# 2023年度“经开先锋”职工职业技能大赛
# （网络与信息安全管理员）
# 理论题库

**一、单项选择题**

1、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. 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

答案：B

2、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

答案：A

3、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

答案：C

4、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

答案：B

5、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

答案：B

6、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

答案：A
7、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
答案：A
8、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
答案：A
9、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
答案：B
10、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
答案：A
11、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
答案：A
12、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
答案：D
13、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

答案：A
14、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
答案：A
15、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
答案：D
16、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
答案：A
17、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
答案：A
18、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
答案：C
19、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
答案：B
20、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
答案：A
21、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
答案：B
22、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
答案：A
23、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
答案：A
24、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
答案：A
25、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
答案：B
26、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
答案：B
27、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
答案：B
28、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
答案：B
29、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
答案：C
30、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
答案：A
31、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
答案：A
32、NT/2K 模型符合哪个安全级别？
A. B2
B. C2
C. B1
D. C1
答案：B
33、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
答案：A
34、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
答案：D

35、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
答案：A
36、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
答案：B
37、《中华人民共和国网络安全法》自（　）起施行。
A. 42681
B. 42887
C. 42736
D. 42705
答案：B
38、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
答案：B
39、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
答案：B
40、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
答案：A
41、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
答案：D
42、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
答案：A
43、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
答案：A
44、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
答案：A
45、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
答案：B
46、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
答案：D
47、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
答案：C
48、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
答案：A
49、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
答案：B
50、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
答案：C
51、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
答案：B
52、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
答案：D
53、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
答案：B
54、上网行为审计记录内容应保留（　）天以上。
A. 30
B. 60
C. 90
D. 120
答案：B
55、输入 enable，进入防火墙（　）模式。
A. 用户
B. 特权
C. 关机
D. 待机
答案：B
56、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
答案：C
57、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
答案：A
58、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
答案：A
59、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
答案：A
60、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
答案：A
61、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
答案：B
62、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

答案：D
63、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
答案：B
64、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
答案：A
65、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
答案：A
66、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
答案：D
67、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
答案：A
68、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
答案：C
69、数据库是由逻辑相关的（　）组成。
A. 记录
B. 文件
C. 数据
D. 信息
答案：B
70、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
答案：A
71、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
答案：A
72、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
答案：A
73、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
答案：A
74、Windows 操作系统的注册表运行命令是：
A. Regsvr32
B. Regedit
C. Regedit. msc
D. Regedit. Mmc
答案：B
75、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
答案：B
76、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
答案：A
77、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
答案：C
78、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
答案：B
79、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
答案：B
80、（　）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
答案：A
81、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
答案：A
82、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
答案：D
83、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
答案：B
84、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
答案：A
85、二进制代码是由（　）组成的。
A. 0 0
B. 0 1
C. 1 1
D. 1 2
答案：B
86、HTTPS 采用（　）协议实现安全网站访问。
A. SSL
B. IPsec
C. PGP
D. SET
答案：A
87、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
答案：A
88、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
答案：A
89、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
答案：A
90、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
答案：A
91、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

答案：D
92、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
答案：C
93、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
答案：A
94、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
答案：A
95、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
答案：A
96、最简单的防火墙是（　）。
A. 路由器
B. 以太网桥
C. 交换机
D. 网卡
答案：B
97、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
答案：A
98、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）

答案：A
99、（　）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
答案：A
100、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
答案：A
101、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
答案：A
102、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
答案：C
103、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
答案：B
104、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
答案：A
105、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
答案：D

106、分布式拒绝服务攻击的简称是（　）
A. DDOS
B. DROS
C. LAND
D. SDOS
答案：A
107、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
答案：A
108、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
答案：D
109、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
答案：B
110、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
答案：B
111、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
答案：C
112、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
答案：B
113、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
答案：A
114、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
答案：A
115、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
答案：C
116、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
答案：A
117、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
答案：A
118、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
答案：D
119、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
答案：A
120、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
答案：A
121、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
答案：A
122、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
答案：A
123、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
答案：B
124、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
答案：B
125、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
答案：C
126、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）
答案：B
127、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
答案：D
128、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
答案：A
129、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
答案：A
130、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
答案：A
131、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
答案：A
132、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
答案：A
133、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
答案：D

134、下面不属于虚拟化平台的是（　）。
A. Vmware
B. Hyper-v
C. Citrix
D. DOS
答案：D
135、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
答案：A
136、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
答案：A
137、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
答案：A
138、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
答案：A
139、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
答案：B
140、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

答案：B
141、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
答案：A
142、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
答案：B
143、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
答案：A
144、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：B
145、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
答案：A
146、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
答案：B
147、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. 完全防止传送已被病毒感染的软件和文件
答案：B
148、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
答案：A
149、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
答案：A
150、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
答案：B
151、下列 RAID 技术无法提高读写性能的是（　）。
A. RAID0
B. RAID1
C. RAID3
D. RAID5
答案：B
152、Windows Server 2003 标准版支持的 CPU 数量为（　）。
A. 4
B. 6
C. 8
D. 12
答案：A
153、（　）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
答案：A
154、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
答案：A
155、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
答案：B
156、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
答案：A
157、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
答案：A
158、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
答案：B
159、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
答案：C
160、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
答案：D
161、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
答案：B
162、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
答案：A
163、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
答案：A
164、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
答案：B
165、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
答案：A
166、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
答案：A
167、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
答案：A

168、（　）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
答案：A
169、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
答案：A
170、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
答案：A
171、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
答案：B
172、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
答案：B
173、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
答案：C
174、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
答案：B
175、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
答案：A
176、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
答案：A
177、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
答案：B
178、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
答案：D
179、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
答案：A
180、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
答案：B
181、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
答案：A
182、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）
答案：B
183、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
答案：C
184、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
答案：D
185、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。
答案：B
186、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
答案：D
187、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
答案：B

188、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
答案：D
189、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
答案：B
190、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
答案：B
191、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
答案：B
192、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
答案：B
193、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
答案：C
194、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
答案：A

195、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
答案：A
196、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
答案：B
197、（　）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
答案：A
198、《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
答案：B
199、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
答案：A
200、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
答案：A
201、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

答案：A

202、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
答案：B

203、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
答案：A

204、主要用于加密机制的协议是( )
A.HTTP
B.FTP
C.TELNET
D.SSL
答案：D

205、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.缓存溢出攻击;
B.钓鱼攻击
C.暗门攻击;
D.DDOS 攻击
答案：B

206、Windows 系统能设置为在几次无效登录后锁定帐号,这可以防止( )
A.木马;
B.暴力攻击;
C.IP 欺骗;
D.缓存溢出攻击
答案：B

207、在以下认证方式中，最常用的认证方式是：( )
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
答案：A

208、以下哪项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
答案：B

209、下列不属于系统安全的技术是(　)
A.防火墙
B.加密狗
C.认证
D.防病毒
答案：B

210、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
答案：D

211、第三级信息系统测评过程中，关于数据安全及备份恢复的测评，应测试应用系统，通过用（　　）工具获取系统传输数据包，查看其是否采用了加密或其他有效措施实现传输保密性。
A.测试
B.运维
C.嗅探
D.以上都不对
答案：C

