江苏省职业技能鉴定

**高级网络与信息安全管理员理论知识试卷**

**一、单项选择(第1题～第300题。选择一个正确的答案，将相应的字母填入题内的括号中。每题1分，满分300分。)**

1.( A )标志着一个从业者的能力因素是否能胜任工作的基本条件，也是实现人生价值的基本条件。

A、职业技能 B、职业能力 C、职业情感 D、职业意识

2.（　B　）的确立，一般与三种因素相联系，即个人的兴趣、生活的需要和共同理想的追求。

 A、职业义务 B、职业态度 C、职业技能 D、职业理想

3.应对信息安全风险的主要目标是什么（B）?

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

4.计算机病毒造成的危害是（ A ）。

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

5.中间件在操作系统、网络和数据库（ A ），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 D.之外

6.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 ）。

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

7.关于OSI参考模型层次划分原则的描述中，错误的是（D ）。

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

8.使用防毒面具时，空气中氧气浓度不得低于（ C ）%，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

9.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（A ），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

10.在 IPsec协议族中，以下哪个协议必须提供验证服务?（A）

A.AN B.ESP C.GRE D.以上都是

209.移动存储介质按需求可以划分为（A ）。

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

11.最简单的防火墙是（B ）。

A.路由器 B.以太网桥 C.交换机 D.网卡

12.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 ）。

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

13.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 ）

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）

14.（ A ）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

15.进程管理可把进程的状态分成（ C ）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

16.下列哪些选项不属于 NIDS 的常见技术?（B）

A.协议分析 B.零拷贝 C.SYNCookie D.IP 碎片重组

17.每个用户电话的处理时间不应超过（ B ）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

18.窃听是一种（ A ）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

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

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

20.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（ A ）账户开放。

A.everyone B.users C.administrator D.guest

21.NTFS文件系统中,（B ）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

22.下列关于防火墙功能的说法最准确的是：（A）。

A.访问控制 B.内容控制 C.数据加密 D.查杀病毒

23.下列哪些措施不是有效的缓冲区溢出的防护措施?（A）

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

24.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（ D ）。

A.文件的集合 B.程序的集合 C.命令的集合 D.数据的集合

25.下列关于防火墙的主要功能包括：（A）

A.访问控制 B.内容控制 C.数据加密 D.查杀病毒

26.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 ）。

A.RAID 2 B.RAID 3 C.RAID 1 D.RAID 5

27.事件的来源有（ D ）。

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

28.下列对防火墙技术分类描述正确的是 ( A )

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

29.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 ）

A.社会工程 B.非法窃取 C.电子欺骗 D.电子窃听

30.计算机机房的净高依机房的面积大小而定，一般为（C）。

A.2--3m B.2.5--3m C.2.5—3.2m D.2.5--3.5m

31.下面关于IIS错误的描述正确的是？（ B ）

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

32.所谓网络内的机器遵循同一“协议”就是指：( A )

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

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

A.WindowsNTServer B.Windows2000Server C.WindowsServer2003 D.WindowsXP

34.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（ A ）文件

A.hosts B.sysconfig C.network D.hostname

35.信息化建设和信息安全建设的关系应当是:( B )

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

36.《中华人民共和国网络安全法》自（B ）起施行。

A.42681 B.42887 C.42736 D.42705

37.Window nt/2k中的.pwl文件是？( B )

A.路径文件 B.口令文件 C.打印文件 D.列表文件

38.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：（ A ）、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

39.从安全属性对各种网络攻击进行分类，阻断攻击是针对（ B ）的攻击。

A.机密性 B.可用性 C.完整性 D.真实性

40.关于Unix版本的描述中，错误的是（ A ）。

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

41.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、（ A ）、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

42.U 盘病毒的传播是借助 Windows 系统的什么功能实现的？( A )

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

43.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（ B ），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

