**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。）

201.应对信息安全风险的主要目标是什么?

A.消除可能会影响公司的每一种威胁

B.管理风险，以使由风险产生的问题降至最低限度

C.尽量多实施安全措施以消除资产暴露在其下的每一种风险

D.尽量忽略风险，不使成本过高

【参考答案】：B

202.计算机病毒造成的危害是（ ）。

A.破坏计算机系统软件或文件内容

B.造成硬盘或软盘物理破损

C.使计算机突然断电

D.使操作员感染病毒

【参考答案】：A

203.中间件在操作系统、网络和数据库（ ），应用软件的下层，总的作用是为处于自己上层的应用软件提供运行与开发的环境，帮助用户灵活、高效地开发和集成复杂的应用软件。

A.之上

B.之下

C.中间

【参考答案】：A

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2，即a加密成c。这种算法的密钥就是2，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

【参考答案】：A

205.关于OSI参考模型层次划分原则的描述中，错误的是（ ）。

A.各结点都有相同的层次

B.不同结点的同等层具有相同的功能

C.高层使用低层提供的服务

D.同一结点内相邻层之间通过对等协议实现通信

【参考答案】：D

206.使用防毒面具时，空气中氧气浓度不得低于（ ）%，温度为-30～45℃，不能用于槽、罐等密闭容器环境。

A.16

B.17

C.18

D.19

【参考答案】：C

207.在数据库的安全性控制中，为了保护用户只能存取他有权存取的数据。在授权的定义中，数据对象的（ ），授权子系统就越灵活。

A.范围越小

B.范围越大

C.约束越细致

D.范围越适中

【参考答案】：A

208.在 IPsec协议族中，以下哪个协议必须提供验证服务?

A.AN

B.ESP

C.GRE

D.以上都是

【参考答案】：A

209.移动存储介质按需求可以划分为（ ）。

A.交换区和保密区

B.验证区和保密区

C.交换区和数据区

D.数据区和验证区

【参考答案】：A

210.最简单的防火墙是（ ）。

A.路由器

B.以太网桥

C.交换机

D.网卡

【参考答案】：B

211.差异备份、增量备份、完全备份三种备份策略的备份速度由快到慢依次为（ ）。

A.增量备份、差异备份、完全备份

B.差异备份、增量备份、完全备份

C.完全备份、差异备份、增量备份

D.完全各份、增量备份、差异备份

【参考答案】：A

212.以下哪项功能使用快照为物理和虚拟桌面提供回复功能？（ ）

A.Horizon Mirage地平线海市蜃楼

B.vCenter Operations Manager for ViewVCenter视图操作管理

C.vCenter虚拟化中心

D.Horizon View（地平线视图的客户）

【参考答案】：A

213.（ ）技术不能保护终端的安全。

A.防止非法外联

B.防病毒

C.补丁管理

D.漏洞扫描

【参考答案】：A

214.进程管理可把进程的状态分成（ ）3种。

A.提交、运行、后备

B.等待、提交、完成

C.就绪、运行、等待

D.等待、提交、就绪

【参考答案】：C

215.下列哪些选项不属于 NIDS 的常见技术?

A.协议分析

B.零拷贝

C.SYNCookie

D.IP 碎片重组

【参考答案】：B

216.每个用户电话的处理时间不应超过（ ）分钟，如果超过（ ）分钟仍不能解决，除非用户愿意继续，否则应礼貌的告知用户将分派人员进行处理。

A.5，5

B.10，10

C.15，15

D.20，20

【参考答案】：B

217.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

【参考答案】：A

218.对于Windows Server 2003的终端服务，下列描述正确的是（ ）。

A.Windows Server 2003通过终端服务技术，提供两大功能：远程桌面管理、多人同时执行位于终端服务器内的应用程序

B.若安装了终端服务器，则必须配置终端服务授权服务器

C.利用终端服务可以使任何用户对终端服务器进行远程管理

D.最多只允许两个终端客户端访问终端服务器

【参考答案】：A

219.技术访问控制的目的在于通过限制用户对特定资源的访问。在WINDOWS系统中，重要目录不能对（ ）账户开放。

A.everyone

B.users

C.administrator

D.guest

【参考答案】：A

220.NTFS文件系统中,（ ）可以限制用户对磁盘的使用量

A.活动目录

B.磁盘配额

C.文件加密

D.稀松文件支持

【参考答案】：B

221.下列关于防火墙功能的说法最准确的是：

A.访问控制

B.内容控制

C.数据加密

D.查杀病毒

【参考答案】：A

222.下列哪些措施不是有效的缓冲区溢出的防护措施?

