**二、多项选择题，【每题1分】**（下列各题中，分别有两个或两个以上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题，每小题1分，共100分。多选。错选、不选均不得分。）

201.具备扩展性的存储架构有

A.DAS

B.NAS

C.SAN

D.IPSAN

【参考答案】：BCD

202.影响网络安全的因素包括（ ）

A.信息处理环节存在不安全的因素

B.计算机硬件有不安全的因素

C.操作系统有漏洞

D.黑客攻击

【参考答案】：ACD

203.虚拟机可获取其所运行主机的 （ ）。

A.CPU资源

B.内存资源

C.存储资源

D.网络资源

【参考答案】：ABCD

204.防范IP欺骗的技术包括（ ）

A.反查路径RPF，即针对报文源IP反查路由表

B.针对报文的目的IP查找路由表

C.IP与MAC绑定

D.部署入侵检测系统

【参考答案】：AC

205.linux支持哪些编程语言（ ）。

A.Perl

B.Python

C.C++

D.Fortran

【参考答案】：ABCD

206.防火墙的缺陷主要有（ ）

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

【参考答案】：ABCD

207.《网络与信息安全事件及预警分类分级规范》按照网络与信息安全突发事件的危害程度、影响范围和造成的损失，将公司网络与信息安全突发事件分为：（ ）。

A.特别重大突发事件（Ⅰ级）

B.重大突发事件（Ⅱ级）

C.较大突发事件（Ⅲ级）

D.一般突发事件（Ⅳ级）

【参考答案】：ABCD

208.系统管理角色是信息安全运行角色之一，负责操作系统、数据库等系统的安全运维和监管，其主要职责包括：（ ）。

A.设计操作系统、数据库等系统的安全管理制度、安全策略及配置

B.负责操作系统、数据库等系统的日常运维管理

C.负责操作系统、数据库等系统的安全运行监控，包括升级、加固、漏洞扫描、日志审计等

D.负责操作系统、数据库等系统的应急处置及定期提交操作系统、数据库等系统安全运行报告

【参考答案】：ABCD

209.信息机房及其办公场地应选择在具有（ ）、（ ）和（ ）等能力的建筑内。

A.防震

B.防风

C.防雨

D.防火

【参考答案】：ABC

210.系统上线前，设计研发单位应回收所有开发过程中使用的（ ）等临时账号及权限。

A.特权用户

B.测试账户

C.用户账户

D.超级管理员

【参考答案】：ABD

211.2017年深入开展等级保护“回头看”工作，梳理核查系统定级备案情况和安全防护情况，对归属、设施、业务发生变化的系统开展（ ）整改。

A.重新备案

B.重新评估

C.重新审查

D.重新认定

【参考答案】：ABC

212.设备验收内容包括（ ）。

A.设备开箱验收

B.加电测试验收

C.设备集成运行验收

D.设备功能验收

【参考答案】：ABCD

213.需要读写校验盘的RAID技术有（ ）。

A.RAID50

B.RAID6

C.RAID3

D.RAID5

【参考答案】：ABCD

214.无条件共享的数据是指可以直接提供给公司内部所有单位的数据。无条件共享的数据不得涉及任何（ ）、（ ）、（ ）。

A.商业机密

B.敏感数据

C.主数据

D.隐私数据

【参考答案】：ABD

215.下列防止电脑病毒感染的方法，正确的是（ ）

A.不随意打开来路不明的电子邮件

B.不用硬盘启动

C.不用来路不明的程序

D.使用杀毒软件

【参考答案】：ACD

216.网络安全保障包括（ ）

A.技术保障

B.管理保障

C.人员培训保障

D.法律法规保障

【参考答案】：ABCD

217.下列能防止不安全的加密存储的是（ ）

A.存储密码是，用SHA-256等健壮哈希算法进行处理

B.使用足够强度的加密算法

C.产生的密钥不应与加密信息一起存放

D.严格控制对加密存储的访问

【参考答案】：ABCD

218.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）》，将IT运维服务对象分为（ ）

A.关键用户

B.重要用户

C.普通用户

D.一般用户

【参考答案】：ABCD

219.计算机病毒能够（ ）

A.破坏计算机功能或者破坏数据

B.影响计算机使用

C.能够自我复制

D.感染计算机使用者

【参考答案】：ABC

220.关于防火墙说法正确的是（ ）

A.防火墙可以防止所有病毒通过网络传播

B.防火墙可以由代理服务器实现

C.所有进出网络的通信流都应该通过防火墙

D.防火墙可以过滤所有的外网访问

【参考答案】：BCD

221.计算机信息系统的安全保护,应当保障（ ）。

A.计算机及其相关的配套设施、设备（含网络）的安全

B.计算机操作人员的安全

C.计算机运行环境的安全

D.计算机信息的安全

E.计算机数据的安全

【参考答案】：ACDE

222.南网云云上数据的数据安全防护措施包括（ ）

A.数据加密

B.脱敏

C.操作安全审计

D.数据传输

【参考答案】：ABC

223.以下对MAC地址的描述正确的是（ ）。

A.由32位二进制数组成

B.由48位二进制数组成

C.前6位十六进制由IEEE负责分配

D.前6位十六进制由IEEE负责分配

【参考答案】：BC

224.网络按通信方式分类，可分为（ ）。.

