能对Web应用进行攻击。（B）

A、正确 B、错误

885、在Oracle自身的配置上做限定方法是：修改$Oracle\_HOME\network\admin目录下面的SQLNET..ORA文件，类似设置如下：

Tcp\_validnode\_checking=YES

Tcp\_invited\_nodes=

(192.168.0.1,ip2,ip3•••...)。

( A )

A、正确 B、错误

886、不设置必要的日志审核，就无法追踪回溯安全事件，Oracle中若果要审计记录成功的登陆语句”SQL>audit session whenever successful;”. ( A )

A、正确 B、错误

887、对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是DNS服务器。（B）

A、正确 B、错误

888、防止XSS各种方法都有优劣之处，防范XSS的真正挑战不在于全免，而在于细致。（B）

A、正确 B、错误

889、访问控制、强制登陆、自动安全更新都属于Window2000的安全组件（B）

A、正确 B、错误

890、复杂的系统存在大量的相互引用访问，如果开发者不能有效的进行权限控制，就可能被恶意引用。（A）

A、正确 B、错误

891、攻击者可以通过SQL注入手段获取其他用户的密码。（A）

A、正确 B、错误

892、几乎所有的关系数据库系统和相应的SQL语言都面临SQL注入的潜在威胁。（A)

A、正确 B、错误

893、简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架（B）

A、正确 B、错误

894、默认可通过Web程序来远程管理Oracle10g数据库，端口是8080.（A）

A、正确 B、错误

895、如果sa是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。（A）

A、正确 B、错误

896、如果在SQL Server等领域成功并不意味这该用户已经可以访问SQL Server上的数据库。（A）

A、正确 B、错误

897、如果知道Oracle密码长度，用Rainbow表生成器来破解其密码哈希值是绝对成功的。（A）

A、正确 B、错误

898、所有操作系统、数据库、网络设备，包括一部分业务系统，均需要支持基于账号的访问控制功能。（B）

A、正确 B、错误

899、网络拓扑分析为检查是否有配置错误项泄露内部IP地址，从而推断网站系统拓扑。（A）

A、正确 B、错误

900、为Oracle数据库安全考虑，在对人共同对数据库进行维护时应依赖数据库预定义的传统角色。（B）

A、正确 B、错误

901、为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。(A)

A、正确 B、错误

902、系统类型鉴别为检查主机系统与开放服务是否存在安全漏点。（B）

A、正确 B、错误

903、系统漏洞扫描为检查目标的操作系统与应用系统信息。（B）

A、正确 B、错误

904、选择远程破解Oracle的最好账户是SYS，因为此账户永远有效。（A）

A、正确 B、错误

905、一封电子邮件可以拆分成对个IP包，每个IP包可以沿不同的路径到达目的地。（A）

A、正确 B、错误

906、一个共享文件夹。将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有读取的权限。（A）

A、正确 B、错误

907、用Sqlplus登陆到Oracle数据库，使用slesct username, password form dba\_users命令可查看数据库中的用户名和密码明文。（B）

A、正确 B、错误

908、有的Web应用登陆界面允许攻击者暴力猜解口令，在自动工具与字典表的帮助下，可以迅速找到弱密码用户。（A）

A、正确 B、错误

909、在Oracle所有版本在安装的时候都没有提示修改SYS的默认密码。（B）

A、正确 B、错误

910、在ORacle数据库安装补丁时，不需要关闭所有与数据库有关的服务。（B）

A、正确 B、错误

911、在SQL Server安装SP3补丁时不需要系统中已经安装了SP1或SP2。（B）

A、正确 B、错误

912、在SQL Server中具有sysadmin权限的用户可以通过xp\_cmdshell存储扩展以system的权限执行任意系统命令。（A）

A、正确 B、错误

913、Oracle默认配置下，每个账户如果有30次的失败登陆，此账户将被锁定。（B）

A、正确 B、错误

914、定制开发Web系统的安全度不如标准的产品。（A）

A、正确 B、错误

915、对MySQL注入攻击时，经常用到注释符号#来屏蔽剩下的内置SQL语句。（A）

A、正确 B、错误

916、一个登录名只能进入服务器，但是不能让用户访问服务器中的数据库资源。每个登录名的定义存放在msater数据库的syslogins表中。（A）

A、正确 B、错误

917、Web错误信息可能泄露服务器型号版本、数据库型号、路径、代码。（A）

A、正确 B、错误

918、Oracle的密码哈希值存储在SYS.USER$表中。可以通过像DBA USERS这类的视图来访问。（A）

A、正确 B、错误

919、产品的定制开发是应用安全中最薄弱的一环。（A）

A、正确 B、错误

920、Oracle限制了密码由英文字母，数字，#，下划线（\_），美元字符（$）构成，密码的最大长度为30字符；并不能以”$”,”#”,”\_”或任何数字开头。（A）