212、第三级信息系统测评过程中，关于数据安全及备份恢复的测评，应检查（　　）是否不存在关键节点的单点故障。
A.网络拓扑结构
B.主要网络设备
C.主要通信线路
D.主要数据处理系统
答案：A

213、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
答案：A

214、网页病毒主要通过以下途径传播(　)
A.邮件
B.文件交换
C.网络浏览
D.光盘
答案：C

215、不得开放的政务数据，列入非开放类，以下属于非开放类的数据是？（　　）
A.涉及国家秘密
B.商业秘密
C.个人隐私
D.以上全部都是
答案：D

216、数据提供部门应当按照（　　）的原则，负责本部门数据采集、归集、存储、提供、共享、应用和开放等环节的安全管理。
A.谁主管、谁负责，谁提供、谁负责
B.谁经手、谁负责，谁提供、谁负责
C.谁使用、谁负责，谁管理、谁负责
D.谁经手、谁负责，谁使用、谁负责
答案：A

217、一般等级保护建设的流程是什么？
A.定级、备案、监督检查、建设整改、等级测评
B.定级、备案、建设整改、等级测评、监督检查
C.建设整改、等级测评、监督检查、定级、备案
D.等级测评、定级、备案、建设整改、监督检查
答案：B

218、关键信息基础设施和等级保护之间的关系？
A.关键信息基础设施在等级保护第二级对象中确定
B.等级保护第三级对象一定是关键信息基础设施
C.关键信息技术设施防护和等级保护安全防护要求一致
D.关键信息基础设施在等级保护第三级以上对象中确定
答案：D

219、等保 2.0 已发布的核心标准不包括下面哪一项？（　）
A.基本要求
B.定级指南
C.设计指南
D.测评指南
答案：B

220、等保 2.0 有安全扩展要求不包括下面哪一项？（　）
A.云计算安全扩展要求
B.移动互联安全扩展要求
C.物联网安全扩展要求
D.人工智能系统安全扩展要求
答案：D

221、第三级信息系统测评过程中，关于应用安全的测评，应检查应用系统，查看其是否采用了（　　）身份鉴别技术的组合来进行身份鉴别，并保证至少有一种是不可伪造的。
A.两个及两个以上
B.三个及三个以上
C.四个及四个以上
D.五个及五个以上
答案：A

222、第三级信息系统测评过程中，关于应用安全的测评，应（　　），查看其提供的登录失败处理功能，是否根据安全策略配置了相关参数。
A.测试应用系统
B.渗透测试应用系统
C.检查应用系统
D.访谈应用系统管理员
答案：C

223、第三级信息系统测评过程中，关于应用安全的测评，应测试应用系统，试图非授权（　）审计记录，验证安全审计的保护情况。
A.删除
B.修改
C.覆盖
D.都可
答案：D

224、第三级信息系统测评过程中，关于数据安全及备份恢复的测评，应检查（　　）中是否为专用通信协议或安全通信协议服务，避免来自基于通信协议的攻击破坏数据完整性。
A.操作系统和网络设备
B.数据库管理系统
C.应用系统
D.都需检查
答案：D
225、等级保护有几个安全保护级别？（　）
A.3 个
B.4 个
C.5 个
D.6 个
答案：C

226、什么样的系统可以作为定级对象？（　　）
A.某台终端
B.云平台
C.某台服务器
D.某台路由器
答案：B
227、等级保护的全称是（　　）。（　）
A.网络安全测评等级保护
B.信息安全等级保护
C.网络信息等级保护
D.网络安全等级保护
答案：D

228、《个人信息保护法》通过的时间是（　　）。
A.2021 年 8 月 1 日
B.2021 年 8 月 10 日
C.2021 年 8 月 20 日
D.2021 年 8 月 30 日
答案：C

229、关于《个人信息保护法》立法宗旨，不正确的是（　　）。
A.为了保护个人信息权益
B.规范个人信息处理活动
C.提高个人信息数据质量
D.促进个人信息合理利用
答案：C

230、以下不是关键信息基础设施重要行业和领域的是？（　　）
A.公共通信和信息服务
B.能源、交通、水利、金融
C.公共服务、电子政务、国防科技工业
D.各类网购平台
答案：D

231、《关键信息基础设施安全保护条例》规定安全保护措施应当与关键信息基础设施（　　）。
A.同步规划
B.同步建设
C.同步使用
D.以上都是
答案：D

232、运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的（　　）对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大

网络安全事件处置工作，组织研究解决重大网络安全问题。
A.安全负责人
B.主要负责人
C.信息中心负责人
D.生产负责人
答案：B

233、运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行（　　）网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。
A.一次
B.二次
C.三次
D.四次
答案：A

234、保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、（　　），预警通报网络安全威胁和隐患，指导做好安全防范工作。
A.安全态势
B.风险状态
C.人员情况
D.保障措施
答案：A

235、运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，应当对以下哪个部门依法开展的关键信息基础设施网络安全检查工作应当予以配合？（　）
A.公安、国家安全、保密行政管理、密码管理
B.应急
C.通信
D.数据管理部门
答案：A

236、《数据安全法》经十三届全国人大常委会第二十九次会议通过并正式发布，于（　　）起施行。
A.2021 年 6 月 1 日
B.2021 年 8 月 1 日
C.2021 年 9 月 1 日
D.2021 年 10 月 1 日
答案：C
237、下列数据中不属于国家核心数据的是（　　）。
A.关系国家安全的数据
B.关系国民经济命脉的数据
C.关系重要民生的数据
D.关系公共利益的数据

答案：D

238、国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以（　　）为关键要素的数字经济发展。
A.信息
B.数据
C.技术
D.创新
答案：B

239、国家统筹（　　），坚持以数据促进数据安全，以数据安全保障数据开发利用和产业发展。
A.发展和安全
B.利用和保护
C.成本和效益
D.自主和引用
答案：A
240、《个人信息保护法》施行的时间是（　　）。
A.2021 年 8 月 20 日
B.2021 年 10 月 1 日
C.2021 年 11 月 1 日
D.2021 年 12 月 1 日
答案：C

241、《个人信息保护法》是在（　　）全国人民代表大会常务委员会第三十次会议通过的。
A.第十一届
B.第十二届
C.第十三届
D.第十四届
答案：C

242、依据《中华人民共和国数据安全法》，开展数据处理活动应当依照法律、法规的规定，建立健全（　　）管理制度。
A.全流程数据安全
B.“谁处理谁负责”
C.风险评估
D.应急处置
答案：A
243、关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用（　　）的规定。
A.《中华人共和国宪法》
B.《中华人民共和国网络安全法》
C.《中华人民共和国国家安全法》
D.《中华人民共和国境外非政府组织境内活动管理法》

答案：B

244、以下哪部法律适用于适用于在中华人民共和国境外开展数据处理活动及其安全监管。（　）
A.《中华人民共和国网络安全法》
B.《中华人民共和国国家安全法》
C.《中华人民共和国数据安全法》
D.《安徽省政务数据资源管理办法》
答案：C

245、重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送（　　）。
A.风险评估报告
B.数据安全风险清单
C.应急补救措施
D.风险报告单
答案：A