A.点对点传输网络

B.广播式传输网络

C.数据传输网络

D.对等式网络

【参考答案】：AB

225.值班人员应做好值班日志，值班日志内容包括：（ ）等。

A.值班运行日志

B.重要操作记录

C.告警处理记录

D.故障处理记录

【参考答案】：ABCD

226.以下哪些网络行为涉嫌侵犯个人隐私？（ ）

A.未经许可，在网上公开个人姓名、肖像、住址和电话号码

B.非法获取他人财产状况或未经本人允许在网上公布

C.偷看他人邮件，窃取他人私人文件内容，并将其公开

D.非法调查他人社会关系并在网上发布

【参考答案】：ABCD

227.公司秘密包括（ ）两类。

A.商业秘密

B.个人秘密

C.工作秘密

D.部门文件

【参考答案】：AC

228.下列属于配置存储安全要求的是（ ）

A.避免在WEB目录使用配置文件，以防止可能出现的服务器配置漏洞导致配置文件被下载

B.避免以纯文本形式存储重要配置，如数据库连接字符串或账户凭证

C.通过加密确保配置的安全，并限制对包含加密数据的注册表项，文件或表的访问权限

D.确保对配置文件的修改、删除和访问等权限的变更。都验证授权并且详细记录

【参考答案】：ABCD

229.在日常的信息生活中，对于病毒的防治，正确的是（ ）。

A.不要随便复制和使用盗版软件

B.及时对数据文件进行备份

C.定期对计算机系统进行病毒检查

D.不用关注最新的病毒报告和病毒发作预告

【参考答案】：ABC

230.擦亮1000号回访可采用电话或短信方式开展，每次选择以下（ ）等问题中2个问题回访，并记录用户意见和建议。

A.请问服务人员是否穿工装？

B.请问服务人员是否佩戴工牌？

C.请问服务人员用语是否礼貌？

D.您是否看到1000号宣传屏保？

【参考答案】：ABCD

231.电压过高的影响有哪些？（ ）

A.设备不能正常工作

B.造成危险

C.降低工作强度

D.无影响

【参考答案】：AB

232.软件访问控制主要包括（ ）部分

A.用户管理

B.用户认证

C.会话控制

D.授权控制

【参考答案】：ABCD

233.对mssql进行安全配置正确的是（ ）。

A.禁用sql端口的外部访问

B.禁用xp\_cmdshell等危险扩展命令

C.sa用户弱口令且Mssql端口对外开放

D.安装时选择的安全模式应为sql和windows混合安全模式

E.启用sql端口的外部访问

【参考答案】：ABD

234.属于第二层隧道协议的是（ ）

A.PPTP

B.L2TP

C.L2F

D.SSL

【参考答案】：ABC

235.关于网络安全事件管理和应急响应，以下说法正确的是（ ）

A.应急响应是指组织为了应对突发／重大网络安全事件的发生所做的准备，以及在事件发生后所采取的措施

B.应急响应方法，将应急响应管理过程分为遏制、根除、处置、恢复、报告和跟踪6个阶段

C.对网络安全事件的分级主要参考信息系统的重要程度、系统损失和社会影响三方面因素

D.根据网络安全事件的分级参考要素，可将网络安全事件划分为4个级别：特别重大事件(Ⅰ级)、重大事件(Ⅱ级)、较大事件(Ⅲ级)和一般事件(Ⅳ级)

【参考答案】：ACD

236.程序默认情况下应对所有的输入信息进行验证，不能通过验证的数据应会被拒绝，以下输入需要进行验证的是（ ）

A.HTTP请求消息

B.第三方接口数据

C.不可信来源的文件

D.临时文件

【参考答案】：ABCD

237.文件操作中应对上传文件进行限制，下列操作中（ ）能对上传文件进行限制

A.上传文件类型应遵循最小化原则，仅准许上传必须的文件类型

B.上传文件大小限制，应限制上传文件大小的范围

C.上传文件保存路径限制，过滤文件名或路径名中的特殊字符

D.应关闭文件上传目录的执行权限

【参考答案】：ABCD

238.IPV4由那几部分组成（ ）

A.网络号

B.主机号

C.主机数量

D.地址长度

【参考答案】：AB

239.VPN通常用于建立（ ）之间的安全通道

A.总部与分支机构

B.与合作伙伴

C.与移动办公用户

D.与外部网站

【参考答案】：ABC

240.设计研发单位应严格按照公司软件著作权管理要求及时进行软件著作权资料的移交，并确保提交资料的（ ），确保提交代码与安全测试通过代码版本一致。

A.真实性

B.完整性

C.保密性

D.可用性

【参考答案】：AB

241.属于常见的木马伪装手段的是（ ）

A.修改图标

B.捆绑文件

C.修改文件名

D.删除所有文件

【参考答案】：ABC

242.下面属于对称算法的是（ ）

A.DES算法

B.序列算法

C.RSA算法

D.AES算法

【参考答案】：ABD

243.南方电网公司安全防护对象主要包括（ ）。.

