# 1.Chinese Wall 模型的设计宗旨是：( )。

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

**正确答案：** A

# 2.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( )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

**正确答案：** B

# 3.从风险分析的观点来看，计算机系统的最主要弱点是( )。

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

**正确答案：** B

# 4.当今IT的发展与安全投入，安全意识和安全手段之间形成( )。

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

**正确答案：** B

# 5.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：( )

A、访问控制列表

B、系统服务配置情况

C、审计记录

D、用户账户和权限的设置

**正确答案：** C

# 6.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？( )

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

**正确答案：** D

# 7.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？( )

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

**正确答案：** B

# 8.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、自动软件管理

B、书面化制度

C、书面化方案

D、书面化标准

**正确答案：** A

# 9.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、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

**正确答案：** A

# 10.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、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

**正确答案：** A

# 11.我国的国家秘密分为几级？( )

A、3

B、4

C、5

D、6

**正确答案：** A

# 12.下列哪一个说法是正确的？( )

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

**正确答案：** C

# 13.下面哪项能够提供最佳安全认证功能？( )

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

**正确答案：** B

# 14.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？( )

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

**正确答案：** C

# 15.下面哪一项最好地描述了组织机构的安全策略？( )

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

**正确答案：** A

# 16.下面有关我国标准化管理和组织机构的说法错误的是？( )

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

**正确答案：** C

# 17.信息安全的金三角是( )。

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

**正确答案：** C

# 18.信息安全风险应该是以下哪些因素的函数？( )

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

**正确答案：** A

# 19.信息安全管理最关注的是？( )

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

**正确答案：** C

# 20.信息网络安全的第三个时代是( )

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

**正确答案：** A

# 21.以下哪个不属于信息安全的三要素之一？( )

A、机密性

B、完整性

C、抗抵赖性

D、可用性

**正确答案：** C

# 22.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、制度和措施

B、漏洞分析

C、意外事故处理计划

D、采购计划

**正确答案：** A

# 23.以下哪一种人给公司带来了最大的安全风险？( )

A、临时工

B、咨询人员

C、以前的员工

D、当前的员工

**正确答案：** D

# 24.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？( )

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

**正确答案：** C

# 25.以下人员中，谁负有决定信息分类级别的责任？( )

A、用户

B、数据所有者

C、审计员

D、安全官

**正确答案：** B

# 26.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？( )

A、自下而上

B、自上而下

C、上下同时开展

D、以上都不正确

**正确答案：** B

# 27.在国家标准中，属于强制性标准的是：( )

A、GB/T XXXX-X-200X

B、GB XXXX-200X

C、DBXX/T XXX-200X

D、QXXX-XXX-200X

**正确答案：** B

# 28.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、标准（Standard）

B、安全策略（Security policy）

C、方针（Guideline）

D、流程(Proecdure)

**正确答案：** A

# 29.在许多组织机构中，产生总体安全性问题的主要原因是( )。

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

**正确答案：** A

# 30.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( )。

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

**正确答案：** D

# 31.著名的橘皮书指的是( )。

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）

**正确答案：** A

# 32.重要系统关键操作操作日志保存时间至少保存( )个月。

A、1

B、2

C、3

D、4

**正确答案：** C

# 33.不属于安全策略所涉及的方面是( )。

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

**正确答案：** D

# 34.对MBOSS系统所有资产每年至少进行( )次安全漏洞自评估。

A、1

B、2

C、3

D、4

**正确答案：** A

# 35.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”( )级以上。

A、A级

B、B级

C、C级

D、D级

**正确答案：** C

# 36.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( )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

**正确答案：** B

# 37.《国家保密法》对违法人员的量刑标准是( )。

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

**正确答案：** A

# 38./etc/ftpuser文件中出现的账户的意义表示( )。

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

**正确答案：** A

# 39.Linux系统/etc目录从功能上看相当于Windows的哪个目录？( )

A、program files

B、Windows

C、system volume information

D、TEMP

**正确答案：** B

# 40.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、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

**正确答案：** A

# 41.Linux中，向系统中某个特定用户发送信息，用什么命令？( )

A、wall

B、write

C、mesg

D、net send

**正确答案：** B

# 42.NT/2K模型符合哪个安全级别？( )

A、B2

B、C2

C、B1

D、C1

**正确答案：** B

# 43.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？( )

A、chmod 744 /n2kuser/.profile

B、chmod 755 /n2kuser/.profile

C、chmod 766 /n2kuser/.profile

D、chmod 777 /n2kuser/.profile

**正确答案：** D

# 44.Solaris系统使用什么命令查看已有补丁列表？( )

A、uname –an

B、showrev

C、oslevel –r

D、swlist –l product ‘PH??’

**正确答案：** C

# 45.Unix系统中的账号文件是( )。

A、/etc/passwd

B、/etc/shadow

C、/etc/group

D、/etc/gshadow

**正确答案：** A

# 46.Unix中，哪个目录下运行系统工具，例如sh,cp等？( )

A、/bin/

B、/lib/

C、/etc/

D、/

**正确答案：** A

# 47.Windows nt/2k中的.pwl文件是？( )

A、路径文件

B、口令文件

C、打印文件

D、列表文件

**正确答案：** B

# 48.Windows 2000系统中哪个文件可以查看端口与服务的对应？( )

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

**正确答案：** D

# 49.Windows NT/2000中的.pwl文件是？( )

A、路径文件

B、口令文件

C、打印文件

D、列表文件

**正确答案：** B

# 50.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：( )。

A、木马

B、暴力破解

C、IP欺骗

D、缓冲区溢出攻击

**正确答案：** B

# 51.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( )攻击。

A、缓冲区溢出攻击

B、木马攻击

C、暗门攻击

D、DOS攻击

**正确答案：** D

# 52.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( )。

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

**正确答案：** D

# 53.一般来说，通过web运行http服务的子进程时，我们会选择( )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

**正确答案：** D

# 54.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？( )

A、缓冲区溢出攻击

B、钓鱼攻击

C、暗门攻击

D、DDos攻击

**正确答案：** B

# 55.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？( )

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

**正确答案：** B

# 56.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?( )

A、-/etc/default/login

B、/etc/nologin

C、/etc/shadow

D、var/adm/loginlog

**正确答案：** D

# 57.在Windows 2000中可以察看开放端口情况的是:( )。

A、nbtstat

B、net

C、net show

D、netstat

**正确答案：** D

# 58.周期性行为，如扫描，会产生哪种处理器负荷?( )

A、Idle Ioad

B、Usage Ioad

C、Traffic load

D、以上都不对

**正确答案：** A

# 59.HP-UX系统中，使用( )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

**正确答案：** A

# 60.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?( )

A、惠普

B、Juniper

C、Cisco与Vmware

D、博科Brocade

**正确答案：** C

# 61.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?( )

A、惠普

B、uniper

C、Cisco与Vmware

D、博科Brocade

**正确答案：** B

# 62.网络营业厅提供相关服务的可用性应不低于( )。

A、99.99%

B、99.9%

C、99%

D、98.9%

**正确答案：** A

# 63.Windows NT的安全标识符是由当前时间、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:( )。

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

**正确答案：** D

# 64.下面哪一个情景属于身份验证过程?( )

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

**正确答案：** A

# 65.下列哪一条与操作系统安全配置的原则不符合?( )

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

**正确答案：** D

# 66.关于PPP协议下列说法正确的是:( )。

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)