A、正确 B、错误

921、网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。（B）

A、正确 B、错误

922、计算机场地可以选择在公共区域人流量比较大的地方。（B）

A、正确 B、错误

923、EMC测试盒约束用户关心的信息信号的电磁发射、TEMPEST只测试盒约束系统和设备的所有电磁发射。（B）

A、正确 B、错误

924、加密传输是一种非常有效并经常使用的方法，也能解决输入和输出端的电磁信息泄露问题。（B）

A、正确 B、错误

925、出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。（B）

A、正确 B、错误

926、红区：红新号的传输通道或单元电路称为红区，反之为黑区。（A）

A、正确 B、错误

927、机房应设置相应的活在报警和灭火系统。（A）

A、正确 B、错误

928、计算机机房的建设应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。（A）

A、正确 B、错误

929、计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。（B）

A、正确 B、错误

930、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。（A）

A、正确 B、错误

931、提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。（A）

A、正确 B、错误

932、在计算机机房附近施工，不负有维护计算机信息系统安全的责任和义务。（B）

A、正确 B、错误

933、只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。（B）

A、正确 B、错误

934、主管计算机信息系统安全的公安机关和城建及规划部门，应与设施单位进行协调，在不危害用户利益的大前提下，制定措施。合理施工，做好计算机信息系统安全保护工作。（B）