A.使用标准的C语言字符串库进进行操作

B.严格验证输入字符串长度

C.过滤不合规则的字符

D.使用第三方安全的字符串库操作

【参考答案】：A

223.数据库是在计算机系统中按照一定的数据模型组织，存储和应用的（ ）。

A.文件的集合

B.程序的集合

C.命令的集合

D.数据的集合

【参考答案】：D

224.下列关于防火墙的主要功能包括：

A.访问控制

B.内容控制

C.数据加密

D.查杀病毒

【参考答案】：A

225.以下不是采用奇偶校验方式作为数据冗余方式的RAID级别是（ ）。

A.RAID 2

B.RAID 3

C.RAID 1

D.RAID 5

【参考答案】：A

226.事件的来源有（ ）。

A.用户电话申报

B.用户事件自助受理

C.系统监控自动报警

D.以上全都是

【参考答案】：D

227.下列对防火墙技术分类描述正确的是

A.防火墙技术一般分为网络级防火墙和应用级防火墙两类

B.防火墙可以分为双重宿主主机体系、屏蔽主机体系、屏蔽子网体系

C.防火墙采取的技术，主要是包过滤、应用网关、子网屏蔽等

D.防火墙可以分为网络防火墙和主机防火墙

【参考答案】：A

228.在某个攻击中，由于系统用户或系统管理员主动泄漏，使得攻击者可以访问系统资源 的行为被称作:

A.社会工程

B.非法窃取

C.电子欺骗

D.电子窃听

【参考答案】：A

229.计算机机房的净高依机房的面积大小而定，一般为（ ）。

A.2--3m

B.2.5--3m

C.2.5—3.2m

D.2.5--3.5m

【参考答案】：C

230.下面关于IIS错误的描述正确的是？（ ）

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

【参考答案】：B

231.所谓网络内的机器遵循同一“协议”就是指：

A.采用某一套通信规则或标准

B.采用同一种操作系统

C.用同一种电缆互连

D.用同一种程序设计语言

【参考答案】：A

232.微软公司的Windows操作系统中，下面哪个是桌面PC操作系统（ ）。

A.WindowsNTServer

B.Windows2000Server

C.WindowsServer2003

D.WindowsXP

【参考答案】：D

233.当内网内没有条件建立dns 服务器，又不想用IP访问网站，应配置（ ）文件

A.hosts

B.sysconfig

C.network

D.hostname

【参考答案】：A

234.信息化建设和信息安全建设的关系应当是:

A.信息化建设的结束就是信息安全建设的开始

B.信息化建设和信息安全建设应同步规划、同步实施

C.信息化建设和信息安全建设是交替进行的，无法区分谁先谁后

D.以上说法都正确

【参考答案】：B

235.《中华人民共和国网络安全法》自（ ）起施行。

A.42681

B.42887

C.42736

D.42705

【参考答案】：B

236.哪种信息收集方法存在风险（ ）。

A.收集目标服务器的whois、nslookup等信息

B.对服务器进行远程漏洞扫描

C.利用baidu、google收集目标服务器的相关信息

D.利用社会工程学原理获取相关管理员的敏感信息

【参考答案】：B

237.Window 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

【参考答案】：B

238.备份策略的调整与修改应首先由应用系统或数据库管理员提出需求，将需要改变的内容如：（ ）、备份时间、备份类型、备份频率和备份保存周期等以书面方式提交给存储系统管理员。（ ）