**正确答案：** C

# 67.接入控制方面，路由器对于接口的要求包括：( )。

A、串口接入

B、局域网方式接入

C、Internet方式接入

D、VPN接入

**正确答案：** D

# 68.拒绝服务不包括以下哪一项？( )。

A、DDoS

B、畸形报文攻击

C、Land攻击

D、ARP攻击

**正确答案：** D

# 69.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：( )。--》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、

**正确答案：** C

# 70.什么命令关闭路由器的finger服务？( )

A、disable finger

B、no finger

C、no finger service

D、no service finger

**正确答案：** C

# 71.实现资源内的细粒度授权，边界权限定义为：( )。

A、账户

B、角色

C、权限

D、操作

**正确答案：** B

# 72.使用TCP 79端口的服务是：( )。

A、telnet

B、SSH

C、Web

D、Finger

**正确答案：** D

# 73.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？( )

A、100.0.0.0

B、172.15.0.0

C、192.168.0.0

D、244.0.0.0

**正确答案：** C

# 74.随着安全要求的提高、技术的演进，( )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

**正确答案：** D

# 75.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：( )

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

**正确答案：** D

# 76.网络安全工作的目标包括：( )。

A、信息机密性

B、信息完整性

C、服务可用性

D、以上都是

**正确答案：** D

# 77.应限制Juniper路由器的SSH( )，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

**正确答案：** A

# 78.应用网关防火墙在物理形式上表现为？( )

A、网关

B、堡垒主机

C、路由

D、交换机

**正确答案：** B

# 79.用于保护整个网络IPS系统通常不会部署在什么位置？( )

A、网络边界

B、网络核心

C、边界防火墙内

D、业务终端上

**正确答案：** D

# 80.有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是( )。

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

**正确答案：** D

# 81.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：( )

A、Web代理

B、端口转发

C、文件共享

D、网络扩展

**正确答案：** B

# 82.域名服务系统（DNS）的功能是( )。

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

**正确答案：** A

# 83.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、TTL

B、源IP地址

C、目的IP地址

D、源IP地址+目的IP地址

**正确答案：** A

# 84.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？( )

A、LAC

B、LNS

C、VPN Client

D、用户自行配置

**正确答案：** B

# 85.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？( )

A、表示层

B、应用层

C、传输层

D、数据链路层

**正确答案：** B

# 86.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、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

**正确答案：** A

# 87.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？( )

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

**正确答案：** D

# 88.在建立堡垒主机时，( )。

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

**正确答案：** A

# 89.在零传输（Zone transfers）中DNS服务使用哪个端口？( )

A、TCP 53

B、UDP 53

C、UDP 23

D、TCP23

**正确答案：** A

# 90.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( )

A、show all access-lists

B、show access-lists

C、show ip interface

D、show interface

**正确答案：** B

# 91.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？( )

A、报文服务拒绝

B、假冒

C、数据流分析

D、报文服务更改

**正确答案：** C

# 92.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？( )

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

**正确答案：** B

# 93.只具有( )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

**正确答案：** A

# 94.主动方式FTP服务器要使用的端口包括( )。

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

**正确答案：** A

# 95.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( )。

A、PPTP

B、L2TP

C、SOCKS v5

D、IPSec

**正确答案：** D

# 96.下列措施不能增强DNS安全的是( )。

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

**正确答案：** C

# 97.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？( )

A、回应的比例

B、被动的防御

C、主动的防御

D、都不对

**正确答案：** D

# 98.下列哪一项能够提高网络的可用性？( )

A、数据冗余

B、链路冗余

C、软件冗余

D、电源冗余

**正确答案：** B

# 99.下列哪一项是arp协议的基本功能？( )

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

**正确答案：** A

# 100.以下哪个属于IPS的功能？( )

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

**正确答案：** A

# 101.以下属于4A策略管理模块可以管理的为( )。

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

**正确答案：** C

# 102.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( )。

A、内容过滤

B、地址转换

C、透明代理

D、内容中转

**正确答案：** C

# 103.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( )。

A、多重安全网关

B、防火墙

C、Vlan隔离

D、物理隔离

**正确答案：** D

# 104.一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、最小特权

B、阻塞点

C、失效保护状态

D、防御多样化

**正确答案：** A

# 105.对于日常维护工作，连接路由器的协议通常使用：( )。

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、HTTP，跨平台，容易搭建

**正确答案：** B

# 106.监听的可能性比较低的是( )数据链路。

A、Ethernet

B、电话线

C、有线电视频道

D、无线电

**正确答案：** B

# 107.网络环境下的security是指( )。

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

**正确答案：** A

# 108.为了保护DNS的区域传送（zone transfer），应该配置防火墙以阻止( )。

1.UDP 2.TCP 3.53 4.52  
A、1,3

B、2,3

C、1,4

D、2,4

**正确答案：** B

# 109.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( )。

A、60%

B、70%

C、80%

D、90%

**正确答案：** C

# 110.交换机转发以太网的数据基于：( )。

A、交换机端口号

B、MAC地址

C、IP地址

D、数据类别

**正确答案：** B

# 111.网络安全的基本属性是( )。

A、机密性

B、可用性

C、完整性

D、以上都是

**正确答案：** D

# 112.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( )。

A、系统分析员

B、程序员

C、数据库管理员

D、操作员

**正确答案：** C

# 113.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。( )

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

**正确答案：** D

# 114.Oracle默认的用户名密码为( )。

A、Scote/tiger

B、root

C、null

D、rootroot

**正确答案：** A

# 115.Oracle中启用审计后，查看审计信息的语句是下面哪一个？( )

A、select \* from SYS.AUDIT$

B、select \* from syslogins

C、select \* from SYS.AUD$

D、AUDIT SESSION

**正确答案：** C

# 116.SQL Server的登录账户信息保存在哪个数据库中？( )

A、model

B、msdb

C、master

D、tempdb

**正确答案：** C

# 117.SQL Sever的默认通讯端口有哪些？( )

A、TCP 1025

B、TCP 1433

C、UDP 1434

D、TCP 14333 E、TCP 445

**正确答案：** B

# 118.SQL Sever中下面哪个存储过程可以执行系统命令？( )

A、xp\_regread

B、xp\_command

C、xp\_cmdshell

D、sp\_password

**正确答案：** C

# 119.SQL数据库使用以下哪种组件来保存真实的数据？( )

A、Schemas

B、Subschemas

C、Tables

D、Views

**正确答案：** C

# 120.SQL语言可以( )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

**正确答案：** B

# 121.不属于数据库加密方式的是( )。

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

**正确答案：** D

# 122.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。( )。

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

**正确答案：** B

# 123.对于IIS日志记录，推荐使用什么文件格式？( )

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

**正确答案：** D

# 124.对于IIS日志文件的访问权限，下列哪些设置是正确的？( )

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）

**正确答案：** D

# 125.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、sys\_ertproc

B、icache\_extproc

C、PLSExtproc

D、extproc

**正确答案：** A

# 126.关系型数据库技术的特征由一下哪些元素确定的？( )

A、行和列

B、节点和分支

C、Blocks和Arrows

D、父类和子类

**正确答案：** A

# 127.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( )？

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

**正确答案：** D

# 128.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、Database Creators

B、System Administrators

C、Server Administrators

D、Security Adiministrators

