**一、单项选择题，【每题1分】**（下列各题中，分别只有一个符合题意的正确答案，请按答题卡要求，用2B铅笔填涂你选定的信息点。本类题共100小题，每小题1分，共100分。多选、错选、不选均不得分。）

301.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

【参考答案】：A

302.有关NTFS文件系统优点的描述中，（ ）是不正确的

A.NTFS可自动地修复磁盘错误

B.NTFS可防止未授权用户访问文件

C.NTFS没有磁盘空间限制

D.NTFS支持文件压缩功能

【参考答案】：C

303.以下那个解决可以帮助减少物理硬件成本？（ ）

A.VCenter Operation Manager for View VCenter视图操作管理

B.Thin Client（精简型计算机）

C.Horizon View Client（地平线视图的客户）

D.Horizon Mirage（地平线海市蜃楼）

【参考答案】：B

304.微软推荐的有关域中组的使用策略是（ ）。

A.A-G-P

B.DL-P

C.A-DL-G-P

D.A-G-DL-P

【参考答案】：D

305.应实现设备特权用户的（ ），系统不支持的应部署日志服务器保证管理员的操作能够被审计，并且网络特权用户管理员无权对审计记录进行操作。

A.权限分离

B.多样性

C.唯一性

D.权限最大化

【参考答案】：A

306.雨天在户外操作电气设备时，操作杆的绝缘部分应有（ ），罩的上口应与绝缘部分紧密结合，无渗漏现象。

A.防雨罩

B.防尘罩

C.防触电罩

D.防抖装置

【参考答案】：A

307.逻辑强隔离装置采用代理模式，也称为（ ）

A.SQL代理

B.TNS代理

C.ORACLE代理

D.OCI代理

【参考答案】：A

308.如果需要创建一个RAID 10的RAID组，至少需要（ ）块硬盘？

A.2

B.3

C.4

D.5

【参考答案】：C

309.下列方法（ ）最能有效地防止不安全的直接对象引用漏洞。

A.检测用户访问权限

B.使用参数化查询

C.过滤特殊字符

D.使用token令牌

【参考答案】：A

310.boot.ini文件是一个文本文件，其作用是（ ）。

A.设置启动项

B.计算机硬件配置

C.用户配置文件

D.以上均不是

【参考答案】：A

311.应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性是否受到破坏，并在检测到完整性错误时采取必要的（ ）措施。

A.修复

B.恢复

C.格式化

D.备份

【参考答案】：B

312.（ ）是因特网中最重要的设备，它是网络与网络连接的桥梁。

A.路由器

B.中继站

C.集线器

D.服务器

【参考答案】：A

313.《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】：B

314.在Windows操作系统中可以通过安装（ ）组件创建FTP站点。

A.IIS

B.IE

C.WWW

D.DNS

【参考答案】：A

315.一个C/S应用系统通过本地命名的方法配置客户端到服务器的连接，客户端和服务器运行在两台电脑上，当从客户端连接数据库时，收到一个TNS错误，检查发现只在服务器上有一个tnsnames.ora文件，拷贝该文件到客户端，客户端能够连接的服务器，下面哪一句描述是正确的？

A.配置本地命名连接tnsnames.ora必须在客户端电脑上

B.为了客户端的连接tnsnames.ora必须从服务器上删除

C.配置本地命名连接tnsnames.ora必须在客户端和服务器端都配置

D.客户端不需要tnsnames.ora文件;这个问题与拷贝该文件到客户端无关

【参考答案】：A

316.以下哪个不属于iis自带的服务（ ）。

A.telnet服务

B.web服务

C.ftp服务

D.smtp服务

【参考答案】：A

317.下面哪种工具不是Windows Server 2003中默认安装的AD管理工具（ ）。

A.ActiveDirectoryuserandcomputer

B.ActiveDirectorySiteandService

C.ActiveDirectorydomainandtrust

D.GPMC

【参考答案】：D

318.下面不属于虚拟化平台的是（ ）。

A.Vmware

B.Hyper-v

C.Citrix

D.DOS

【参考答案】：D

319.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

【参考答案】：B

320.破解双方通信获得明文是属于（ ）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

【参考答案】：A

321.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。

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

【参考答案】：B

322.防火墙能够（ ）。

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.完全防止传送己被病毒感染的软件和文件

【参考答案】：B

323.在取得目标系统的访问权之后，黑客通常还需要采取进一步的行动以获得更多权限，这一行动是（ ）

A.提升权限，以攫取控制权

B.扫描、拒绝服务攻击、获取控制权、安装后门、嗅探

C.网络嗅探

D.进行拒绝服务攻击

【参考答案】：A

324.下列哪一项可以用于查看网络流量并确定网络上所运行的服务？

A.Sniffer

B.IDS

C.防火墙

D.路由器

【参考答案】：A

325.风险评估不包括以下哪个活动?