A.计算环境

B.区域边界

C.网络与基础设施

D.网络安全设备

【参考答案】：ABC

244.计算机病毒的传播途径有（ ）。

A.存储介质

B.点对点通信系统

C.计算机网络

D.无线通道

【参考答案】：ABCD

245.除《网络安全法》第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：（ ）

A.设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查

B.定期对从业人员进行网络安全教育、技术培训和技能考核

C..对重要系统和数据库进行容灾备份

D.制定网络安全事件应急预案，并定期进行演练；E.法律、行政法规规定的其他义务

【参考答案】：ABCD

246.VPN技术采用的主要协议包括（ ）

A.IPSec

B.PPTP

C.WEP

D.L2TP

【参考答案】：ABD

247.《电力安全事故应急处理和调查处理条例》（国务院令第599号）事故报告应当包括下列内容（ ）。

A.事故发生的时间、地点（区域）以及事故发生单位

B.已知的电力设备、设施损坏情况，停运的发电（供热）机组数量、电网减供负荷或者发电厂减少出力的数值、停电（停热）范围

C.事故原因的初步判断

D.事故发生后采取的措施、电网运行方式、发电机组运行状况以及事故控制情况

【参考答案】：ABCD

248.我国实施网络通信管制措施非常严肃和谨慎，需具备的条件包括：（ ）

A.必须是为了处置重大突发社会安全事件的需要

B.处置的范围是特定区域，且是临时性措施

C.实施网络通信管制须经国务院决定或批准

D.实施网络通信管制须经省级以上人民政府决定或批准

【参考答案】：ABCD

249.静电对电子产品产生损害的特点有（ ）。

A.吸尘

B.放电破坏

C.放电产生热

D.放电产生电磁场（电磁干扰）

【参考答案】：ABCD

250.AIXIBMINFORMIX数据库备份分为（ ）和（ ）。

A.系统备份

B.逻辑日志备份

C.指令备份

D.操作备份

【参考答案】：AB

251.如何正确地使用防静电手套：（ ）。

A.佩戴时手要清洁，干燥

B.使用后，清洁手套

C.放到适当的地方储存

D.定期更换

【参考答案】：ABCD

252.属于社会工程学在安全意识培训方面进行防御的措施是（ ）

A.构建完善的技术防御体系

B.知道什么是社会工程学攻击

C.知道社会工程学攻击利用什么

D.有效的安全管理体系和操作

【参考答案】：BC

253.杀毒软件可以杀掉的病毒是（ ）

A.只读型光盘上的病毒

B.硬盘上的病毒

C.软盘上的病毒

D.U盘上的病毒

【参考答案】：BCD