**正确答案：** A

# 129.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( )？

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

**正确答案：** B

# 130.数据库系统与文件系统的最主要区别是( )。

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

**正确答案：** B

# 131.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( )？

A、SMTP身份认证

B、逆向名字解析

C、黑名单过滤

D、内容过滤

**正确答案：** D

# 132.下列不属于WEB安全性测试的范畴的是( )？

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

**正确答案：** A

# 133.下列关于IIS的安全配置，哪些是不正确的( )？

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

**正确答案：** C

# 134.下列哪些属于WEB脚本程序编写不当造成的( )？

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

**正确答案：** C

# 135.下列哪种工具不是WEB服务器漏洞扫描工具( )？

A、Nikto

B、Web Dumper

C、paros Proxy

D、Nessus

**正确答案：** B

# 136.下列哪项中是数据库中涉及安全保密的主要问题( )？

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

**正确答案：** A

# 137.下面关于IIS报错信息含义的描述正确的是( )？

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

**正确答案：** B

# 138.下面哪一项是与数据库管理员（DBA）职责不相容的( )？

A、数据管理

B、信息系统管理

C、系统安全

D、信息系统规划

**正确答案：** C

# 139.下面选型中不属于数据库安全模型的是( )。

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

**正确答案：** D

# 140.一下不是数据库的加密技术的是( )。

A、库外加密

B、库内加密

C、硬件加密

D、固件加密

**正确答案：** D

# 141.以下几种功能中，哪个是DBMS的控制功能( )？

A、数据定义

B、数据恢复

C、数据修改

D、数据查询

**正确答案：** A

# 142.以下哪个是数据库管理员（DBA）可以行使的职责( )？

A、系统容量规划

B、交易管理

C、审计

D、故障承受机制

**正确答案：** A

# 143.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？( )

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’ --

**正确答案：** B

# 144.以下是对层次数据库结构的描述，请选择错误描述的选项。( )

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

**正确答案：** C

# 145.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。( )

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

**正确答案：** D

# 146.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、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

**正确答案：** A

# 147.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。( )

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

**正确答案：** D

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

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

**正确答案：** C

# 149.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。( )

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

**正确答案：** D

# 150.在Oracle中，将scott的资源文件改为otherprofile，下列哪个是正确的？( )

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

**正确答案：** C

# 151.在Oracle中，用ALTER将scott的口令改为hello，下列哪个是正确的？( )

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

**正确答案：** A

# 152.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( )。

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

**正确答案：** C

# 153.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？( )

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

**正确答案：** C

# 154.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？( )

A、自主性

B、可靠性

C、灵活性

D、数据备份

**正确答案：** D

# 155.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( )。

A、设计型漏洞

B、开发型漏洞

C、运行型漏洞

D、以上都不是

**正确答案：** C

# 156.影响WEB系统安全的因素，不包括？( )

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

**正确答案：** C

# 157.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。( )

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

**正确答案：** D

# 158.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？( )

A、--

B、-

C、-=

D、-+

**正确答案：** B

# 159.以下破解Oracle密码哈希值的步棸，其中哪个描述是错误的？( )

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

**正确答案：** B

# 160.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( )。

A、audit=filename

B、sys=filename

C、event=filename

D、log=filename

**正确答案：** D

# 161.网上营业中间件如果启用了SSl，应采用不低于( )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

**正确答案：** C

# 162.( )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

**正确答案：** A

# 163.《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( )。

A、GA 163-1997

B、GA 267-2000

C、GA 243-2000

D、GB 17859-1999

**正确答案：** B

# 164.使用IIalon灭火的工作原理是什么？( )

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

**正确答案：** C

# 165.被电击的人能否获救，关键在于( )。

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

**正确答案：** D

# 166.电流为( )毫安是，称为致命电流。

A、50

B、100

C、120

D、150

**正确答案：** B

# 167.根据国家相关规定，电压( )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

**正确答案：** D

# 168.关于空气的正向压力，下面哪项描述是正确的？( )

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

**正确答案：** B

# 169.计算机电源系统的所有节点均应镀铅锡处理( )连接。

A、热压

B、冷压

C、焊锡

D、直接

**正确答案：** B

# 170.防雷保安器：防止( )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

**正确答案：** B

# 171.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

**正确答案：** B

# 172.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？ ( )

A、产生静电

B、计算机部件腐蚀

C、有污染物

D、B+A

**正确答案：** B

# 173.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( )。

A、屏蔽配置

B、接地配置

C、分流配置

D、均压配置

**正确答案：** B

# 174.多层的楼房中，最适合做数据中心的位置是( )。

A、楼

B、地下室

C、顶楼

D、除以上外的任何楼层

**正确答案：** D

# 175.区域安全，首先应考虑( )，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

**正确答案：** B

# 176.( )基于IDEA算法。

A、S/MIME

B、SET

C、PGP

D、SSL

**正确答案：** C

# 177.( )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

**正确答案：** C

# 178.( )协议主要用于加密机制。

A、HTTP

B、FTP

C、TELNET

D、SSL

**正确答案：** D

# 179.( )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

**正确答案：** D

# 180.3DES加密算法的密钥长度是：( )。

A、168

B、128

C、56

D、256

**正确答案：** A

# 181.AES算法是哪种算法？( )。

A、对称密钥加密

B、非对称密钥加密

C、哈希算法

D、流加密

**正确答案：** A

# 182.CA指的是( )。

A、证书授权

B、加密认证

C、虚拟专用网

D、安全套接层

**正确答案：** A

# 183.DES算法是哪种算法？( )

A、对称密钥加密

B、非对称密钥加密

C、哈希算法

D、流加密

**正确答案：** A

# 184.DNSSec中并未采用( )。

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

**正确答案：** C

# 185.EC-DSA复杂性的程度是( )。

A、简单

B、最简单

C、困难

D、最困难

**正确答案：** D

# 186.IDEA的密钥长度是多少bit？( )。

A、56

B、64

C、96

D、128

**正确答案：** D

# 187.Kerberos是为TCP/IP网络设计的基于( )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

**正确答案：** B

# 188.Kerberos算法是一个( )。

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

**正确答案：** B

# 189.MD5产生的散列值是多少位？( )。

A、56

B、64

C、128

D、160

**正确答案：** C

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

A、16个

B、32个

C、64个

D、128个

**正确答案：** A

# 191.PKI（公共密钥基础结构）中应用的加密方式为( )。

A、对称加密

B、非对称加密

C、HASH加密

D、单向加密

**正确答案：** B

# 192.PKI无法实现( )。

A、身份认证

B、数据的完整性

C、数据的机密性

D、权限分配

**正确答案：** D

# 193.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( )。

A、他的公钥

B、她的公钥

C、他的私钥

D、她的私钥

**正确答案：** C

# 194.RSA算法建立的理论基础是( )。

A、DES

B、替代想组合

C、大数分解和素数检测

D、哈希函数

**正确答案：** C

# 195.按密钥的使用个数，密码系统可以分为( )。

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