A.备份内容

B.备份手段

C.备份方法

D.备份效率

【参考答案】：A

239.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

【参考答案】：B

240.关于Unix版本的描述中，错误的是（ ）。

A.IBM的Unix是Xenix

B.SUN的Unix是Solaris

C.伯克利的Unix是UnixBSD

D.HP的Unix是HP-UX

【参考答案】：A

241.事件：指导致或可能导致服务中断或服务质量下降的任一事态，事件包括用户的申告、（ ）、咨询以及监控系统自动产生的告警。

A.故障

B.隐患

C.缺陷

D.故障隐患

【参考答案】：A

242.U 盘病毒的传播是借助 Windows 系统的什么功能实现的？

A.自动播放

B.自动补丁更新

C.服务自启动

D.系统开发漏洞

【参考答案】：A

243.建立全面、完整、有效的信息安全保障体系，必须健全、完善信息安全（ ），这是南方电网公司信息安全保障体系建立的首要任务。

A.管理机构

B.管理组织

C.规章制度

D.发展规划

【参考答案】：B

244.AIX中页面空间不能多于所有磁盘空间的（ ）。

A.0.1

B.0.2

C.0.15

D.0.3

【参考答案】：B

245.下列关于防火墙的说法中错误的是（ ）。

A.防火墙无法阻止来自防火墙内部的攻击

B.防火墙可以防止感染病毒的程序或文件的传输

C.防火墙通常由软件和硬件组成

D.防火墙可以记录和统计网络利用数据以及非法使用数据的情况

【参考答案】：B

246.在RIP中有三个重要的时钟，其中路由无效时钟一般设为（ ）。

A.30秒

B.90秒

C.270秒

D.不确定

【参考答案】：B

247.创建虚拟目录的用途是（ ）。

A.一个模拟主目录的假文件夹

B.以一个假的目录来避免染毒

C.以一个固定的别名来指向实际的路径,这样,当主目录变动时,相对用户而言是不变的

D.以上皆非

【参考答案】：C

248.下列属于C类计算机机房安全要求范围之内的是（ ）。

A.火灾报警及消防设施

B.电磁波的防护

C.防鼠害

D.防雷击

【参考答案】：A

249.SSL协议比IPSEC协议的优势在于：

A.实现简单、易于配置

B.能有效的工作在网络层

C.能支撑更多的应用层协议

D.能实现更高强度的加密

【参考答案】：A

250.NT/2K模型符合哪个安全级别？

A.B2

B.C2

C.B1

D.C1

【参考答案】：B

251.事件管理流程主要角色有：（ ）、一线支持人员、二线支持人员、三线支持人员。

A.事件经理

B.问题经理

C.系统管理员

D.话务员

【参考答案】：A

252.综合布线一般采用什么类型的拓扑结构。

A.总线型

B.扩展树型

C.环型

D.分层星型

【参考答案】：D

253.8个300G的硬盘做RAID 1后的容量空间为（ ）。

A.1.2T

B.1.8T

C.2.1T

D.2.4T

【参考答案】：A

254.下列（ ）不属于计算机病毒感染的特征。

A.基本内存不变

B.文件长度增加

C.软件运行速度减慢

D.端口异常

【参考答案】：A

255.数据备份范围包括（ ）、数据库数据及裸设备数据。

A.文件数据

B.操作系统数据

C.应用系统数据

D.缓存数据

【参考答案】：A

256.下面是恶意代码生存技术是（ ）。

A.三线程技术

B.加密技术

C.变换技术

D.本地隐藏技术

【参考答案】：B

257.计算机产生病毒的原因（ ）。

A.用户程序有错误

B.计算机硬件故障

C.计算机系统软件有错误

D.人为制造

【参考答案】：D

258.对路由器而言，下列（ ）功能是唯一的。

A.路由器捆绑了MAC地址和IP地址

B.路由器接受广播报文，并提供被请求的信息

C.路由器建立了ARP表，描述所有与它相连接的网络

D.路由器对ARP请求作出应答

【参考答案】：C

259.下面哪一项通常用于加密电子邮件消息?