A.中断引入风险的活动

B.识别资产

C.识别威胁

D.分析风险

【参考答案】：A

326.在"选项"对话框的"文件位置"选项卡中可以设置（ ）。

A.表单的默认大小

B.默认目录

C.日期和时间的显示格式

D.程序代码的颜色

【参考答案】：B

327.下列RAID技术无法提高读写性能的是（ ）。

A.RAID0

B.RAID1

C.RAID3

D.RAID5

【参考答案】：B

328.Windows Server 2003标准版支持的CPU数量为（ ）。

A.4

B.6

C.8

D.12

【参考答案】：A

329.若每次打开Word程序文档时，计算机都会把文档传送到另一台FTP服务器，那么可以怀疑Word程序被黑客植入（ ）。

A.病毒

B.特洛伊木马

C.FTP匿名服务

D.陷门

【参考答案】：B

330.以下对于拒绝服务攻击描述错误的是：

A.通过盗取管理员账号使得管理员无法正常登录服务器

B.通过发送大量数据包导致目标网络带宽拥塞，正常请求无法通过

C.通过发送大量连接请求导致操作系统或应用的资源耗尽，无法响应用户的正常请求

D.通过发送错误的协议数据包引发系统处理错误导致系统崩溃

【参考答案】：A

331.信息安全风险的三要素是指:

A.资产/威胁/脆弱性

B.资产/使命/威胁

C.使命/威胁/脆弱性

D.威胁/脆弱性/使命

【参考答案】：A

332.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

【参考答案】：C

333.依据数据包的基本标记来控制数据包的防火墙技术是

A.包过滤技术

B.应用代理技术

C.状态检侧技术

D.有效载荷

【参考答案】：A

334.溢出攻击的核心是（ ）。

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

【参考答案】：A

335.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（ ）。

A.使用IP加密技术

B.日志分析工具

C.攻击检测和报警

D.对访问行为实施静态、固定的控制

【参考答案】：D

336.信息系统软件本身及其处理的信息在时间、范围和强度上的保密特性描述的系统安全属性是（ ）。

A.机密性

B.完整性

C.可用性

D.可控性

【参考答案】：A

337.绝缘安全工器具应存放在温度-15℃～35℃，相对湿度5%～80%的干燥（ ）的工具室（柜）内。

A.通风

B.密闭

C.封闭

D.阴凉

【参考答案】：A

338.电子邮件客户端通常需要用（ ）协议来发送邮件。

A.仅 SMTP

B.仅 POP

C.SMTP 和 POP

D.以上都不正确

【参考答案】：A

339.DNS在计算机术语中是（ ）？

A.域名服务器

B.邮局协议

C.文件传输服务

D.网页服务器

【参考答案】：A

340.数据安全主要包含（ ）。

A.数据加密和数据解密

B.数据加密和数据恢复

C.数据解密和数据恢复

D.数据存储和数据加密

【参考答案】：B

341.IIS写权限漏洞是由于开启了IIS上的哪项服务引起的（ ）。

A.FastCGI

B.Webdav

C.PHP-fpm

D.IIS URL Rewite

【参考答案】：B

342.设备的硬件维护操作时必须戴（ ）。

A.安全帽

B.安全带

C.防静电手套

D.针织手套

【参考答案】：C

343.公司的WEB服务器受到来自某个IP地址的黑客反复攻击，你的主管要求你通过防火墙来阻止来自那个地址的所有连接，以保护WEB服务器，那么你应该选择哪一种防火墙?（ ）。