**正确答案：** C

# 196.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？( )。

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

**正确答案：** B

# 197.电路网关防火墙工作在OSI协议的哪一层？( )。

A、传输层

B、链路层

C、应用层

D、物理层

**正确答案：** A

# 198.端对端加密只需要保证消息都在哪里进行加密？( )

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

**正确答案：** A

# 199.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、节点加密

B、链路加密

C、端到端加密

D、DES加密

**正确答案：** A

# 200.高级加密标准AES算法中，加密回合数不可能是( )。

A、10

B、12

C、14

D、16

**正确答案：** D

# 201.公钥加密体制中，没有公开的是( )。

A、明文

B、密文

C、公钥

D、算法

**正确答案：** A

# 202.关于CA和数字证书的关系，以下说法不正确的是( )。

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

**正确答案：** B

# 203.基于私有密钥体制的信息认证方法采用的算法是( )。

A、素数检测

B、非对称算法

C、RSA算法

D、对称加密算法

**正确答案：** D

# 204.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、分组加密技术

C、公钥加密技术

D、单项函数密码技术

**正确答案：** A

# 205.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( )。

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

**正确答案：** B

# 206.链路加密要求必须先对链路两端的加密设备进行( )。

A、异步

B、重传

C、同步

D、备份

**正确答案：** C

# 207.密码分析的目的是什么？( )

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

**正确答案：** A

# 208.如今，DES加密算法面临的问题是( )。

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

**正确答案：** A

# 209.散列算法可以做哪些事？( )。

A、碰撞约束

B、入侵检测

C、组合散列

D、随机数生成器

**正确答案：** C

# 210.数字签名常用的算法有( )。

A、DES算法

B、RSA算法

C、Hash函数

D、AES算法

**正确答案：** B

# 211.数字签名可以解决( )。

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

**正确答案：** D

# 212.数字信封是用来解决( )。

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

**正确答案：** C

# 213.数字证书的应用阶段不包括( )。

A、证书检索

B、证书验证

C、密钥恢复

D、证书撤销

**正确答案：** D

# 214.下列算法中，哪种不是对称加密算法？( )

A、AES

B、DES

C、RSA

D、RC5

**正确答案：** C

# 215.以下对于链路加密哪项是正确的？( )

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

**正确答案：** B

# 216.以下各种加密算法中属于双钥制加密算法的是( )。

A、DES加密算法

B、Caesar替代法

C、Vigenere算法

D、Diffie-Hellman加密

**正确答案：** D

# 217.以下关于CA认证中心说法正确的是( )。

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

**正确答案：** C

# 218.以下关于数字签名说法正确的是( )。

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

**正确答案：** D

# 219.以下哪个不包含在证书中？( )

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

**正确答案：** C

# 220.以下哪项不属于数据库系统实体安全？( )

A、环境安全

B、线路安全

C、设备安全

D、媒体安全

**正确答案：** B

# 221.以下认证方式中，最为安全的是( )。

A、用户名+密码

B、卡+密码

C、用户名+密码+验证码

D、卡+指纹

**正确答案：** D

# 222.在3DES算法中，密钥最高可达到多少位？( )

A、96

B、128

C、168

D、200

**正确答案：** C

# 223.在IPSec中，IKE提供( )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

**正确答案：** B

# 224.在非对称加密算法中，涉及到的密钥个数是？( )

A、一个

B、两个

C、三个

D、三个以上

**正确答案：** B

# 225.在给定的密钥体制中，密钥与密码算法可以看成是( )。

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

**正确答案：** A

# 226.在密码学中，需要被交换的原消息被称为什么？( )

A、密文

B、算法

C、密码

D、明文

**正确答案：** D

# 227.一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：( )

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

**正确答案：** D

# 228.在一个网络节点中，链路加密仅在以下哪项中提供安全性？( )

A、数据链路层

B、物理层

C、通信层

D、通信链路

**正确答案：** D

# 229.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？( )

A、ECC

B、RSA

C、DES

D、D-H

**正确答案：** B

# 230.目前最安全的身份认证机制是( )。

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

**正确答案：** A

# 231.PGP加密算法是混合使用( )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

**正确答案：** B

# 232.如果消息接受方要确定发送方身价，则要使用( )原则。

A、保密性

B、鉴别

C、完整性

D、访问控制

**正确答案：** B

# 233.非对称密码技术的缺点有哪些？( )

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

**正确答案：** B

# 234.以下关于混合加密方式说法正确的是( )。

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

**正确答案：** B

# 235.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？( )

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

**正确答案：** D

# 236.( )的攻击者发生在Web应用层？

A、25%

B、50%

C、75%

D、90%

**正确答案：** C

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

A、Gsrss.exe

B、msbast.exe

C、msblast.exe

D、lsass.exe

**正确答案：** C

# 238.病毒的传播机制主要有哪些？( )

A、移动存储

B、电子邮件

C、网络共享

D、以上均是

**正确答案：** D

# 239.病毒在感染计算机系统时，一般( )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

**正确答案：** B

# 240.蠕虫的目标选择算法有( )。

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

**正确答案：** D

# 241.不属于常见把入侵主机的信息发送给攻击者的方法是( )。

A、E-MAIL

B、UDP

C、ICMP

D、连接入侵主机

**正确答案：** D

# 242.不属于黑客前期收集信息的工具是( )

A、Nmap

B、Xscan

C、Nslookup

D、LC

**正确答案：** D

# 243.常用的抓包软件有( )。

A、Fiddler

B、MS office

C、fluxay

D、netscan

**正确答案：** A

# 244.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？( )

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

**正确答案：** C

# 245.给电脑设置多道口令，其中进入电脑的第一道口令是( )。

A、系统口令

B、CMOS口令

C、文件夹口令

D、文档密码

**正确答案：** B

# 246.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( )。

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

**正确答案：** C

# 247.关于黑客注入攻击说法错误的是： ( )

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

**正确答案：** D

# 248.计算机病毒会对下列计算机服务造成威胁，除了( )。

A、完整性

B、有效性

C、保密性

D、可用性

**正确答案：** C

# 249.什么方式能够从远程绕过防火墙去入侵一个网络？( )

A、IP services\_

B、Active ports

C、Identified network topology

D、Modem banks

**正确答案：** D

# 250.特洛伊木马攻击的威胁类型属于( )。

A、授权侵犯威胁

B、植入威胁

C、渗入威胁

D、旁路控制威胁

**正确答案：** B

# 251.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、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

**正确答案：** A

# 252.下列除了( )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

**正确答案：** B

# 253.下列措施中，( )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

**正确答案：** C

# 254.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？( )

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

**正确答案：** D

# 255.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、Rollback. exe

B、Recover. exe

C、Zap. exe

D、Reset. exe

**正确答案：** A

# 256.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？( )

A、密码

B、加密标志

C、硬件加密

D、加密数据文件

**正确答案：** C

# 257.以下哪项不属于针对数据库的攻击？( )

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

**正确答案：** D

# 258.以下哪项是SYN变种攻击经常用到的工具？( )

A、sessionIE

B、synkill

C、TFN

D、Webscan

**正确答案：** B

# 259.一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？( )

A、访问路径

B、时戳

C、数据定义

D、数据分类

**正确答案：** B

# 260.以下哪一项不属于计算机病毒的防治策略？( )

A、防毒能力

B、查毒能力

C、杀毒能力

D、禁毒能力

**正确答案：** D

# 261.以下哪种工具能从网络上检测出网络监听软件( )

A、sniffdet, ,

B、purify, ,

C、Dsniff

D、WireShark

**正确答案：** A

# 262.下面哪部分不属于入侵的过程？( )

A、数据采集

B、数据存储

C、数据检测

D、数据分析

**正确答案：** B

# 263.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、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

**正确答案：** A

# 264.在确定威胁的可能性时，可以不考虑以下哪项？( )

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

**正确答案：** D

# 265.下面哪一种攻击方式最常用于破解口 令？( )

A、哄骗( spoofing)

B、字典攻击(dictionary attack)

C、拒绝服务(DoS)