254.下列操作中，（ ）可能清除文件型计算机病毒。

A.删除感染计算机病毒的文件

B.格式化感染计算机病毒的磁盘

C.将感染计算机病毒的文件更名

D.用杀毒软件进行清除

【参考答案】：ABD

255.在信息系统联网测试期间不得采用真实业务数据。如因联网测试发生安全事件，将追究（ ）相关责任。

A.信息通信系统业务主管部门

B.信息通信系统运维单位

C.信息通信系统研发单位

D.信息通信系统测评单位

【参考答案】：ABC

256.下列属于输入验证方法的是（ ）

A.检查数据是否符合期望的类型

B.集成数据是否符合期望的长度

C.检查数值数据是否符合期望的数值范围

D.集成数据是否包含特殊字符

【参考答案】：ABCD

257.以下不属于输入设备的是（ ）。

A.显示器

B.打印机

C.扫描仪

D.显示卡

E.键盘

【参考答案】：ABD

258.linux中，echo命令可以用来显示（ ）。

A.参数

B.文本字符

C.过滤内容

D.shell变量

【参考答案】：BD

259.信息机房UPS设备日常检查事项包括（ ）。

A.检查控制面板

B.设备有误异常噪声

C.检查风扇是否运行正常

D.检查设备电压是否正常

【参考答案】：ABCD

260.为防止主机器件的损坏，主机启动后不正确的操作是（ ）。

A.拔不需的系统部件

B.插所需的系统部件

C.不可插系统部件

D.不可拔系统部件

【参考答案】：AB

261.32位微机是指他所用的CPU是（ ）。

A.一次能处理32位二进制数

B.能处理32位十进制数

C.只能处理32位二进制定点数

D.一次能处理4字节二进制数

【参考答案】：AD

262.下面属于SOCKS的组成部分包括（ ）：

A.运行在防火墙系统上的代理服务器软件包

B.链接到各种网络应用程序的库函数包

C.SOCKS服务程序

D.SOCKS客户程序

【参考答案】：ABCD

263.计算机中常用的指令类型有（ ）。

A.数据操作指令

B.数据传送指令

C.十进制运算指令

D.程序控制指令

E.八进制运算指令

【参考答案】：ABD

264.以下属于防火墙类型的有（ ）。

A.软件防火墙

B.液态防火墙

C.硬件防火墙

D.空气防火墙

E.三层防火墙

【参考答案】：AC

265.目前防火墙用来控制访问和实现站点安全策略的技术包括（ ）。

A.服务控制

B.方向控制

C.用户控制

D.行为控制

E.资产控制

【参考答案】：ABCD

266.公司和社会在网络空间上建立了广泛的联系，特别是智能电表和自动缴费的业务应用，使用户大量增加。用户接入网络所带来的（ ）等各类安全风险不断扩大，安全责任的落实更加复杂，《网络安全法》也对保障客户信息安全提出了严格要求。