246、国家大力推进电子政务建设，提高政务数据的（　　），提升运用数据服务经济社会发展的能力。
A.公益性、准确性、时效性
B.科学性、准确性、高效性
C.公益性、准确性、高效性
D.科学性、准确性、时效性
答案：D

247、国家鼓励开发网络数据安全保护和利用技术，促进（　　）开放，推动技术创新和经济社会发展。
A.公共图书馆资源
B.国家数据资源
C.公共数据资源
D.公共学校资源
答案：C

248、网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构（　　）或者安全检测符合要求后，方可销售或者提供。
A.认证产品合格
B.安全认证合格
C.认证设备合格
D.认证网速合格
答案：B

249、网络产品、服务应当符合相关国家标准的（　　）要求。
A.规范性

B.自觉性
C.强制性
D.建议性
答案：C

250、国家实施网络（　　）战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。
A.认证身份
B.可信身份
C.信誉身份
D.安全身份
答案：B

251、国家建立网络安全监测预警和（　　）制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。
A.信息输送
B.信息通报
C.信息共享
D.信息传达
答案：B

252、关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订（　　），明确安全和保密义务与责任。
A.保密合同
B.安全保密协议
C.安全责任条款
D.安全服务合同
答案：B

253、根据《网络安全法》的规定，国家实行网络安全（　　）保护制度。
A.结构
B.分层
C.等级
D.行政级别
答案：C

254、根据《网络安全法》的规定，（　　）应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。
A.电信企业
B.电信科研机构
C.网络运营者
D.网络合作商
答案：C

255、国家支持研究开发有利于未成年人健康成长的网　络产品和服务，依法惩治利用网络从事（　　）的活动，为未成年人提供安全、健康的网络环境。
A.危害未成年人身心健康
B.针对未成年人黄赌毒
C.侵害未成年人受教育权
D.灌输未成年人错误网络思想
答案：A

256、关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的（　　）。
A.国家安全审查
B.国家网络审查
C.国家网信安全审查
D.国家采购审查
答案：A

257、国家推进网络安全（　　）建设，鼓励有关企业、机　构开展网络安全认证、检测和风险评估等安全服务。
A.社会化认证体系
B.社会化识别体系
C.社会化服务体系
D.社会化评估体系
答案：C

258、网络产品、服务的提供者不得设置（　　），发现其　网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
A.病毒程序
B.攻击程序
C.风险程序
D.恶意程序
答案：D

259、国家建立和完善网络安全标准体系。（　　）和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。
A.电信研究机构
B.国务院标准化行政主管部门
C.网信部门
D.电信企业
答案：B

260、关键信息基础设施的运营者应当自行或者委托网　络安全服务机构对其网络的安全性和可能存在的风险（　　）至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

A.三年
B.两年
C.每年
D.四年
答案：C

261、在 IP 互联网层提供安全的一组协议是。（ ）
A.Tls
B.SSH
C.PGP
D.IPSec
答案：D

262、黑客利用 IP 地址进行攻击的方法有:（ ）
A. IP 欺骗
B.解密
C.窃取口令
D.发送病毒
答案：A

263、不属于黑客被动攻击的是（ ）
A.网页木马
B.缓冲区溢出
C.浏览恶意网页
D.打开病毒附件
答案：B

264、TCP 负责___ 之间的通信，它使用端口号进行寻址（ ）
A.主机到主机
B.进程到进程
C.端口号
D. IP
答案：B

265、在应用层协议中，____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
答案：B

266、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（ ）。
A. 机密性

B.完整性
C.可用性
D.可控性
答案：C

267、屏蔽路由器型防火墙采用的技术是基于:（ ）
A.数据包过滤技术
B.应用网关技术
C.代理服务技术
D.三种技术的结合
答案：B

268、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（ ）。
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
答案：D

269、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：D

270、IP 地址欺骗通常是（ ）
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
D.是属于链路层的攻击
答案：A

271、VPN 的加密手段为（ ）
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
答案：C

272、不属于 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
答案：C

273、()拒绝服务攻击通过向目标主机发送畸形的报文导致目标主机在报文重组时崩溃。
A.死亡之 ping
B.Finger 炸弹
C.泪滴攻击
D.Land 攻击
答案：C

274、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
答案：A

275、当访问 web 网站的某个页面资源不存在时，将会出现的 HTTP 状态码是(  )
A.200
B.302
C.401
D.404
答案：D

276、(  ）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
答案：A

278、你想发现到达目标网络需要经过哪些路由器，你应该使用的命令是 (  )。
A.ping
B.nslookup
C.tracert
D.ipconfig
答案：C

279、主要用于加密机制的协议是_____
A.HTTP
B.FTP
C.TELNET

D.SSL
答案：D

280、ARP 欺骗的实质是（　　）
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
答案：A

281、以下不属于代理服务技术优点的是(　)
A.可以实现身份认证
B.内部地址的屏蔽和转换功能
C.可以实现访问控制
D.可以防范数据驱动侵袭
答案：D

282、CA 的主要功能为（　　）
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
答案：C

283、IPS 能够实时检查和阻止入侵的原理在于 IPS 拥有众多的（　）
A. 主机传感器
B. 网络传感器
C. 过滤器
D. 管理控制台
答案：C

284、在以下人为的恶意攻击行为中，属于主动攻击的是( )
A.身份假冒
B.数据 GG
C.数据流分析
D.非法访问
答案：A

285、有关 PPTP（ Point-to-Point Tunnel Protocol) 说法正确的是（ ）
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
答案：C

286、以下对 DoS 攻击的描述，正确的是(　)
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.导致目标系统无法正常处理用户的请求
D.若目标系统没有漏洞,远程攻击就不会成功
答案：C

287、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
答案：B

288、下列协议中， 哪个不是一个专用的安全协议(　)
A.SSL
B.ICMP
C. VPN
D.HTTPS
答案：B

289、针对下列各种安全协议，最适合使用外部网 VPN 上，用于在客户机到服务器的连接模式的是（）
A. IPsec
B. PPTP
C. SOCKS v5
D. L2TP
答案：C

290、专用于窃听网上传输的口令信息的工具是(　)
A.PGP
B.SMB
C.dsniff
D.strobe
答案：C
291、包过滤技术与代理服务技术相比较(　)
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.包过滤技术对应用和用户是绝对透明的
C.代理服务技术安全性较高、但不会对网络性能产生明显影响
D.代理服务技术安全性高，对应用和用户透明度也很高
答案：B

292、常规端口扫描和半开式扫描的区别是?(　)

A.没什么区别
B.没有完成三次握手，缺少 ACK 过程
C.半开式采用 UDP 方式扫描
D.扫描准确性不一样
答案：B

293、防火墙技术是一种(　)安全模型。
A.被动式
B.主动式
C.混合式
D.以上都不是
答案：A

294、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
答案：D

295、(　)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
答案：C

296、NAT 提供了（）安全策略。
A.充当网络之间的代理服务器
B.配置网关
C.隐藏内部 IP 地址
D.创建检查点
答案：C

297、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,保证数据接受方收到的信息与发送方发送的信完全一致
D.确保数据数据是由合法实体发出的
答案：A