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

【参考答案】：A

344.信息系统使用中，当会话控制应在会话处于非活跃一定时间或会话结束后（ ）。

A.终止网络连接

B.关闭计算机

C.关闭服务器

D.关闭数据库

【参考答案】：A

345.公钥密码基础设施PKI解决了信息系统中的问题。

A.身份信任

B.权限管理

C.安全审计

D.加密

【参考答案】：A

346.下面RAID级别中，数据冗余能力最弱的是？（ ）

A.RAID 0

B.RAID 1

C.RAID 3

D.RAID 5

【参考答案】：A

347.严格执行带电作业工作规定，严禁无工作方案或采用未经审定的（ ）进行带电作业工作；严禁使用不合格工器具开展带电作业；严禁约时停用或恢复重合闸。

A.安全措施

B.工作方案

C.工作票

D.运行方式

【参考答案】：B

348.更换部件或设备工作变更时，全程工作必须至少有（ ）人以上参加，工作完成后及时做好维修记录。

A.1

B.2

C.3

D.4

【参考答案】：B

349.不能防范ARP欺骗攻击的是（ ）

A.使用静态路由表

B.使用ARP防火墙软件

C.使用防ARP欺骗的交换机

D.主动查询IP和MAC地址

【参考答案】：A

350.简单包过滤防火墙主要工作在

A.链路层/网络层

B.网络层/传输层

C.应用层

D.会话层

【参考答案】：B

351.A.B类计算机机房的空调设备应尽量采用（ ）。

A.风冷式空调

B.立式的

C.分体的

D.规定中没有要求

【参考答案】：A

352.对DMZ区的描述错误的是（ ）

A.DMZ区内的服务器一般不对外提供服务

B.DMZ功能主要为了解决安装防火墙之后外部网络无法访问内部服务器的问题

C.通过DMZ区可以有效保护内部网络

D.DMZ区位于企业内网和外部网络之间

【参考答案】：A

353.一台需要与互联网通信的 WEB服务器放在以下哪个位置最安全？

A.在DMZ 区

B.在内网中

C.和防火墙在同一台计算机上

D.在互联网防火墙外

【参考答案】：A

354.（ ）加强了WLAN的安全性。它采用了802.1x的认证协议、改进的密钥分布架构和AES加密。

A.802.11i

B.802.11j

C.802.11n

D.802.11e

【参考答案】：A

355.2011年，Skype存在用户端对端加密的密钥直接写在代码里（hardcodedkey）的安全漏洞，由此可知Skype存在（ ）安全漏洞。

A.不安全的加密存储

B.安全配置错误

C.不安全的直接对象引用

D.传输层保护不足

【参考答案】：A

356.数据保密性指的是（ ）。

A.保护网络中各系统之间交换的数据，防止因数据被截获而造成泄密。

B.提供连接实体身份的鉴别

C.防止非法实体对用户的主动攻击，保证数据接收方收到的信息与发送方发送的信息完全移植

D.确保数据是由合法实体发出的

【参考答案】：A

357.下面哪种方法不能够更新针对计算机的组策略设定（ ）。

A.重启机器

B.当前用户重新登陆

C.gpupdate

D.后台更新

【参考答案】：B

358.网络216.12.128.0/24 — 216.12.143.0/24，都经过路由器R接入到骨干网中，为减少骨干网路由器的路由表空间，需将上述网络的路由进行合并，合并后这些网络在骨干路由器的路由表中的地址是：（ ）。