A.权限

B.内容

C.数据

D.操作

【参考答案】：ABCD

267.计算机信息系统安全保护的目标是要保护计算机信息系统的（ ）

A.实体安全

B.运行安全

C.网络安全

D.人员安全

【参考答案】：ABCD

268.网络运营者，是指（ ）。

A.网络运维者

B.网络所有者

C.网络服务提供者

D.网络管理者

【参考答案】：BCD

269.下列RAID组中需要的最小硬盘数为3个的是（ ）。

A.RAID1

B.RAID3

C.RAID5

D.RAID10

【参考答案】：BC

270.常用查看系统各项设备信息命令，正确的是（ ）。

A.#ioscan–fn列出各I/O卡及设备的所有相关信息：如逻辑单元号，硬件地址及设备文件名等

B.#ps–ef列出正在运行的所有进程的各种信息：如进程号及进程名等

C.#netstat–rn列出网卡状态及路由信息等

D.#lanscan列出网卡状态及网络配置信息

【参考答案】：ABCD

271.防火墙的审计，包括对防火墙的（ ）、（ ）和操作内容的审计。

A.系统日志

B.登陆

C.设备状态

D.操作权限

【参考答案】：AB

272.下列属于安全协议的是（ ）

A.SSL

B.ICMP

C.VPN

D.HTTPS

【参考答案】：ACD

273.属于常见的操作系统安全机制的是（ ）

A.隐蔽信道分析

B.安全审计

C.内容安全

D.最小特权管理

【参考答案】：BCD

274.恶意二维码一般出现在（ ）

A.微信

B.微博

C.QQ

D.论坛

【参考答案】：ABCD

275.VLAN的实现途径有（ ）

A.基于端口的VLAN

B.基于MAC地址的VLAN

C.基于IP地址的VLAN

D.基于主机名的VLAN

【参考答案】：ABC

276.下列属于安装Windows2003 Server系统前准备的工作和注意事项是（ ）。

A.备份当前重要数据文件

B.检查BIOS和Windows2003的兼容性

C.禁用磁盘镜像

D.规划主分区的空间

【参考答案】：ABCD

277.二级系统和三系统均应满足以下安全加固的控制要求：

A.按照安全策略对操作系统和数据库进行安全配置检查与设置

B.对设备的管理采用安全的SSH，HTTPS代替不安全的Telnet及HTTP管理方式

C.关闭系统中不必要的服务和端口及定期进行系统安全补丁的更新

D.制定用户安全策略，包括制定用户登录超时策略、口令复杂度及生存周期策略、帐号锁定策略等

【参考答案】：ABCD

278.下列RAID技术中可以提高可靠性的是（ ）。

A.RAID0

B.RAID1

C.RAID10

D.RAID0+1

【参考答案】：BCD

279.分子公司信息管理部门是南网云分节点建设和运营的责任主体，主要职责包括（ ）

A.负责按照公司统一部署，基于统一的南网云平台开展数字化转型和数字南网建设工作

B.配合公司数字化部完成南网云分节点规划、设计、项目立项审查、资金安排及项目统筹推进

C.按照公司统一部署，负责南网云分节点物理资源建设、扩容、运维与运营

D.负责按照公司统一要求落实安全管理，负责分节点云平台运行安全

【参考答案】：ABCD

280.计算机信息系统安全管理包括（ ）

A.组织建设

B.事前检查

C.制度建设

D.人员意识

【参考答案】：ACD

281.信息机房主设备巡检需要带好（ ）手环，检查各设备有无（ ）提示。

A.防静电

B.工作

C.警报

D.告警

【参考答案】：AD

282.《网络安全法》的特征有：（ ）

A.整体性

B.协调性

C.稳定性

D.可操作性

【参考答案】：ABCD

283.下列措施中，（ ）是系统在进行重定向和转发检查时需要进行的检查措施。