298、“会话侦听和劫持技术”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
答案：B

299、 将利用虚假 IP 地址进行 ICMP 报文传输的攻击方法称为（　　）
A. ICMP 泛洪
B. LAND 攻击
C. 死亡之 ping
D. Smurf 攻击
答案：D

300、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
答案：A

**二、多项选择题**

1、《网络安全法》规定,国家维护网络安全的主要任务是（　）
A.检测、防御、处置网络安全风险和威胁
B.保护关键信息基础设施安全
C.依法惩治网络违法犯罪活动
D.维护网络空间安全和秩序
答案：ABCD
2、因网络安全事件，发生突发事件或者生产安全事故的，应当依照（　）等有关法律、行政法规的规定处置。
A.《中华人民共和国网络安全法》
B.《中华人民共和国突发事件应对法》
C.《中华人民共和国安全生产法》
D.《中华人民共和国应急法》
答案：BC
3、数字签名不能通过（　）来实现的。
A.认证
B.程序
C.签字算法
D.仲裁
答案：ABD
4、以下哪一项属于信息欺骗的范畴（　）
A.会话劫持
B.IP 欺骗
C.重放攻击

D.社交工程
答案：BCD
5、强制访问控制用户与访问的信息的读写关系正确的是（　）。
A.下读:用户级别大于文件级别的读操作
B.上写:用户级别大于文件级别的写操作
C.上读:用户级别低于文件级别的读操作
D.下写:用户级别小于文件级别的写操作
答案：AC
6、RIP（路由信息协议）作为路由协议采用方式有误的是哪几种。
A.距离向量
B.链路状态
C.分散通信量
D.固定查表
答案：BCD
7、计算机犯罪的主要特征包括（　）。
A.犯罪主体的智能化
B.犯罪取证简单化
C.社会危害严重化
D.犯罪手段特殊化
E、社会危害轻微化
答案：ACD
8、关于黑客攻击中肉鸡的认识，正确的是（　）
A.肉鸡通常不是自愿的
B.肉鸡事先已经被植入木马
C.黑客通过木马控制肉鸡参与攻击
D.完全无法判断电脑是否已成为肉鸡
答案：ABC
9、资产处置方式包括报废、盘亏、（　）、作价投资、出租、抵押、抵债等。
A.调拨
B.转让
C.置换
D.捐赠
答案：ABCD
10、未来的防火墙产品与技术应用有哪些特点：（　）。
A.防火墙从远程上网集中管理向对内部网或子网管理发展
B.单向防火墙作为一种产品门类出现
C.利用防火墙建 VPN 成为主流
D.过滤深度向 URL 过滤、内容过滤、病毒清除的方向发展
答案：BCD
11、在系统投运前，应对系统运行的稳定性、安全性进行严格测试。包括检查（　）等。
A.应用系统是否存在安全漏洞和隐患
B.安装最新的补丁软件
C.关闭不必要的服务端口和不必要的服务进程
D.删除不必要的用户

答案：ABCD
12、在 IPSec 中，使用 IKE 建立通道时使用的端口号，错误的是（　）。
A.TCP500
B.UDP500
C.TCP50
D.UDP50
答案：ACD
13、你是一台 Windows Server 2008 计算机的系统管理员，你不可以使用（　）工具来管理该计算机中的组账号。
A.活动目录用户和计算机
B.域用户和计算机
C.活动目录用户与用户组
D.本地用户和组
答案：ABD
14、根据《广西电网有限责任公司企业信息门户系统作业指导书（2015 年）》，企业信息门户系统应用页面每日巡检内容包括（　　）。
A.查看页面上的新闻、通知信息等信息显示是否正常
B.查看登录后各项数据显示是否正常
C.查看登录后能否发布信息
D.查看登录后系统管理功能是否能使用
答案：ABCD
15、《网络安全法》在完善个人信息保护法律制度方面的亮点有：（　）
A.合法、正当、必要原则
B.明确原则和知情同意原则
C.明确个人信息的删除权和更正权制度
D.公民个人信息、隐私和商业秘密的保密制度
答案：ABCD
16、信息系统建转运管理审查点审查要求包括（　）三个方面。其中，（　） 审查指查看要求文档是否存在；（　） 审查指审核文档内容是否符合要求；（　）审查指按照文档操作以审查文档是否具备可操作性。
A.文档完整性
B.内容合规性
C.文档可用性
D.内容合理性
答案：ABC
17、下列方法中（　）可以作为防止跨站脚本的方法
A.验证输入数据类型是否正确
B.使用白名单对输入数据进行安全检查或过滤
C.使用黑名单对输入数据进行安全检查或过滤
D.对输出数据进行净化
答案：ABCD

18、在设计密码的存储和传输安全策略时应考虑的原则包括（　）。
A.禁止文明传输用户登录信息机身份凭证

B.禁止在数据库或文件系统中明文存储用户密码
C.必要时可以考虑 COOKIE 中保存用户密码
D.应采用单向散列值在数据库中存储用户密码，并使用强密码，在生产单向散列值过程中加入随机值
答案：ABD
19、下面说法正确的是（　）
A.EXCEL 的行高是固定的
B.EXCEL 单元格的宽度是固定的，为 8 个字符宽
C.EXCEL 单元格的宽度是可变的，默认宽度为 8 个字符宽
D.EXCEL 的行高和列宽是可变的
答案：BD
20、公司自主移动应用必须在公司范围内省级及以上集中部署，应采用公司统一的移动架构与防护标准，落实“（　）”的要求，做到集中部署与集中防护。
A.统一审核
B.安全入口
C.测评发布
D.统一监测
答案：ABCD
21、下列（　）是域控制器存储所有的域范围内的信息。
A.安全策略信息
B.用户身份验证信息
C.账户信息
D.工作站分区信息
答案：ABC
22、（　）是由失效的身份认证和会话管理而造成的危害
A.窃取用户凭证和会话信息
B.冒出用户身份察看或者变更记录，甚至执行事务
C.访问未授权的页面和资源
D.执行超越权限操作
答案：ABCD
23、日志分析重点包括（　）
A.源
B.请求方法
C.请求链接
D.状态代码
答案：ABCD
24、《网络安全法》的网络运营者包括（　）
A.网络所有者
B.网络管理者
C.网络使用者
D.网络服务提供者
答案：ABD
25、应根据情况综合采用多种输入验证的方法，以下输入验证方法需要采用（　）
A.检查数据是否符合期望的类型