A.216.12.128.0/24

B.216.12.128.0/20

C.216.12.0.0/16

D.216.12.128.0/11

【参考答案】：B

359.计算机病毒是指（ ）。

A.带细菌的磁盘

B.已损坏的磁盘

C.具有破坏性的特制程序

D.被破坏了的程序

【参考答案】：C

360.在上网行为管理设备存储空间耗尽、遭受入侵攻击等异常情况下，上网行为管理设备应采取预防措施，保证已存储的上网行为管理记录数据的（ ）。

A.可靠性

B.可用性

C.连续性

D.有效性

【参考答案】：B

361.公司对各单位互联网流量和应用情况进行监控，在IT运维月报中（ ）公布各单位流量排名靠前的使用情况。

A.定期

B.不定期

C.长期

D.临时

【参考答案】：A

362.终端涉密检查的文件动态监控是指（ ）。

A.在文件的打开和关闭的瞬间对此文档进行检索

B.随机抽取文档进行检索

C.文档拷贝过程中，进行检索

D.对删除文档进行检索

【参考答案】：A

363.由于频繁出现软件运行时被黑客远程攻击获取数据的现象，某软件公司准备加强软件安全开发管理，在下面做法中，对于解决问题没有直接帮助的是（ ）。

A.要求规范软件编码，并制定公司的安全编码准则

B.要求开发人员采用敏捷开发模型进行开发

C.要求所有的开发人员参加软件安全意识培训

D.要求增加软件安全测试环节，尽早发现软件安全问题

【参考答案】：B

364.Internet信息服务在Windows的哪个组件下（ ）。

A.索引服务

B.网络服务

C.应用程序服务器

D.Windows网络服务

【参考答案】：D

365.SA指的是（ ）

A.数字签名算法

B.数字系统算法

C.数字签名协议

D.数字签名协议

【参考答案】：A

366.网络运营者应当对其收集的用户信息严格保密，并建立健全（ ）。

A.用户信息保密制度

B.用户信息保护制度

C.用户信息加密制度

D.用户信息保全制度

【参考答案】：B

367.以下代码中存在（ ）的安全漏洞FormFile theFile = advertiseform.getFilepath（ ）;String up\_path = servlet.getServletContext（ ）.getRealPath（"/"）;if（theFile != null ）{}

A.上传文件漏洞

B.不安全的直接对象引用

C.SQL注入

D.未验证的重定向和转发

【参考答案】：A

368.在下面的NT/2K安全模型的空白处，应该是哪个安全组件？

A.LONGON过程（LP）

B.安全帐号管理（SAM）

C.安全参考监控器（SRM）

D.本地安全授权（LSA）

【参考答案】：B

369.按系统保护（G2）的要求，系统应提供在管理维护状态中运行的能力，管理维护状态只能被（ ）使用。

A.领导

B.机房管理员

C.系统管理员

D.系统操作员

【参考答案】：C

370.（ ）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.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

【参考答案】：A

371.公司总部以及供电局信息运行维护部门每天定时对门户系统进行巡检。检查数据备份是否备份正常：基本配置库和IPP数据库的备份周期为一天（ ）次全备，保留周期为30天。

A.一

B.二

C.三

D.无

【参考答案】：A

372.冯.诺伊曼机工作方式的基本特点是（ ）。

A.多指令流单数据流

B.按地址访问并顺序执行指令

C.堆栈操作

D.存储器按内容选择地址

【参考答案】：B

373.降级容灾是指灾备中心的IT系统在处理能力、可靠性等指标（ ）生产中心。

A.低于

B.相当

C.高于

D.不能衡量

【参考答案】：A

374.不属于信息安全与信息系统的“三个同步”的是（ ）

A.同步管理

B.同步建设

C.同步规划

D.同步投入

【参考答案】：A

375.下列不属于URL的是（ ）。

A.http://www.163.com

B.www.163.com

C.ftp://www.163.com

D.ftp://www.163.com:1000

【参考答案】：B

376.一门课程同时有若干个学生选修，而一个学生可以同时选修多门课程，则课程与学生之间具有（ ）关系。

A.一对一

B.一对多

C.多对多

D.多对一

【参考答案】：C

377.要使用默认选项安装 WSUS，不须在计算机上安装的软件是（ ）。

A.Microsoft Internet 信息服务（IIS）6.0

B.用于 Windows Server 2003 的 Microsoft .NET Framework 1.1 Service Pack 1

C.Background Intelligent Transfer Service（BITS）2.0

D.Microsoft office 2003

【参考答案】：D

378.某单位通过防火墙进行互联网接入，外网口地址为 20210111，内网口地址为 19216811， 这种情况下防火墙工作模式为：

A.透明模式

B.路由模式

C.代理模式

D.以上都不对

【参考答案】：B

379.下列（ ）技术不属于预防病毒技术的范畴。

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

【参考答案】：A

380.网页挂马是指（ ）

A.攻击者通过在正常的页面中（通常是网站的主页）插入一段代码。浏览者在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序，进而控制浏览者的主机