A.S/MIME

B.BIND

C.DES

D.SSL

【参考答案】：A

260.攻击者通过扫描（ ）漏洞，产生大量不可用的Sendmail子进程，导致Sendmail长时间挂起，从而耗尽服务器内存，达到攻击的目的。

A.CGI

B.SMTP

C.RPC

D.DNS

【参考答案】：B

261.如果我们要在一台电脑上安装活动目录服务,应该选择以下哪一种文件系统（ ）。

A.FAT16

B.FAT32

C.NTFS

D.UDF

【参考答案】：C

262.信息系统高危漏洞补丁在漏洞发布（ ） 个工作日之内；中（低）危漏洞补丁在漏洞发布（ ） 个工作日之内，完成补丁制作及自测工作。

A.15，30

B.7，15

C.3，5

D.9，18

【参考答案】：B

263.触犯新刑法 285 条规定的非法侵入计算机系统罪可判处

A.三年以下有期徒刑或拘役

B.1000 元罚款

C.三年以上五年以下有期徒刑

D.10000 元罚款

【参考答案】：A

264.Windows 操作系统的注册表运行命令是：

A.Regsvr32

B.Regedit

C.Regedit．msc

D.Regedit．Mmc

【参考答案】：B

265.信息安全应急预案中对服务器设备故障安全事件描述正确的是（ ）。

A.如能自行恢复，则记录事件即可

B.若数据库崩溃应立即启用备用系统

C.立即联系设备供应商，要求派维护人员前来维修

D.不动服务器设备并立即上报

【参考答案】：B

266.下列说法错误的是（ ）。

A.缓冲区一定会被黑客利用

B.缓冲区溢出是非常危险的漏洞

C.不良的编程习惯容易导致缓冲区溢出

D.堆栈溢出是缓冲区溢出的一种

【参考答案】：A

267.防火墙的基本构件包过滤路由器工作在OSI的哪一层（ ）。

A.物理层

B.传输层

C.网络层

D.应用层

【参考答案】：C

268.以下关于 VPN 说法正确的是：

A.VPN 指的是用户自己租用线路，和公共网络完全隔离的、安全的线路

B.VPN 是用户通过公用网络建立的临时的安全的连接

C.VPN 不能做到信息验证和身份认证

D.VPN 只能提供身份认证、不能提供加密数据的功能

【参考答案】：B

269.下面哪种是兼顾业务与安全的最佳策略（ ）。

A.业务至上，关闭流量过滤

B.在不影响业务的前提下做最大范围的流量过滤

C.在业务受一定范围的情况下做流量过滤

D.安全至上，关闭业务

【参考答案】：B

270.（ ）是物理服务器的虚拟化层，它将处理器、内存、存储器和资源虚拟化（交换机）为多个虚拟机，是vSphere服务器虚拟化基础架构组件

A.ESXI

B.IOS

C.Unix

D.Vmware

【参考答案】：A

271.某单位采购主机入侵检测，用户提出了相关的要求，其中哪条要求是错误的？

A.实时分析网络数据，检测网络系统的非法行为

B.不占用其他计算机系统的任何资源

C.不会增加网络中主机的负担

D.可以检测加密通道中传输的数据

【参考答案】：A

272.下面是关于SCSI（小型计算机标准接口）的叙述，其中错误的是（ ）。

A.SCSI总线上连接的设备，可以是启动设备，也可以是目标设备

B.一个SCSI适配器能通过SCSI总线连接多个外设

C.连接在SCSI总线上的外设可以相互通信，不会加重主机的负担

D.SCSI总线以串行方式传送数据

【参考答案】：D

273.针对操作系统安全漏洞的蠕虫病毒根治的技术措施是（ ）。

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

【参考答案】：B

274.基本磁盘包括（ ）。

A.主分区和扩展分区

B.主分区和逻辑分区

C.扩展分区和逻辑分区

D.分区和卷

【参考答案】：A

275.二进制代码是由（ ）组成的。

A.0 0

B.0 1

C.1 1

D.1 2

【参考答案】：B

276.HTTPS 采用（ ）协议实现安全网站访问。

A.SSL

B.IPsec

C.PGP

D.SET

【参考答案】：A

277.安全防护体系要求建立完善的两个机制是（ ）

A.风险管理机制、应急管理机制

B.风险管理机制、报修管理机制

C.应急管理机制、报修管理机制

D.审批管理机制、报修管理机制

【参考答案】：A

278.下列不是信息安全的目标的是（ ）

A.可靠性

B.完整性