B.检查数据是否符合期望的长度
C. 检查数据是否符合期望的数值范围
D.检查数据是否包含特殊字符
答案：ABCD
26、网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施（ ）。
A.要求有关部门、机构和人员及时收集、报告有关信息
B.加强对网络安全风险的监测
C.组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估
D.向社会发布网络安全风险预警，发布避免、减轻危害的措施
答案：ACD
27、下列关于跨站请求伪造的说法正确的是（ ）
A.只要你登陆一个站点 A 且没有退出，则任何页面都以发送一些你有权限执行的请求并执行
B.站点 A 的会话持续的时间越长，受到跨站请求伪造攻击的概率就越大
C.目标站点的功能采用 GET 还是 POST 并不重要，只不过 POST 知识加大了一点点跨站请求伪造的难度而已
D.有时候负责的表单采用多步提交的方式防止跨站请求伪造攻击其实并不可靠，因为可以发送多个请求来模拟多步提交
答案：ABCD
28、对于防火墙不足之处，描述正确的是（ ）
A.无法防护基于尊重作系统漏洞的攻击
B.无法防护端口反弹木马的攻击
C.无法防护病毒的侵袭
D.无法进行带宽管理
答案：ABC
29、防火墙能够作到些什么？
A.包过滤
B.包的透明转发
C.阻挡外部攻击
D.记录攻击
答案：ABCD
30、使用中间件带来的好处有（ ）。
A.节省应用开发费用
B.简化应用集成
C.降低软件维护费用
D.增强应用程序吸引力
答案：ABCD
31、对于远程访问 VPN 须制定的安全策略有：（ ）
A.访问控制管理
B.用户身份认证、智能监视和审计功能
C.数据加密
D.密钥和数字证书管理
答案：ABCD
32、加密技术包括两个元素 （ ）。

A.算法
B.编码
C.数字
D.密钥
E、字节
答案：AD
33、以下有助于减少收到垃圾邮件数量的是（　）
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该小心谨慎
C.安装入侵检测软件
D.收到垃圾邮件后向有关部门举报
答案：ABD
34、系统投运阶段的工作需遵循公司关于（　）等方面的管理办法和管理细则的相关要求。
A.IT 管理
B.IT 服务
C.IT 运维
D.安全防护
答案：BCD
35、IPSAN 由（　）组成。
A.设备整合，多台服务器可以通过存储网络同时访问后端存储系统，不必为每台服务器单独购买存储设备，降低存储设备异构化程度，减轻维护工作量，降低维护费用
B.数据集中，不同应用和服务器的数据实现了物理上的集中，空间调整和数据复制等工作可以在一台设备上完成，大大提高了存储资源利用率
C.兼容性好，FC 协议经过长期发展，已经形成大规模产品化，而且厂商之间均遵循统一的标准，以使目前 FCSAN 成为了主流的存储架构
D.高扩展性，存储网络架构使得服务器可以方便的接入现有 SAN 环境，较好的适应应用变化的需求
答案：ABD
36、（　）将引起文件上传的安全问题
A.文件上传路径控制不当
B.可以上传可执行文件
C.上传文件的类型控制不严格
D.上传文件的大小控制不当
答案：ABCD
37、数字证书含有的信息包括（　）。
A.用户的名称
B.用户的公钥
C.用户的私钥
D.证书有效期
答案：ABD
38、在数据库安全配置中，下列（　）需要修改的默认用户和对应的默认密码
A.sys/change_install
B.system/manager
C.aqadm/aqadm

D.Dbsnmp/Dbsnmp
答案：ABCD
39、工作许可人安全责任包括（　）。
A.负责审查变更管理票所列安全措施是否正确完备，是否符合现场条件
B.工作现场布置的安全措施是否完善
C.负责检查停电设备有无突然来电的危险
D.对变更管理票中所列内容即使发生很小疑问，也必须向变更管理票签发人询问清楚，必要时应要求作详细补充
答案：ABCD
40、以下关于计算机病毒说法，错误的是（　）。
A.发现计算机病毒后，删除磁盘文件是能彻底清除病毒的方法
B.使用只读型光盘不可能使计算机感染病毒
C.计算机病毒是一种能够给计算机造成一定损害的计算机程序
D.计算机病毒具有隐蔽性、传染性、再生性等特性
E、制造和传播计算机病毒应受到行政处罚
答案：ABDE
41、南网云各节点须加强平台常态运营监控分析，监控内容包括（　）
A.运营指标
B.资源使用情况
C.业务承载
D.业务承载
答案：ABCD
42、《网络安全法》强化了关键信息基础设施运营者的责任和义务，除了履行网络运营者的责任义务外，还应履行（　）
A.关于“三同步”的要求
B.关于国家安全审计的要求
C.关于安全和保密义务的要求
D.关于提供技术支持和协助的要求
答案：ABC
43、关于《网络安全法》以下正确的是（　）
A.《网络安全法》提出制定网络安全战略，明确网络空间治理目标，提高了我国网络安全政策的透明度
B.《网络安全法》进一步明确了政府各部门的职责权限，完善了网络安全监管体制
C.《网络安全法》强化了网络运行安全，重点保护关键信息基础设施
D.《网络安全法》将监测预警与应急处置措施制度化、法制化
答案：ABCD
44、公共信息网络安全监察工作的一般原则:（　）。
A.预防与打击相结合的原则
B.专门机关监管与社会力量相结合的原则
C.纠正与制裁相结合的原则
D.教育和处罚相结合的原则
答案：ABCD
45、采用混合运维外包策略时，（　）等核心业务应采用自主运维，其他运维服务内容可采用外包运维。

A.核心设备的日常配置管理
B.重要应用系统的数据管理
C.用户权限管理
D.桌面终端运维服务
答案：ABC
46、下列可以引起安全配置错误的是（　）
A.服务器没有及时安全补丁
B.没有对用户输入数据进行验证
C.没有对系统输出数据进行处理
D.网站没有禁止目录浏览功能
答案：AD
47、对于网络安全的特征,下列说法正确的有（　）
A.网络安全是一个系统的安全
B.网络安全是一个动态的安全
C.网络安全是一个无边界的安全
D.网络安全是一个非传统的安全
答案：ABCD
48、开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令（　），对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。
A.暂停相关业务
B.停业整顿
C.关闭网站
D.吊销相关业务许可证或者吊销营业执照
答案：ABCD
49、网络安全事件应急预案应当按照事件发生后的（　）、（　）等因素对网络安全事件进行分级。
A.危害程度
B.影响范围
C.事件等级
D.关注程度
答案：AB
50、张三将微信个人头像换成微信群中某好友头像，并将昵称改为该好友的昵称，然后向该好友的其他好友发送一些欺骗消息。该攻击行为属于以下哪类攻击？描述错误的是（　）
A.暴力破解
B.拒绝服务攻击
C.社会工程学攻击
D.口令攻击
答案：ABD
51、下述描述中，正确的是（　）。
A.设置了交换机的管理地址后，就可使用 Telnet 方式来登录连接交换机，并实现对交换机的管理与配置
B.首次配置交换机时，必须采用 Console 口登录配置