D、WinNuk

**正确答案：** B

# 266.下列哪项不是安全编码中输入验证的控制项？( )

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

**正确答案：** D

# 267.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、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

**正确答案：** A

# 268.URL访问控制不当不包括( )

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

**正确答案：** D

# 269.Web应用漏洞按类别进行排名，由多到少正确的顺序为？( )

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

**正确答案：** A

# 270.( )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

**正确答案：** C

# 271.与RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括( )

A、数字签名

B、鉴别机制

C、加密机制

D、数据完整性

**正确答案：** C

# 272.以下哪项数据中涉及安全保密的最主要问题？( )

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

**正确答案：** A

# 273.TCP SYN Flood网络攻击时利用了TCP建立连接过程需要( )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

**正确答案：** C

# 274.以下哪项是计算机网络中用于防止未授权访问的物理安全措施？（ ）

A. 防火墙

B. 加密技术

C. 访问控制

D. 视频监控

**正确答案：** A

# 275.以下哪个是一种常用的对称加密算法？（ ）

A、RSA

B、DES

C、AES

D、SSL

**正确答案：** B

# 276.计算机病毒是一种\_\_\_。（ ）

A、硬件故障

B、操作系统错误

C、恶意软件

D、网络攻击

**正确答案：** C

# 277.以下哪个术语表示将数据转换为无法读取的形式？（ ）

A、加密

B、解密

C、编码

D、压缩

**正确答案：** A

# 278.以下哪个是一种网络攻击手段，攻击者通过伪造IP地址来隐藏自己的真实身份？（ ）

A、DDoS攻击

B、钓鱼攻击

C、中间人攻击

D、IP地址伪造

**正确答案：** D

# 279.以下哪个术语表示将数据从一种形式转换为另一种形式？（ ）

A、加密

B、解密

C、编码

D、压缩

**正确答案：** C

# 280.以下哪项是一种常见的网络攻击，攻击者通过猜测或破解密码来获取未授权访问？（ ）

A、病毒攻击

B、密码攻击

C、拒绝服务攻击

D、钓鱼攻击

**正确答案：** B

# 281.以下哪个术语表示将加密后的数据转换回原始数据？（ ）

A、加密

B、解密

C、编码

D、压缩

**正确答案：** B

# 282.以下哪个是一种常用的非对称加密算法？（ ）

A、RSA

B、DES

C、AES

D、SSL

**正确答案：** A

# 283.以下哪个术语表示在网络通信过程中，数据传输双方使用相同的密钥进行加密和解密？（ ）

A、非对称加密

B、对称加密

C、哈希函数

D、数字签名

**正确答案：** B

# 284.以下哪个是一种网络安全工具，用于检测和报告网络中的漏洞和弱点？（ ）

A、防火墙

B、加密技术

C、访问控制

D、漏洞扫描

**正确答案：** D

# 285.以下哪个术语表示在网络通信过程中，数据传输双方使用不同的密钥进行加密和解密？（ ）

A、非对称加密

B、对称加密

C、哈希函数

D、数字签名

**正确答案：** A

# 286.以下哪项是一种网络攻击手段，攻击者通过篡改或伪造数据来误导接收者？（ ）

A、DDoS攻击

B、钓鱼攻击

C、中间人攻击

D、IP地址伪造

**正确答案：** C

# 287.以下哪个术语表示在网络安全中，对网络资源进行管理和控制以防止未授权访问？（ ）

A、防火墙

B、数据加密

C、访问控制

D、漏洞扫描

**正确答案：** C

# 288.以下哪项是一种网络攻击手段，攻击者通过发送大量请求来使目标服务器瘫痪？（ ）

A、DDoS攻击

B、密码攻击

C、拒绝服务攻击

D、钓鱼攻击

**正确答案：** A

# 289.以下哪个术语表示在网络安全中，用于保护数据传输过程的安全性？（ ）

A、哈希函数

B、加密技术

C、数字签名

D、访问控制

**正确答案：** B

# 290.以下哪个术语表示在网络安全中，用于验证数据完整性和来源的机制？（ ）

A、哈希函数

B、加密技术

C、数字签名

D、访问控制

**正确答案：** D

# 291.以下哪个术语表示在网络安全中，用于验证用户身份的机制？（ ）

A、身份验证

B、访问控制

C、加密技术

D、防火墙

**正确答案：** A

# 292.以下哪项是一种网络攻击手段，攻击者通过利用系统漏洞来获取未授权访问？（ ）

A、DDoS攻击

B、密码攻击

C、中间人攻击

D、漏洞利用

**正确答案：** D

# 293.以下哪个术语表示在网络安全中，用于保护网络设备免受未授权访问的措施？（ ）

A、数据加密

B、物理安全

C、访问控制

D、防火墙

**正确答案：** B

# 294.以下哪个术语表示在网络安全中，用于确保数据在传输过程中不被篡改或伪造的机制？（ ）

A、数字签名

B、哈希函数

C、加密技术

D、访问控制

**正确答案：** A

# 295.以下哪项是一种网络攻击手段，攻击者通过发送恶意软件来感染目标系统？（ ）

A、DDoS攻击

B、病毒攻击

C、拒绝服务攻击

D、钓鱼攻击

**正确答案：** B

# 296.以下哪个术语表示在网络安全中，用于验证数据来源和完整性的技术？（ ）

A、加密技术

B、身份验证

C、数字签名

D、访问控制

**正确答案：** C

# 297.以下哪个术语表示在网络安全中，用于防止网络设备受到物理损害或盗窃的措施？（ ）

A、数据加密

B、网络隔离

C、访问控制

D、物理安全

**正确答案：** D

# 298.在网络安全中，CIA三元素模型指的是哪三个原则？（ ）

A、可用性. 完整性. 保密性

B、机密性. 完整性. 可用性

C、公开性. 完整性. 可用性

D、不可否认性. 完整性. 保密性

**正确答案：** B

# 299.以下哪个原则主要关注保护信息的保密性？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** A

# 300.以下哪个原则主要关注保护信息的完整性？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** B

# 301.以下哪个原则主要关注保护信息的可用性？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** C

# 302.以下哪个原则主要关注确保信息的来源不可否认？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** D

# 303.以下哪个模型是网络安全中的一个重要安全模型？（ ）

A、Bell-LaPadula模型

B、OSI七层模型

C、TCP/IP模型

D、身份验证模型

**正确答案：** A

# 304.以下哪个模型主要关注保护信息的保密性？（ ）

A、Bell-LaPadula模型

B、OSI七层模型

C、TCP/IP模型

D、身份验证模型

**正确答案：** A

# 305.以下哪个模型主要关注保护信息的完整性和保密性？（ ）

A、Bell-LaPadula模型

B、OSI七层模型

C、TCP/IP模型

D、身份验证模型

**正确答案：** B

# 306.以下哪个模型主要关注保护信息的可用性？（ ）

A、Bell-LaPadula模型

B、OSI七层模型

C、TCP/IP模型

D、身份验证模型

**正确答案：** C

# 307.以下哪个模型主要关注保护信息的不可否认性？（ ）

A、Bell-LaPadula模型

B、OSI七层模型

C、TCP/IP模型

D、身份验证模型

**正确答案：** D

# 308.在网络安全中，Bell-LaPadula模型主要关注哪两个原则？（ ）

A、可用性. 完整性

B、机密性. 完整性

C、公开性. 可用性

D、不可否认性. 完整性

**正确答案：** B

# 309.以下哪个术语表示确保信息只能被授权用户访问的安全原则？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** A

# 310.以下哪个术语表示确保信息在传输过程中能够被授权用户访问的安全原则？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** C

# 311.以下哪个术语表示确保信息在传输过程中能够正常使用和访问的安全原则？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** C

# 312.以下哪个术语表示确保信息在传输过程中的来源不可否认的安全原则？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯

**正确答案：** D

# 313.以下哪一个模型是用于描述网络安全策略和规则的？（ ）

A、Bell-LaPadula模型

B、访问控制矩阵

C、OSI七层模型

D、TCP/IP模型

**正确答案：** B

# 314.以下哪一个术语表示在网络安全中，确保信息在传输过程中不被泄露给未授权的用户？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** A

# 315.以下哪一个原则是指在网络安全中，确保信息在传输过程中保持未被篡改的状态？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** B

# 316.以下哪一个模型用于定义如何在网络中保护信息的保密性和完整性？（ ）

A、Bell-LaPadula模型

B、访问控制矩阵

C、OSI七层模型

D、TCP/IP模型

**正确答案：** A

# 317.以下哪一个术语表示在网络安全中，对信息进行加密以保护其保密性？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** A

# 318.以下哪一个术语表示在网络安全中，对信息进行加密以保护其完整性？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** B

# 319.以下哪一个术语表示在网络安全中，对信息进行加密以保护其可用性？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** C

# 320.以下哪一个术语表示在网络安全中，确保信息的来源可以被验证和追溯？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** D

# 321.以下哪一个原则是网络安全中的基本安全原则之一？（ ）

A、机密性

B、公开性

C、可用性

D、不可追溯性

**正确答案：** A

# 322.以下哪一个模型是用于描述如何保护网络系统免受未经授权的访问和攻击的？（ ）

A、Bell-LaPadula模型

B、访问控制矩阵

C、OSI七层模型

D、TCP/IP模型

**正确答案：** A

# 323.以下哪一个术语表示在网络安全中，确保信息在传输过程中保持未被泄露的状态？（ ）

A、机密性

B、完整性

C、可用性

D、可追溯性

**正确答案：** A

# 324.在加密技术中，AES算法支持哪种密钥长度？（ ）

A、128位. 192位. 256位

B、40位. 56位. 128位

C、64位. 80位. 1024位

D、32位. 48位. 64位