C.机密性

D.可用性

【参考答案】：A

279.在 linux 系统中拥有最高级别权限的用户是：

A.root

B.administrator

C.mail

D.nobody

【参考答案】：A

280.下列4项中，不属于计算机病毒特征的是（ ）。

A.潜伏性

B.传染性

C.激发性

D.免疫性

【参考答案】：D

281.Linux下常用以下哪个命令来查看与目标之间的路由情况（ ）。

A.Tracert

B.Traceroute

C.Nslookup

D.Ping

【参考答案】：B

282.上网行为审计记录内容应保留（ ）天以上。

A.30

B.60

C.90

D.120

【参考答案】：B

283.输入enable，进入防火墙（ ）模式。

A.用户

B.特权

C.关机

D.待机

【参考答案】：B

284.事件管理流程适用于记录、处理、关闭事件，并（ ）整个过程的管理活动。

A.监护

B.负责

C.监督

D.监控

【参考答案】：C

285.入侵检测产品主要还存在（ ）问题。

A.漏报和误报

B.性能低下

C.价格昂贵

D.不实用

【参考答案】：A

286.hash 算法的碰撞是指:

A.两个不同的消息，得到相同的消息摘要

B.两个相同的消息，得到不同的消息摘要

C.消息摘要和消息的长度相同

D.消息摘要比消息长度更长

【参考答案】：A

287.下列哪一项最准确地描述了灾难恢复计划（DRP）应该包括的内容？（ ）

A.硬件，软件，人员，应急流程，恢复流程

B.人员，硬件，备份站点

C.硬件，软件，备份介质，人员

D.硬件，软件，风险，应急流程

【参考答案】：A

288.在设计访问控制模块时，为了简化管理，通常度访问者（ ），避免访问控制列表过于庞大。

A.分类组织成组

B.严格限制数量

C.按访问时间排序，并删除一些长期没有访问的用户

D.不做任何限制

【参考答案】：A

289.以下（ ）不属于防止口令猜测的措施。

A.严格限定从一个给定的终端进行非法认证的次数

B.确保口令不在终端上再现

C.防止用户使用太短的口令

D.使用机器产生的口令

【参考答案】：B

290.上网行为管理设备应至少生成包含事件主体、事件客体、事件发生的日期和时间、事件的结果、（ ）等内容的上网行为管理记录。

A.事件分析

B.事件记录

C.事件经过

D.采取的措施

【参考答案】：D

291.由于信息系统分为五个安全保护等级，其安全保护能力是（ ）。

A.逐级递减

B.逐级增加

C.与等级无关

D.与安全技术和安全管理相关

【参考答案】：B

292.目前，安全认证系统主要采用基本（ ）的数字证书来实现。

A.PKI

B.KMI

C.VPN

D.IDS

【参考答案】：A

293.应实时监视被监控对象的运行状况，逐项核实系统的显示内容，及时发现各种异常信息，对于系统终端发出的（ ），应立即处理。

A.各种声光告警

B.噪音

C.声响

D.辐射

【参考答案】：A

294.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

【参考答案】：D

295.根据《广西电网有限责任公司信息运维服务人员行为规范业务指导书（2015年）》，运维服务人员应在电话振铃（ ）秒完成接听，报出自己工号，“您好，信息服务中心，工号XXX为您服务！”

A.5

B.10

C.15

D.20

【参考答案】：A

296.信息系统因需求变化、发现重大安全漏洞等原因而进行大规模升级后，根据安全防护技术要求，对信息系统主机操作系统和数据库系统重新开展（ ）。

A.攻防演练

B.打补丁

C.安全测评

D.漏洞扫描

【参考答案】：C

297.数据库是由逻辑相关的（ ）组成。

A.记录

B.文件

C.数据

D.信息

【参考答案】：B

298.下列哪一项与数据库的安全有直接关系

A.访问控制的粒度

B.数据库的大小

C.关系表中属性的数量

D.关系表中元组的数量

【参考答案】：A

299.南方电网一体化风险评估工作采用两种评估方式进行，具体是（ ）。

A.现场评估和远程评估

B.系统评估和设备评估

C.风险评估和安全管理审核

D.综合评估和技术测试

【参考答案】：A

300.下列（ ）不是信息安全CIA三要素。

A.可靠性

B.机密性

C.完整性

D.可用性

【参考答案】：A