C.默认情况下，交换机的所以端口均属于 VLAN1，设置管理地址，实际上就是设置 VLAN1 接口的地址
D.交换机允许同时建立多个 Telnet 登录连接
答案：BCD
52、主机系统高可用技术中在系统出现故障时需要进行主机系统切换的是（　）
A.双机热备份方式
B.双机互备方式
C.多处理器协同方式
D.群集并发存取方式
答案：ABC
53、应用系统进行设计时，设计方案应满足以下要求：（　）。
A.设计软硬件平台架构
B.设计统一监控需求
C.安全设计方案
D.4A 平台
答案：ABCD
54、下列情形中会引起内存溢出的有（　）
A.未对缓存区填充数据时进行边界检查
B.系统资源未及时释放和服务连接未及时关闭
C.数据库查询操作，如果查询返回的结果较多时，未分次提取
D.每次内存分配未检查是否分配失败
答案：ABCD
55、（　）是目录浏览造成的危害
A.非法获取系统信息
B.得到数据库用户名和密码
C.获取配置文件信息
D.获得整改系统的权限
答案：ABCD
56、中间件的产生是为了解决哪些关键问题（　）。
A.有效安全地实现异构资源信息的共享
B.快速开发与集成各种异构应用软件系统
C.降低应用软件开发成本
D.提高系统的稳定性与可维护性
答案：ABCD
57、南方电网安全技术防护总体结构十多个防护项目中，可以归纳为（　）大类别。
A.身份认证与授权管理
B.数据安全防护
C.网络安全防护
D.基础安全防护及安全管理中心
答案：ABCD
58、以下几个选项中，哪些项是对 DBWR 后台进程的错误描述：（　）。
A.负责将数据库高速缓存中的改变后的数据写入到数据文件中
B.负责将重做日志缓冲区中的内容写入到联机日志文件中
C.负责向数据库发出检查点

D.事务提交操作即可触发 DBWR 进程
答案：BCD
59、IT 硬件资产退运后，信息运维部门根据退运情况同步完成 IT 硬件资产台账及资产管理相关系统中对应 IT 硬件资产的（　）等的维护。
A.基本信息
B.价值信息
C.使用信息
D.维护信息
答案：ABCD
60、（　）是不安全的直接对象引用而造成的危害
A.用户无需授权访问其他用户的资料
B.用户无需授权访问支持系统文件资料
C.修改数据库信息
D.用户无需授权访问权限外信息
答案：ABD
61、互联网远程接入控制的安全要求，二级系统和三系统均应满足
A.互联网远程接入必须选择较为安全的 VPN 接入方式
B.应当将 VPN 服务器放置于对外服务区域或 Internet 防火墙之外
C.对经过 VPN 进行的远程业务访问必须设定严格的访问控制规则，应尽量采用强认证，如证书、动态口令等进行远程访问的认证
D.应当进行完整的访问记录事件审计
答案：ABCD
62、实体安全技术包括：（　）。
A.环境安全
B.设备安全
C.人员安全
D.媒体安全
答案：ABD
63、能力管理主管应结合公司发展战略及业务部门职能战略，综合分析（　），每年定期编制能力管理计划。
A.业务能力
B.服务能力
C.IT 资源能力
D.基础设备
答案：ABC
64、木马在建立连接时必须条件的是（　）
A.服务端已经安装木马
B.控制端在线
C.服务端在线
D.已经获取服务端系统口令
答案：ABC
65、《网络安全法》的意义包括（　）
A.落实党中央决策部署的重要举措
B.维护网络安全的客观需要

C.维护民众切身利益的必然要求
D.参与互联网国际竞争和国际治理的必然选择
答案：ABCD
66、公司统一组织对（　）进行安全防护方案评审，包括安全架构遵从度、安全措施等。必要时公司邀请国家专家组对核心系统安全防护方案进行评审。各省市公司、直属单位其他自建系统安全防护方案由各单位自行组织评审并备案。
A.统推系统
B.二级及以上自建系统
C.三级及以上自建系统
D.自建系统
答案：AC
67、若一个组织声称自己的 ISMS 符合 ISO/IBC27001 或 GB/T22080 标准要求，其网络安全措施通常需要在物理和环境安全方面实施常规控制。物理和环境安全领域包括安全区域和设备安全两个控制目标。安全区域的控制目标是防止对组织场所和信息的未授权物理访问、损坏和干扰，关键或敏感信息及信息处理设施应放在安全区域内，并受到相应保护，该目标可以通过以下控制措施来实现（　）
A.物理安全边界、物理入口控制
B.办公室、房间和设施的安全保护，外部和环境威胁的安全防护
C.在安全区域工作，公共访问、交界区安全
D.人力资源安全
答案：ABC
68、“用户信息”可以理解为在用户使用产品或者服务过程中收集的信息构成用户信息，包括（　）
A.IP 地址
B.用户名和密码
C.上网时间
D.Cookie 信息
答案：ABCD
69、下列情况违反“五禁止”的有（　）。
A.在信息内网计算机上存储国家秘密信息
B.在信息外网计算机上存储企业秘密信息
C.在信息内网和信息外网计算机上交叉使用普通优盘
D.在信息内网和信息外网计算机上交叉使用普通扫描仪
答案：ABCD
70、应启用应用系统日志审计功能，审计日志内容应至少包含以下项（　）
A.用户登录、登出、失败登陆日志
B.管理员授权操作日志
C.创建、删除（注销）用户操作日志
D.重要业务操作
答案：ABCD
71、静电产生方式有（　）。
A.固体接触带电
B.固体分离带电（断裂带电，剥削带电）
C.物体摩擦带电

D.固体导体感应带电
答案：ABCD
72、灭火的基本方法有（　）。
A.隔离法
B.窒息法
C.冷却法
D.水灭法
答案：ABC
73、根据公司信息安全防护管理办法，公司信息部负责制定主机安全防护总体策略。下列选项中，属于主机安全防护总体策略的有（　）。
A.操作系统安全防护
B.数据库安全防护
C.应用系统安全防护
D.安全设备防护
答案：AB
74、以下有可能与计算机染上病毒有关的现象是（　）
A.系统出现异常启动或经常“死机”
B.程序或数据突然丢失
C.磁盘空间变小
D.打印机经常卡纸
答案：ABC
75、管理信息大区内部安全域划分原则包括（　）。、
A.业务重要性划分原则
B.业务访问源控制原则
C.连续性原则
D.可用性原则
答案：ACD
76、以下几个选项中，哪些项是对 Oracle 10g 数据库自动共享内存管理功能的正确描述：（　）
A.通过设置 sga_target 参数的值非 0，并将 statistics_level 保持默认值（TYPICAL），即可开启 Oracle 10g 数据库自动共享内存管理的功能
B.可以通过修改 sga_target 参数的值来修改 SGA 的总大小
C.Oracle 10g 数据库的自动共享内存管理功能也可用于管理 PGA
D.自动共享内存管理功能可管理的内存部分有：共享池、Stream 池、大池、Java 池、数据缓存池
答案：ABD
77、数据传输完整性与保密性要求：（　）。
A.采用密码技术支持的数据完整性检验或具有相当安全强度的其它安全机制，以实现网络数据传输完整保护，并在检测到完整性错误时进行一定的恢复；
B.采用密码技术支持的保密性保护机制或具有相当安全强度的其它安全机制，以实现网络数据传输保密性；
C.采用密码技术符合企业密码管理的相关规定。
D.采用的密码技术符合国家密码管理部门的相关规定。
答案：ABD