**正确答案：** A

# 325.以下哪个是一种非对称加密算法？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** B

# 326.以下哪个是一种单向散列函数，通常用于验证数据的完整性？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** D

# 327.以下哪个是一种对称加密算法？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** C

# 328.在加密技术中，公钥通常用于哪个过程？（ ）

A、加密

B、解密

C、认证

D、散列

**正确答案：** B

# 329.以下哪个是一种安全的加密算法，广泛用于保护网络通信的安全？（ ）

A、AES

B、RSA

C、DES

D、MD5

**正确答案：** A

# 330.以下哪个是一种将数据分割成多个部分，然后对每个部分独立加密的加密技术？（ ）

A、分组加密

B、分发加密

C、分层加密

D、分区加密

**正确答案：** A

# 331.以下哪个是一种常见的对称加密算法，广泛用于保护数据的保密性？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** C

# 332.以下哪个是一种安全的加密算法，它的密钥长度可达到256位？（ ）

A、AES

B、RSA

C、DES

D、MD5

**正确答案：** A

# 333.以下哪个是一种非对称加密算法，它使用两个密钥，一个公钥和一个私钥？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** B

# 334.以下哪个是一种单向散列函数，它将数据转换为一个固定长度的散列值？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** D

# 335.以下哪个是一种常见的加密算法，它使用一个128位. 192位或256位的密钥来加密数据？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** C

# 336.以下哪个是一种非对称加密算法，它由Ron Rivest. Adi Shamir和Leonard Adleman在1977年提出？（ ）

A、DES

B、RSA

C、AES

D、MD5

**正确答案：** B

# 337.以下哪个是一种常见的非对称加密算法，它使用椭圆曲线密码学来确保数据的安全传输？（ ）

A、DES

B、RSA

C、ECC

D、MD5

**正确答案：** C

# 338.抵御电子邮箱入侵措施中，不正确的是（ ）

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

**正确答案：** D

# 339.以下哪个是一种非对称加密算法，它使用两个密钥（公钥和私钥）来确保数据的机密性和完整性？（ ）

A、对称加密

B、非对称加密

C、混合加密

D、公钥加密

**正确答案：** B

# 340.以下哪个是安全性能度量中用于衡量系统安全性的一个重要指标？（ ）

A、安全性

B、可靠性

C、可用性

D、性能

**正确答案：** A

# 341.在安全性能度量中，以下哪个概念涉及到评估系统在受到攻击时的稳定性？（ ）

A、安全性

B、鲁棒性

C、可用性

D、性能

**正确答案：** B

# 342.以下哪个是安全性能度量中用于衡量系统在面对恶意输入时的抵抗能力的一个指标？（ ）

A、鲁棒性

B、脆弱性

C、安全性

D、性能

**正确答案：** A

# 343.在安全性能度量中，以下哪个概念涉及到评估系统在特定时间内处理安全事件的能力？（ ）

A、响应性

B、实时性

C、可用性

D、性能

**正确答案：** B

# 344.以下哪个是安全性能度量中用于衡量系统在正常运行期间受到攻击的风险的一个指标？（ ）

A、安全性

B、可靠性

C、脆弱性

D、性能

**正确答案：** A

# 345.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复正常运行的能力？（ ）

A、恢复性

B、韧性

C、可用性

D、性能

**正确答案：** B

# 346.以下哪个是安全性能度量中用于衡量系统在面临威胁时保持正常运行的能力的一个指标？（ ）

A、安全性

B、稳定性

C、韧性

D、性能

**正确答案：** A

# 347.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保护敏感数据的能力？（ ）

A、保密性

B、完整性

C、可用性

D、性能

**正确答案：** B

# 348.以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持数据完整性的能力的一个指标？（ ）

A、安全性

B、可靠性

C、完整性

D、性能

**正确答案：** A

# 349.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持数据机密性的能力？（ ）

A、保密性

B、完整性

C、可用性

D、性能

**正确答案：** B

# 350.以下哪个是安全性能度量中用于衡量系统在正常运行期间保持数据机密性的能力的一个指标？（ ）

A、安全性

B、可靠性

C、保密性

D、性能

**正确答案：** A

# 351.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复数据机密性的能力？（ ）

A、恢复性

B、韧性

C、保密性

D、性能

**正确答案：** B

# 352.以下哪个是安全性能度量中用于衡量系统在面临威胁时保护数据机密性的能力的一个指标？（ ）

A、安全性

B、稳定性

C、韧性

D、性能

**正确答案：** A

# 353.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保护数据完整性的能力？（ ）

A、保密性

B、完整性

C、可用性

D、性能

**正确答案：** B

# 354.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复数据完整性的能力？（ ）

A、恢复性

B、韧性

C、保密性

D、性能

**正确答案：** B

# 355.以下哪个是安全性能度量中用于衡量系统在面临威胁时保护数据完整性的能力的一个指标？（ ）

A、安全性

B、稳定性

C、韧性

D、性能

**正确答案：** A

# 356.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持数据可用性的能力？（ ）

A、保密性

B、可用性

C、完整性

D、性能

**正确答案：** B

# 357.以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持服务可用性的能力的一个指标？（ ）

A、安全性

B、恢复性

C、韧性

D、性能

**正确答案：** A

# 358.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复正常服务的能力？（ ）

A、恢复性

B、韧性

C、保密性

D、性能

**正确答案：** B

# 359.以下哪个是安全性能度量中用于衡量系统在面临威胁时保持服务可用性的能力的一个指标？（ ）

A、安全性

B、稳定性

C、韧性

D、性能

**正确答案：** A

# 360.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持正常操作的能力？（ ）

A、安全性

B、鲁棒性

C、可用性

D、性能

**正确答案：** B

# 361.以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持正常操作的能力的一个指标？（ ）

A、安全性

B、可靠性

C、鲁棒性

D、性能

**正确答案：** A

# 362.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复正常操作的能力？（ ）

A、恢复性

B、韧性

C、保密性

D、性能

**正确答案：** B

# 363.以下哪个是安全性能度量中用于衡量系统在面临威胁时保持正常操作的能力的一个指标？（ ）

A、安全性

B、稳定性

C、韧性

D、性能

**正确答案：** A

# 364.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持业务连续性的能力？（ ）

A、安全性

B、业务连续性

C、可用性

D、性能

**正确答案：** B

# 365.以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持业务连续性的能力的一个指标？（ ）

A、安全性

B、恢复性

C、业务连续性

D、性能

**正确答案：** A

# 366.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复业务连续性的能力？（ ）

A、恢复性

B、韧性

C、保密性

D、性能

**正确答案：** B

# 367.以下哪个是安全性能度量中用于衡量系统在面临威胁时保持业务连续性的能力的一个指标？（ ）

A、安全性

B、稳定性

C、韧性

D、性能

**正确答案：** A

# 368.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持关键资源安全的能力？（ ）

A、安全性

B、关键资源安全

C、可用性

D、性能

**正确答案：** B

# 369.以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持关键资源安全的能力的一个指标？（ ）

A、安全性

B、恢复性

C、关键资源安全

D、性能

**正确答案：** A

# 370.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击后恢复关键资源安全的能力？（ ）

A、恢复性

B、韧性

C、保密性

D、性能

**正确答案：** B

# 371.以下哪个是安全性能度量中用于衡量系统在面临威胁时保持关键资源安全的能力的一个指标？（ ）

A、安全性

B、稳定性

C、韧性

D、性能

**正确答案：** A

# 372.在安全性能度量中，以下哪个概念涉及到评估系统在遭受攻击时保持系统完整性的能力？（ ）

A、安全性

B、系统完整性

C、可用性

D、性能

**正确答案：** B

# 373.以下哪个是安全性能度量中用于衡量系统在遭受攻击时保持系统完整性的能力的一个指标？（ ）

A、安全性

B、恢复性

C、系统完整性

D、性能

**正确答案：** A

# 374.以下哪个是业务连续性管理的目标之一？（ ）

A、确保业务操作在任何情况下都能持续进行

B、减少员工的工作时间

C、提高系统的安全性

D、降低灾难发生的概率

**正确答案：** A

# 375.以下哪个不是业务连续性计划（BCP）的关键组成部分？（ ）

A、风险评估

B、员工培训

C、应急响应计划

D、数据备份

**正确答案：** B

# 376.以下哪个是业务连续性计划中用于确保关键业务流程在灾难发生后能够继续进行的一项措施？（ ）

A、热备份

B、冷备份

C、实时恢复

D、数据加密

**正确答案：** A

# 377.以下哪个不是灾难恢复计划（DRP）的主要目标？（ ）

A、最小化业务中断时间

B、确保数据的安全和完整性

C、快速恢复系统运行

D、预防灾难的发生

**正确答案：** D

# 378.以下哪个是业务连续性计划中用于在灾难发生后迅速恢复关键业务功能的一项措施？（ ）

A、业务恢复中心

B、数据备份

C、安全审计

D、风险评估

**正确答案：** A

# 379.以下哪个不是灾难恢复计划中常用的恢复策略？（ ）

A、热备份

B、温备份

C、冷备份

D、数据泄露

**正确答案：** D

# 380.向有限的空间输入超长的字符串是哪一种攻击手段？（ ）

A、缓冲区溢出;