A.重定向之前，要验证重定向的目标URL

B.使用白名单验证重定向目标

C.如果在网站内重定向，可以使用相对路径URL

D.重定向或者转发之前，要验证用户是否有权限访问访问目标URL

【参考答案】：ABCD

284.下列哪些不属于黑客地下产业链类型？（ ）

A.真实资产盗窃地下产业链

B.互联网资源与服务滥用地下产业链

C.移动互联网金融产业链

D.网络虚拟资产盗窃地下产业链

【参考答案】：ABD

285.入侵检测系统要求具有（ ）等功能。.

A.监视、分析用户及系统活动

B.识别网络入侵攻击的活动模式并提出告警

C.异常行为模式的统计分析

D.查杀病毒

【参考答案】：ABC

286.信息收集与分析的防范措施包括（ ）

A.部署网络安全设备

B.减少攻击面

C.修改默认配置

D.设置安全设备应对信息收集

【参考答案】：ABCD

287.属于VPN的核心技术是（ ）

A.隧道技术

B.身份认证

C.日志记录

D.访问控制

【参考答案】：ACD

288.下列哪些是防火墙的重要行为？（ ）。

A.准许

B.限制

C.日志记录

D.问候访问者

【参考答案】：AB

289.下列属于病毒检测方法的是（ ）

A.特征代码法

B.校验和法

C.行为检测法

D.软件模拟法

【参考答案】：ABCD

290.办公网络中计算机的逻辑组织形式可以有两种，工作组和域。下列关于工作组的描述中错误的是（ ）。

A.工作组中的每台计算机都在本地存储账户

B.本计算机的账户可以登录到其它计算机上

C.工作组中的计算机的数量最好不要超过10台

D.工作组中的操作系统必须一样

【参考答案】：ABD

291.现代主动安全防御的主要手段是（ ）

A.探测

B.预警

C.监视

D.警报

【参考答案】：ABCD

292.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.可审查性

【参考答案】：ABCD

293.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

【参考答案】：ABD

294.《中华人民共和国安全生产法》的目标：（ ）。

A.加强安全生产监督管理

B.防止和减少生产安全事故

C.保障人民群众生命和财产安全

D.促进经济发展

【参考答案】：ABCD

295.计算机后门木马种类包括（ ）

A.特洛伊木马

B.RootKit

C.脚本后门

D.隐藏账号

【参考答案】：ABCD

296.段式和页式存储管理的地址结构很类似，但是它们之间有实质上的不同，表现为：（ ）

A.页式的逻辑地址是连续的，段式的逻辑地址可以不连续

B.页式的地址是一维的，段式的地址是二维的

C.分页是操作系统进行的，分段是用户确定的

D.各页可以分散存放在主存，每段必须占用连续的主存空间

【参考答案】：ABCD

297.（ ）可以有效提高病毒防治能力。

A.安装、升级杀毒软件

B.升级系统、打补丁

C.提高安全防范意识

D.不要轻易打开来历不明的邮件

【参考答案】：ABCD

298.下面属于光存储介质的是（ ）。

A.CD-ROM

B.DVD-ROM

C.CD-R

D.CD-RW

【参考答案】：ABCD

299.任何一个电路的基本组成部分是（ ）。

A.电源

B.负载

C.导线

D.控制部件

【参考答案】：ABCD

300.下列措施中，（ ）用于防范传输层保护不足

A.对所有敏感信息的传输都要加密

B.对于所有的需要认证访问的或者包含敏感信息的内容使用SSL/TLS连接

C.可以对HTTP和HTTPS混合使用

D.对所有的cookie使用Secure标志

【参考答案】：ABD