78、信息系统安全等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：（　）。
A.造成很严重损坏
B.造成一般损害
C.造成严重损害
D.造成特别严重损害
答案：BCD
79、典型的拒绝服务攻击方式包括（　）
A.Ping of death
B.SYN Flood
C.UDP Flood
D.Teardrop
答案：ABCD
80、Virtual Private Network 技术可以提供的功能有：（　）
A.提供 AccessControl
B.加密数据
C.信息认证和身份认证
D.划分子网
答案：ABC
81、根据《中国南方电网有限责任公司信息运维服务体系（2015 年）》，运维管理包括日常维护管理、（　）、系统优化和运维管控业务事项。
A.缺陷管理
B.巡检管理
C.故障管理
D.运维资源管理
答案：ABCD
82、环型拓扑结构的缺点是（　）。、
A.网络扩展配置困难
B.节点故障引起全网故障
C.故障诊断困难
D.拓扑结构影响访问协议
答案：ABCD
83、针对研发核心人员开展安全专业技能培训及资质认定，从事研发核心岗位（　）工作必须取得相应安全技能资质。
A.产品经理
B.项目经理
C.资深研发工程师
D.开发经理等
答案：ABD
84、以下对交换机工作方式的描述，正确的是（　）
A.可以使用半双工方式工作
B.可以使用全双工方式工作
C.使用全双工方式工作时要进行回路和冲突检测
D.使用半双工方式工作时要进行回路和冲突检测
答案：ABD

85、风险评估的内容包括（　）
A.识别网络和信息系统等信息资产的价值
B.发现信息资产在技术、管理等方面存在的脆弱性、威胁
C.评估威胁发生概率、安全事件影响，计算安全风险
D.有针对性地提出改进措施、技术方案和管理要求
答案：ABCD
86、下列关于《网络安全法》的说法正确的有：（　）
A.强化关键信息基础设施安全保护法律制度
B.确定了培养网络安全人才法律制度
C.建立了网络安全监测预警和信息通报法律制度
D.确立限制关键信息基础设施重要数据跨境流动法律制度
答案：ABCD
87、Ping 本机 IP 地址返回有效结果说明（　）。
A.TCP/IP 协议工作正确
B.本机 IP 地址有效
C.本网段正常工作
D.本机可以访问远程主机
答案：AB
88、根据《中国南方电网有限责任公司信息运维服务外包管理指导意见（2015 年）》，关于外协驻场人员评价考核，从（　）方面对外协驻场人员设置考核指标，形成考核指标体系。
A.个人资信
B.工作量
C.工作态度
D.工作质量
答案：ABCD
89、下列 RAID 技术中采用奇偶校验方式来提供数据保护的是（　）。
A.RAID1
B.RAID3
C.RAID5
D.RAID10
答案：BC
90、下列属于系统安全的技术是（　）
A.防火墙
B.加密狗
C.认证
D.防病毒
答案：ACD
91、下列（　）属于活动目录的逻辑结构。
A.域树
B.域林
C.组
D.域控制器
答案：ABC
92、下列哪些软件是用来接收电子邮件的客户端软件？（　）、

A.Foxmail
B.TheBat
C.ICQ
D.OutlookExpress
答案：ABD
93、防火墙有哪些部属方式?
A.透明模式
B.路由模式
C.混合模式
D.交换模式
答案：ABC
94、对 UNIX 中的 trap 指令，下列说法中（　）是正确的。
A.可供用户使用
B.UNIX 的例外处理程序也可使用 trap 指令
C.trap 指令是特权指令
D.trap 指令是在管态下运行
答案：AD
95、活动目录安装后，管理工具里有增加（　）菜单。
A.ActiveDirectory 用户和计算机
B.ActiveDirectory 域和信任关系
C.ActiveDirectory 域站点和服务器
D.ActiveDirectory 管理
答案：ABC
96、下列关于网络安全法的说法错误的有（　）。
A.国家规定关键信息基础设施以外的网络运营者必须参与关键信息基础设施保护体系。
B.关键信息基础设施的运营者可自行采购网络产品和服务不通过安全审查。
C.网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即向上级汇报。
D.国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。
答案：AB
97、以下属于计算机硬件系统的功能部件的是（　）。
A.运算器
B.操作系统
C.存储器
D.输入\输出设备
E、控制器
答案：ACDE
98、下面关于计算机病毒说法正确的是（　）
A.计算机病毒没有文件名
B.计算机病毒的发作是有激发条件的，未必一旦感染，立即发作
C.计算机病毒也会破坏 Word 文档
D.计算机病毒无法破坏压缩文件
答案：ABC

99、为支撑安全运维业务融合需要，信息运维服务体系关键支撑系统主要是（　）
A.IT 服务管理系统
B.IT 集中运行监控系统
C.IT 资产管理系统
D.安全审计系统
答案：ABCD

100、群集技术适用于以下场合：（　）。
A.大规模计算如基因数据的分析、气象预报、石油勘探需要极高的计算性能
B.应用规模的发展使单个服务器难以承担负载
C.不断增长的需求需要硬件有灵活的可扩展性
D.关键性的业务需要可靠的容错机制
答案：ABCD

101、软件盗版是指未经授权对软件进行复制、仿制、使用或生产。下面属于软件盗版的形式是（　）
A.使用的是计算机销售公司安装的非正版软件
B.网上下载的非正版软件——“非正版软件”是指使用没花钱的软件
C.自己解密的非正版软件
D.使用试用版的软件
答案：ABC
102、网络运营者建立企业的管理制度和操作流程，以满足法律合规性的要求，避免法律风险，主要包括（　）
A.健全用户信息保护制度
B.落实网络实名制
C.网络安全事件应急预案
D.关键信息基础设施的安全保护义务
答案：ABCD
103、狠抓网络安全责任落实和绩效考核。构建（　）的网络安全管理体系、（　）。
A.管理统一、职责明确、工作界面清晰
B.管理有效、权责明确、工作界面清楚
C.技术体系、监督体系和保障体系
D.技术体系、稽查体系和保障体系
答案：AC
104、下列关于内外网邮件系统说法正确的有（　）。
A.严禁使用未进行内容审计的信息内外网邮件系统
B.严禁用户使用默认口令作为邮箱密码
C.严禁内外网邮件系统开启自动转发功能
D.严禁用户使用互联网邮箱处理公司办公业务
答案：ABCD
105、下列哪些属于服务器硬件的冗余？（　）
A.磁盘冗余
B.电源冗余

C.网卡冗余
D.双机冗余
答案：ABCD
106、下述描述中，正确的是（　）。.
A.设置了交换机的管理地址后，就可使用 Telnet 方式来登录连接交换机，并实现对交换机的管理与配置
B.首次配置交换机时，必须采用 Console 口登录配置
C.默认情况下，交换机的所以端口均属于 VLAN1，设置管理地址，实际上就是设置 VLAN1 接口的地址
D.交换机允许同时建立多个 Telnet 登录连接
答案：BCD
107、国家采取措施，（　）来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏。
A.监测
B.防御
C.处置
D.隔离
答案：ABC
108、属于安全闭环组成部分的是（　）
A.检测
B.响应
C.防护
D.预警
答案：ABCD
109、系统等保定级主要包括以下几个步骤：（　）。
A.系统识别和描述
B.信息系统划分
C.系统的运行维护
D.安全等级确定
答案：ABD
110、《危险化学品安全管理条例》（国务院令第 491 号）的目标：（　）。
A.加强危险化学品的安全管理
B.预防和减少危险化学品事故
C.保障人民群众生命财产安全
D.保护环境
答案：ABCD
111、根据《中国南方电网有限责任公司 IT 服务管理办法（2014 年）》，IT 服务管理事件经理职责：（　）。
A.负责事件解决过程中的协调和监控
B.负责事件升级的判断与执行
C.负责与其它流程经理的沟通与协调
D.负责收集、分析事件数据，发现潜在问题
答案：ABCD
112、逻辑强隔离装置部署在应用服务器与数据库服务器之间，实现（　）功能