B、网络监听；

C、拒绝服务

D、IP欺骗

**正确答案：** A

# 381.以下哪个是业务连续性计划中用于确保在灾难发生后关键业务功能能够持续运行的一项措施？（ ）

A、连续性运营中心

B、数据备份

C、安全审计

D、风险评估

**正确答案：** A

# 382.以下哪个不是灾难恢复计划中常用的恢复时间目标（RTO）的例子？（ ）

A、1小时

B、4小时

C、24小时

D、1周

**正确答案：** D

# 383.以下哪个是业务连续性管理中用于评估组织在灾难发生时可能面临的威胁和风险的一项措施？（ ）

A、风险评估

B、业务影响分析

C、灾难模拟

D、恢复时间目标

**正确答案：** B

# 384.以下哪个是业务连续性计划中用于确保在灾难发生后关键业务功能能够迅速恢复的一项措施？（ ）

A、数据备份

B、恢复点目标

C、安全控制

D、业务恢复时间目标

**正确答案：** B

# 385.以下哪个不是业务连续性管理中常用的术语？（ ）

A、恢复时间目标（RTO）

B、恢复点目标（RPO）

C、业务影响评估（BIA）

D、数据泄露

**正确答案：** D

# 386.在业务连续性管理中，以下哪个步骤通常是首先进行的？（ ）

A、制定BCP

B、测试BCP

C、实施BCP

D、审查BCP

**正确答案：** A

# 387.以下哪个是业务连续性计划中用于在灾难发生后恢复关键业务功能的一个关键要素？（ ）

A、备用设施

B、员工士气

C、业务流程

D、技术基础设施

**正确答案：** A

# 388.以下哪个不是灾难恢复计划中必须考虑的方面？（ ）

A、数据保护

B、系统恢复

C、通信恢复

D、员工休闲活动

**正确答案：** D

# 389.以下哪个是业务连续性管理中用于确定组织关键业务功能的恢复时间的一个目标？（ ）

A、恢复时间目标（RTO）

B、恢复点目标（RPO）

C、业务影响评估（BIA）

D、成本效益分析

**正确答案：** A

# 390.为了防御网络监听，最常用的方法是（ ）

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

**正确答案：** B

# 391.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、拒绝服务

B、文件共享

C、BIND漏洞

D、远程过程调用

**正确答案：** A

# 392.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、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

**正确答案：** A

# 393.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

**正确答案：** D

# 394.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、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

**正确答案：** C

# 395.黑客在攻击中进行端口扫描可以完成（ ）。

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

**正确答案：** D

# 396.在业务连续性管理中，以下哪个步骤通常是最后进行的？（ ）

A、制定BCP

B、审查和更新BCP

C、测试BCP

D、实施BCP

**正确答案：** B

# 397.在制定安全策略时，以下哪个不是考虑的因素？（ ）

A、资产的价值

B、潜在威胁的评估

C、法律和合规要求

D、员工的工作满意度

**正确答案：** D

# 398.SQL 语言的 GRANT 和 REVOKE 语句主要是用来维护数据库的（ ） 。

A、完整性

B、可靠性

C、安全性

D、一致性

**正确答案：** C

# 399.在数据库的安全性控制中，授权的数据对象的（ ） ，授权子系统就越灵活。

A、范围越小

B、约束越细致

C、范围越大

D、约束范围大

**正确答案：** A

# 400.创建 Web 虚拟目录的用途是（ ） 。

A、用来模拟主目录的假文件夹

B、用一个假的目录来避免感染病毒

C、以一个固定的别名来指向实际的路径，当主目录改变时，相对用户而言是不变的

D、以上都不对

**正确答案：** C

# 401.流量分析通常涉及哪些类型的数据？（ ）

A、源和目的IP地址

B、源和目的端口号

C、数据包大小

D、所有上述选项

**正确答案：** B

# 402.以下哪个不是流量分析中常用的技术？（ ）

A、深度包检测（DPI）

B、网络流量镜像

C、数据包嗅探

D、端口扫描

**正确答案：** C

# 403.以下哪个是网络监控中用于识别异常行为的一种技术？（ ）

A、行为分析

B、异常检测

C、入侵防御

D、安全信息与事件管理（SIEM）

**正确答案：** B

# 404.以下哪个不是流量分析中可以采取的预防措施？（ ）

A、限制异常流量

B、增强防火墙规则

C、应用入侵预防系统（IPS）

D、增加员工工作时间

**正确答案：** D

# 405.以下哪个不是流量分析中常用的指标？（ ）

A、传输速率

B、数据包数量

C、员工工作效率

D、数据包大小

**正确答案：** C

# 406.网络监控和流量分析对于哪个方面的网络安全至关重要？（ ）

A、及时发现和响应安全事件

B、提高员工满意度

C、优化网络性能

D、确保业务连续性

**正确答案：** A

# 407.以下哪个是网络监控中用于监控网络活动的一种技术？（ ）

A、数据包嗅探

B、流量分析

C、端口扫描

D、安全事件管理

**正确答案：** B

# 408.以下哪个不是流量分析中可以采取的响应措施？（ ）

A、隔离受感染的设备

B、阻止恶意流量

C、应用安全补丁

D、调整员工工作量

**正确答案：** D

# 409.（ ）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、电子认证

D、电子证书

**正确答案：** B

# 410.在建立网站的目录结构时，最好的做法是（ ） 。

A、将所有的文件最好都放在根目录下

B、目录层次选在 3～5 层

C、按栏目内容建立子目录

D、最好使用中文目录

**正确答案：** A

# 411.不属于常见的危险密码是（ ）

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

**正确答案：** D

# 412.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（)防火墙的特点。（ ）

A、包过滤型

B、应用级网关型

C、复合型防火墙

D、代理服务型

**正确答案：** D

# 413.在每天下午5点使用计算机结束时断开终端的连接属于（ ）

A、外部终端的物理安全

B、通信线的物理安全

C、窃听数据

D、网络地址欺骗