B.黑客们利用人们的猎奇、贪心等心理伪装构造一个链接或者一个网页，利用社会工程学欺骗方法，引诱点击，当用户打开一个看似正常的页面时，网页代码随之运行，隐蔽性极高

C.把木马服务端和某个游戏/软件捆绑成一个文件通过QQ/MSN或邮件发给别人，或者通过制作BT木马种子进行快速扩散

D.与从互联网上下载的免费游戏软件进行捆绑。被激活后，它就会将自己复制到WINDOWS的系统文件夹中，并向注册表添加键值，保证它在启动时被执行

【参考答案】：A

381.在OSPF使用虚拟链路（Virtual link）主要用于那些目的（ ）。

A.在区域0不连续时进行弥补

B.连接一个没有到主干区域直接物理连接的区域

C.测试路由通路

D.A和B

【参考答案】：D

382.关于安全风险，下列说法不正确的是（ ）。

A.物理安全风险包括火灾、水灾、地震等环境事故，造成整个系统毁灭

B.网络层面的安全风险包括系统弱点被暴露而招致攻击

C.主机层面的安全风险包括计算机病毒的侵害

D.应用安全是指用户在网络上运行的业务应用系统、办公应用系统及其他各种在线应用系统的安全。

【参考答案】：B

383.使用数据库的主要目的之一是为了解决数据的（ ）问题。

A.可靠性

B.传输

C.保密

D.共享

【参考答案】：D

384.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

【参考答案】：B

385.目前使用的防病毒软件的作用是（ ）。

A.查出任何已感染的病毒

B.查出并消除任何已感染的病毒

C.消除已感染的任何病毒

D.查出已知名的病毒，消除部分病毒

【参考答案】：D

386.根据灾难恢复演练的深度不同，可以将演练分为三个级别，这三个级别按演练深度由低到高的排序 正确的是

A.系统级演练、业务级演练、应用级演练

B.系统级演练、应用级演练、业务级演练

C.业务级演练、应用级演练、系统级演练

D.业务级演练、系统级演练、应用级演练

【参考答案】：B

387.内容过滤技术的应用领域不包括

A.防病毒

B.网页防篡改

C.防火墙

D.入侵检测

【参考答案】：B

388.在Windows的DOS窗口中键入命令ipconfig/?，其作用是（ ）。

A.显示所有网卡的TCP/IP配置信息

B.显示ipconfig相关帮助信息

C.更新网卡的DHCP配置

D.刷新客户端DNS缓存的内容

【参考答案】：B

389.企业负责人年度业绩考核减项指标及评价标准，各单位提供的信息系统软硬件产品存在恶意漏洞、恶意代码的，每起减\_\_\_分；引起严重后果的，每起减\_\_\_分。（ ）

A.1，3

B.2，4

C.2，5

D.1，4

【参考答案】：B

390.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

【参考答案】：B

391.Windows 系统下，哪项不是有效进行共享安全的防护措施?

A.使用 netshare\\127．0．0．1\c$/delete 命令,删除系统中C$等管理共享,重启系统

B.确保所有的共享都有高强度的密码防护

C.禁止通过"空会话"连接以匿名的方式列举用户、群组、系统配置和注册表键值

D.安装软件防火培阻止外面对共享目录的连接

【参考答案】：A

392.关于屏蔽子网防火墙，下列说法错误的是（ ）。

A.屏蔽子网防火墙是几种防火墙类型中最安全的

B.屏蔽子网防火墙既支持应用级网关也支持电路级网关

C.内部网对于Internet来说是不可见的

D.内部用户可以不通过DMZ直接访问Internet

【参考答案】：D

393.分布式拒绝服务攻击的简称是（ ）

A.DDOS

B.DROS

C.LAND

D.SDOS

【参考答案】：A

394.在安全编码中，应该按照（ ）为应用程序分配数据库访问权限。

A.最小化原则

B.最大化原则

C.优先原则

D.随意原则

【参考答案】：A

395.入侵检测应用的目的：

A.实时检测网络流量或主机事件

B.数据包过滤

C.在发现攻击事件时及时反应

D.A和C

【参考答案】：D

396.以下能有效预防计算机病毒的方法是（ ）。

A.尽可能多的做磁盘碎片整理

B.及时升级防病毒软件

C.及时清理系统垃圾文件

D.把重要文件压缩处理

【参考答案】：B

397.路由器的路由表包括目的地址，下一站地址以及（ ）。

A.时间.距离

B.距离.计时器.标志位

C.路由.距离.时钟

D.时钟.路由

【参考答案】：B

398.RAID6级别的RAID组的磁盘利用率（N：成员盘个数）为（ ）。

A.N/（N-2）

B.1

C.（N-2）/N

D.1/2N

【参考答案】：C

399.信息系统安全中应用安全方面不包括（ ）。

A.安全评估

B.强制访问控制

C.身份鉴别

D.应用通信安全

【参考答案】：B

400.计算机病毒是指编制或者在（ ）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。

A.计算机程序

B.计算机

C.计算机软盘

D.计算机硬盘

【参考答案】：A