A.访问控制
B.网络强隔离
C.地址绑定
D.防 SQL 注入攻击
答案：ABCD
113、物联网工程师证书是根据国家工信部门要求颁发的一类物联网专业领域下工业和信息化领域人才证书，除物联网工程师外，还有哪些方向（　）。
A.节能环保工程师
B.物联网系统工程师
C.智能电网工程师
D.智能物流工程师
答案：ABCD
114、数据备份系统由哪几部分组成：（　）。
A.备份服务器
B.备份网络
C.备份设备
D.备份软件
E.磁盘阵列
答案：ABCD
115、计算机中通常使用的三种数据单位包括（　）。
A.位
B.编码
C.字
D.字节
E.字段
答案：ACD
116、关于“心脏出血”漏洞的阐述正确的是（　）
A.通过读取网络服务器内存，攻击者可以访问敏感数据
B.该病毒可使用户心脏出血
C.心脏出血漏洞是“灾难性的”
D.“心脏出血”漏洞的危险性在于，它要比一般的漏洞潜伏得更深
答案：ACD
117、中间件的优势特点是（　）。
A.面向程序设计人员
B.缩短应用程序开发周期
C.节约开发成本
D.减少系统初期建设成本
答案：ABCD

118、《网络安全法》规定,网络空间主权的内容包括（　）
A.国内主权
B.依赖性主权
C.独立权
D.自卫权

答案：ABCD
119、OSI 安全体系为异构计算机的进程与进程之间的通信安全性，定义了五类安全服务，以下属于这五类安全服务的是（　）
A.机密性
B.完整性
C.鉴别
D.防抵赖
答案：ABCD
120、在系统投运前，应对系统运行的稳定性、安全性进行严格测试，包括检查（　）等。
A.应用系统是否存在安全漏洞和隐患
B.安装最新的补丁软件
C.关闭不必要的服务端口和不必要的服务进程
D.删除不必要的用户
答案：ABCD

答案：√

90、计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

答案：√

91、报文摘要算法 SHA-1 输出的位数是 160 位

答案：√

92、恢复时间目标（RTO）是指灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。

答案：√

93、国务院电信主管部门负责统筹协调网络安全工作和相关监督管理工作。

答案：×

94、在 unix 操作系统中，mv 的意义为 move,主要是将一档案改名或换至另一个目录。

答案：√

95、防火墙技术是一种主动式安全模型

答案：×

96、与网络相关的设施应有明确的标志，未经管理部门许可，任何人不得擅自进入放置网络设备的专用场所，不得擅自打开放置网络设备机柜，不得中断网络设备的供电，专用设备电源插座不得接入其它负载。

答案：√

97、以太网可以传送最大的 TCP 段为 1480 字节

答案：√

98、NTFS 文件系统中,磁盘配额可以限制用户对磁盘的使用量。

答案：√

99、各个二级系统统一部署在一个安全域中，三级系统每个系统独立在一个安全域中。

答案：√

100、在 Linux 中，可以使用、ip-config 命令为计算机配置 IP 地址

答案：×

101、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。
答案：√

102、在信息安全领域，CIA 通常是指：保密性、完整性和可用性。
答案：√

103、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。
答案：√

104、网络与信息都是资产，具有不可或缺的重要价值。
答案：√

105、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。
答案：×

106、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。
答案：×

107、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。
答案：√

108、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。
答案：×

109、主机加固完成后，一般可以有效保证主机的安全性增强。
答案：√

110、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。
答案：√

101、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。

答案：√

102、屏幕保护的木马是需要分大小写。
答案：×

103、安全审计就是日志的记录。
答案：×

104、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。
答案：√

105、Windows NT 中用户登录域的口令是以明文方式传输的。
答案：×

106、操作系统普通用户账号审批记录应编号、留档。
答案：√

107、计算机病毒是计算机系统中自动产生的。
答案：×

108、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。
答案：√
109、4A 系统的建设能够减轻账户管理员的维护工作。
答案：√

110、DHCP 可以向终端提供 IP 地址、网关、DNS 服务器地址等参数。
答案：√

111、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。
答案：√
112、IPS 的过滤器规则不能自由定义。
答案：×
123、IPS 的某些功能和防火墙类似。
答案：√
124、IPS 和 IDS 都是主动防御系统。
答案：×
125、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。
答案：√

126、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。

答案：√

127、Netscreen 防火墙的外网口应禁止 PING 测试，内网口可以不限制。
答案：×
128、OSI 是开放的信息安全的缩写。
答案：×
129、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。
答案：√
130、OSI 中会话层不提供机密性服务。
答案：√
131、SSH 使用 TCP 79 端口的服务。
答案：×
132、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。
答案：×
133、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。
答案：√

134、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。
答案：×

135、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。
答案：√
136、入侵检测可以处理数据包级的攻击。
答案：×
137、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。
答案：√
138、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。
答案：×
139、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。
答案：√
140、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。
答案：×
141、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。
答案：√
142、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。
答案：×
143、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。
答案：×
144、针对不同的攻击行为，IPS 只需要一个过滤器就足够了。
答案：×

145、主机型 IDS 其数据采集部分当然位于其所检测的网络上。
答案：×
146、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。
答案：×
147、IPS 虽然能主动防御，但是不能坚挺网络流量。
答案：×
148、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。
答案：×
149、审计系统进行关联分析时不需要关注日志时间。
答案：×
150、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。
答案：√
151、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。
答案：√
152、侵检测的　　的被容包括系统、网络、数据及用户活动的状态和行为。
答案：√
153、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。
答案：√
154、VPN 的主要特点是通过加密是信息安全的通过 Internet 传递。
答案：√
155、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。
答案：×
156、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。
答案：√
157、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。
答案：√
158、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。
答案：√
159、HTTP 协议是文本协议，可利用回车换行做边界干扰。
答案：√
160、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。
答案：√
161、Oracle 默认情况下，口令的传输方式是加密。
答案：×
162、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）

答案：√
163、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。
答案：√
164、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。
答案：√
165、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。
答案：√

166、Web 攻击面不仅仅是浏览器中可见的内容。
答案：√
167、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。
答案：×
168、暴力猜解不能对 Web 应用进行攻击。
答案：×
169、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。
答案：×
170、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。
答案：×
171、攻击者可以通过 SQL 注入手段获取其他用户的密码。
答案：√
172、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。
答案：√
173、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。
答案：√
174、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。
答案：√
175、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。
答案：√
176、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。
答案：×
177、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。
答案：×
178、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。
答案：√
179、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。
答案：×
180、将公司的机密信息通过互联网络传送时，必须予以加密。

答案：√