**正确答案：** A

# 414.2003年上半年发生的较有影响的计算机及网络病毒是什么（ ）

A、SARS

B、SQL杀手蠕虫

C、手机病毒

D、小球病毒

**正确答案：** B

# 415.SQL杀手蠕虫病毒发作的特征是什么（ ）

A、大量消耗网络带宽

B、攻击个人PC终端

C、破坏PC游戏程序

D、攻击手机网络

**正确答案：** A

# 416.我国的计算机年犯罪率的增长是（ ）

A、10％

B、160％

C、60%

D、300％

**正确答案：** C

# 417.信息安全风险缺口是指（ ）

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

**正确答案：** A

# 418.人对网络的依赖性最高的时代（ ）

A、专网时代

B、PC时代

C、多网合一时代

D、主机时代

**正确答案：** C

# 419.网络攻击与防御处于不对称状态是因为（ ）

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

**正确答案：** C

# 420.网络攻击的种类（ ）

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

**正确答案：** A

# 421.语义攻击利用的是（ ）

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

**正确答案：** A

# 422.1995年之后信息网络安全问题就是（ ）

A、风险管理

B、访问控制

C、消除风险

D、回避风险

**正确答案：** A

# 423.风险评估的三个要素（ ）

A、政策，结构和技术

B、组织，技术和信息

C、硬件，软件和人

D、资产，威胁和脆弱性

**正确答案：** D

# 424.信息网络安全(风险）评估的方法（ ）

A、定性评估与定量评估相结合

B、定性评估

C、定量评估

D、定点评估

**正确答案：** A

# 425.信息安全中PDR模型的关键因素是（ ）

A、人

B、技术

C、模型

D、客体

**正确答案：** A

# 426.计算机网络最早出现在哪个年代（ ）

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

**正确答案：** B

# 427.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、计算机网络带宽和速度大大提高。

B、计算机网络采用了分组交换技术。

C、计算机网络采用了电路交换技术。

D、计算机网络的可靠性大大提高。

**正确答案：** B

# 428.关于80年代Mirros蠕虫危害的描述,哪句话是错误的？（ ）

A、该蠕虫利用Unix系统上的漏洞传播

B、窃取用户的机密信息，破坏计算机数据文件

C、占用了大量的计算机处理器的时间，导致拒绝服务

D、大量的流量堵塞了网络，导致网络瘫痪

**正确答案：** B

# 429.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？（ ）

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

**正确答案：** C

# 430.下面哪个功能属于操作系统中的安全功能（ ）

A、控制用户的作业排序和运行

B、实现主机和外设的并行处理以及异常情况的处理

C、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

D、对计算机用户访问系统和资源的情况进行记录

**正确答案：** C

# 431.下面哪个功能属于操作系统中的日志记录功能（ ）

A、控制用户的作业排序和运行

B、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

C、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

D、对计算机用户访问系统和资源的情况进行记录

**正确答案：** D

# 432.网络防御中，哪项措施可以减少网络拥塞？（ ）

A、限制访问

B、使用通用账号

C、优化网络路由

D、不限制网络访问

**正确答案：** C

# 433.网络防御中，哪项策略强调在网络遭受攻击时能够快速恢复正常运行？（ ）

A、预防

B、检测

C、响应

D、灾难恢复

**正确答案：** D

# 434.网络防御中，哪项措施有助于防止未授权的远程访问？（ ）

A、实施VPN

B、使用弱密码

C、允许所有流量

D、不限制网络访问

**正确答案：** A

# 435.网络防御中，哪项措施可以提高网络的透明度？（ ）

A、限制访问

B、使用通用账号

C、日志记录和监控

D、不限制网络访问

**正确答案：** C

# 436.信息风险主要是指（ ）

A、信息存储安全

B、信息传输安全

C、信息访问安全

D、以上都正确

**正确答案：** D

# 437.（ ）不是信息失真的原因。

A、信源提供的信息不完全. 不准确

B、信息在编码. 译码和传递过程中受到干扰

C、信宿（信箱）接受信息出现偏差

D、信息在理解上的偏差

**正确答案：** D

# 438.（ ）是用来保证硬件和软件本身的安全的。

A、实体安全

B、运行安全

C、信息安全

D、系统安全

**正确答案：** A

# 439.黑客搭线窃听属于（ ）风险。

A、信息存储安全

B、信息传输安全

C、信息访问安全

D、以上都不是

**正确答案：** B

# 440.（ ）策略是防止非法访问的第一道防线。

A、入网访问控制

B、网络权限控制

C、目录级安全控制

D、属性安全控制

**正确答案：** A

# 441.信息不泄露给非授权的用户. 实体或过程，指的是信息（ ）特性。

A、保密性

B、完整性

C、可用性

D、可控性

**正确答案：** A

# 442.提高 IE 浏览器安全性的措施不包括（ ） 。

A、禁止使用 Cookies

B、禁止 ActiveX 控件

C、禁止使用 Java 及活动脚本

D、禁止访问国外网站

**正确答案：** D

# 443.在（ ）属性对话框中，可以设置几次无效登录后就锁定账户。

A、账户锁定阈值

B、密码策略

C、账户锁定时间

D、复位账户锁定计数器

**正确答案：** A

# 444.Windows Server 2003 系统的安全日志通过（ ）设置。

A、事件查看器

B、服务管理器

C、本地安全策略

D、网络适配器

**正确答案：** C

# 445.（ ）不是 Windows 的共享访问权限。

A、只读

B、完全控制

C、更改

D、读取及执行

**正确答案：** D

# 446.入侵检测系统是对（ ）的合理补充，帮助网络抵御网络攻击。

A、交换机

B、路由器

C、服务器

D、防火墙

**正确答案：** D

# 447.为了保障网络安全，防止外部网络对内部网络的侵犯，多在内部网络与外部网络之间设置（ ） 。

A、密码认证

B、入侵检测

C、数字签名

D、防火墙

**正确答案：** D