A、正确 B、错误

935、防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。（A）

A、正确 B、错误

936、对于公司机密信息必须根据公司的相关规定予以适当的标识。（A）

A、正确 B、错误

937、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。（A）

A、正确 B、错误

938、如果在电话、电视会议中涉及讨论工伤机密信息，会议主持人或组织人在会议全过程中一定要确认每一个与会者是经授权参与的。（A）

A、正确 B、错误

939、为防止信息非法泄露，需要销毁存储介质时，应该批准后自行销毁。（B）

A、正确 B、错误

940、将公司的机密信息通过互联网络传送时，必须予以加密。（A）

A、正确 B、错误

941、机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。（A）

A、正确 B、错误

942、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式进行保密。（A）

A、正确 B、错误

943、“一次一密”属于序列密码的一种。（A）

A、正确 B、错误

944、3DES算法的加密过程就是用一个秘钥对待加密的数据执行三次DES算法的加密操作。（B）

A、正确 B、错误

945、AES加密算法的秘钥长度为128、192或256位。（A）

A、正确 B、错误

946、AES是一种非对称算法。（B）

A、正确 B、错误

947、DES3和RSA是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。（A）

A、正确 B、错误

948、Diffie-Hellman算法的安全性取决于离散对数计算的困难性，可以实现秘钥交换。（A）

A、正确 B、错误

949、DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。（A）

A、正确 B、错误

950、MD5是一种加密算法。（B）

A、正确 B、错误

951、PGP协议缺省的压缩算法是ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。（A）

A、正确 B、错误

952、PKI是一个用对称密码算法和技术来实现并提供安全服务的具有通用性的安全基础设施。（B）

A、正确 B、错误

953、RC4是典型的的序列密码算法。（A）

A、正确 B、错误

954、RSA算法作为主要的非对称算法，使用公钥加密的秘闻一定要采用公钥来街。（B）

A、正确 B、错误

955、安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。（A）

A、正确 B、错误

956、常见的公钥密码算法有RSA算法、Diffie-Hellman算法和EIGamal算法。（A）

A、正确 B、错误

957、当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（A）

A、正确 B、错误

958、发送方使用AH协议处理数据包，需要对整个IP的数据包计算MAC，包括IP头的所有字段和数据。（B）

A、正确 B、错误

959、分组密码的优点是错误扩展小、速度快、安全程度高。（B）

A、正确 B、错误

960、公共迷药密码体制在秘钥管理上比对称秘钥密码体制更安全。（A）

A、正确 B、错误

961、古典加密主要采用的主要方法是置换，代换。（A）

A、正确 B、错误

962、古典加密主要是对加密算法的保密，现代加密算法是公开的，主要是针对秘钥进行保密。（A）

A、正确 B、错误

963、基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。（A）

A、正确 B、错误

964、口令应在120天至少更换一次。（B）

A、正确 B、错误

965、链路加密方式适用于在广域网系统中应用。（B）

A、正确 B、错误

966、密码保管不善属于操作失误的安全隐患。（B）

A、正确 B、错误

967、日常所见的校园饭卡是利用身份认证的单因素法。（A）

A、正确 B、错误

968、身份认证要求对数据和信息来源进行验证，以确保发信人的身份。（B）

A、正确 B、错误

969、身份认证与权限控制是网络社会的管理基础。（A）

A、正确 B、错误

970、数据在传输过程中用哈希算法保证其完整性后，非法用户无法无法对数据进行任何修改。（B）

A、正确 B、错误

971、数字签名比较的是摘要结果长度是否都是128位。（B）

A、正确 B、错误

972、通信数据与文件加密是同一个概念。（B）

A、正确 B、错误

973、为AES开发的Rijndae1算法的秘钥长度是128位，分组长度也为128位。（B）

A、正确 B、错误

974、为了保证安全性，密码算法应该进行保密。（B）

A、正确 B、错误

975、文件压缩变换是一个单向加密过程。（B）

A、正确 B、错误

976、我的公钥证书不能在网络上公开，否则其他人可能冒充我的身份或伪造我的数字签名。（B）

A、正确 B、错误

977、现代加密算法可以分为对称加密算法和非对称加密。（A）

A、正确 B、错误

978、虚拟专用网VPN的关键技术主要是隧道技术、加解密技术、秘钥管理技术以及使用者与设备身份认证技术。（A）

A、正确 B、错误

979、以当前的技术来说，RSA体制是无条件安全的。（B）

A、正确 B、错误

980、在4A系统的远期建设中，应用系统自身不需要保留系统从账户信息。（B）

A、正确 B、错误

981、在MD5算法中，要先将以初始化的A、B、C、D这四个变量分别复制到a、b、c、d中。（A）

A、正确 B、错误

982、在MD5算法中要用到4个变量，分别表示A、B、C、D，均为32位长。（A）

A、正确 B、错误

983、在PKI中，注册机构RA是必要的组件。（B）

A、正确 B、错误

984、在SSL握手协议过程中，需要服务器发送自己的证书。（A）

A、正确 B、错误

985、在非对称加密过程中，加密和解密使用的是不同的秘钥。（A）

A、正确 B、错误

986、在公钥加密系统中，用公钥加密的密文可以由私钥解密，但用公钥加密的密文，不能用公钥解密。 （B）

A、正确 B、错误

987、在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一种“破解”。 （A）

A、正确 B、错误

988、账户管理的Agent不适用于在网络设备中部署。 （A）

A、正确 B、错误

989、整个PKI系统有证书服务器AS、票据许可服务器TGS、客户机和应用服务器四部分组成。 （B）

A、正确 B、错误

990、最基本的认证方式选择证书是数字证书。（B）

A、正确 B、错误

991、最小特权、纵深防御是网络安全原则之一。（A）

A、正确 B、错误

992、数字证书是由权威机构CA发行的一种权威的电子文档，是网络环境中的一种身份证。（A）

A、正确 B、错误

993、数字证书是由权威机构PKI发行的一种权威性的电子文档，是网络环境中的一种身份证。 （B）

A、正确 B、错误

994、信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段。（A）

A、正确 B、错误

995、病毒能隐藏在电脑的CMOS存储器里。（B）

A、正确 B、错误

996、对感染病毒的软盘进行浏览会导致硬盘被感染。（B）

A、正确 B、错误

997、已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（B）

A、正确 B、错误

998、重新格式化硬盘可以清楚所有病毒。（B）

A、正确 B、错误

999、专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，并根据评估结果提供评估报告。 （A）

A、正确 B、错误

1000、冒充信件回复、假装纯文字ICON、冒充微软雅虎发信、下载电子贺卡同意书、是使用的叫做字典攻击法的方法。（B）

A、正确 B、错误