44.AIX中页面空间不能多于所有磁盘空间的（ B ）。

A.0.1

B.0.2

C.0.15

D.0.3

45.下列关于防火墙的说法中错误的是（ B ）。

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

46.在RIP中有三个重要的时钟，其中路由无效时钟一般设为（ B ）。

A.30秒

B.90秒

C.270秒

D.不确定

47.创建虚拟目录的用途是（ C ）。

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

48.下列属于C类计算机机房安全要求范围之内的是（A ）。

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

49.SSL协议比IPSEC协议的优势在于：( A )

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

50.NT/2K模型符合哪个安全级别？( B )

A.B2

B.C2

C.B1

D.C1

51.事件管理流程主要角色有：（ A ）、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

52.综合布线一般采用什么类型的拓扑结构。( D )

A.总线型

B.扩展树型

C.环型

D.分层星型

53.8个300G的硬盘做RAID 1后的容量空间为（A ）。

A.1.2T

B.1.8T

C.2.1T

D.2.4T

54.下列（ A ）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

55.数据备份范围包括（ A ）、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

56.下面是恶意代码生存技术是（ B ）。

A.三线程技术

B.加密技术

C.变换技术

D.本地隐藏技术

57.计算机产生病毒的原因（ D ）。

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

58.对路由器而言，下列（ C ）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

59.下面哪一项通常用于加密电子邮件消息?(A)

A.S/MIME

B.BIND

C.DES

D.SSL

60.攻击者通过扫描（ B ）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

61.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（ C ）。

A.FAT16

B.FAT32

C.NTFS

D.UDF

62.信息系统高危漏洞补丁在漏洞发布（ B ） 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

63.触犯新刑法 285 条规定的非法侵入计算机系统罪可判处(A)

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

64.Windows 操作系统的注册表运行命令是：(B)

A.Regsvr32

B.Regedit

C.Regedit．msc

D.Regedit．Mmc

65.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（ B ）。

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

66.下列说法错误的是（ A ）。

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

67.防火墙的基本构件包过滤路由器工作在OSI的哪一层（ C ）。

A.物理层

B.传输层

C.网络层

D.应用层

68.以下关于 VPN 说法正确的是：(B)

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

69.下面哪种是兼顾业务与安全的最佳策略（ B ）。

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

70.（ A ）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

71.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)

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

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

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

73.针对操作系统安全漏洞的蠕虫病毒根治的技术措施是（ B ）。

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

74.基本磁盘包括（ A ）。

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

75.二进制代码是由（ B ）组成的。

A.0 0

B.0 1

C.1 1

D.1 2

76.HTTPS 采用（ A ）协议实现安全网站访问。

A.SSL

B.IPsec

C.PGP

D.SET

77.安全防护体系要求建立完善的两个机制是（ A ）

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

78.下列不是信息安全的目标的是（ A ）

A.可靠性

B.完整性

C.机密性

D.可用性

79.在 linux 系统中拥有最高级别权限的用户是：(A)

A.root

B.administrator

C.mail

D.nobody

80.下列4项中，不属于计算机病毒特征的是（ D ）。

A.潜伏性

B.传染性

C.激发性

D.免疫性

81.Linux下常用以下哪个命令来查看与目标之间的路由情况（ B ）。

A.Tracert

B.Traceroute

C.Nslookup

D.Ping

82.上网行为审计记录内容应保留（ B ）天以上。

A.30

B.60

C.90

D.120

83.输入enable，进入防火墙（ B ）模式。

A.用户

B.特权

C.关机

D.待机

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

A.监护

B.负责

C.监督

D.监控

85.入侵检测产品主要还存在（ A ）问题。

A.漏报和误报

B.性能低下

C.价格昂贵

D.不实用

86.hash 算法的碰撞是指:(A)

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

87.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 ）

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

88.在设计访问控制模块时，为了简化管理，通常度访问者（ A ），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

89.以下（ B ）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

90.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、（ D ）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

91.由于信息系统分为五个安全保护等级，其安全保护能力是（ B ）。

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

92.目前，安全认证系统主要采用基本（ A ）的数字证书来实现。

A.PKI

B.KMI

C.VPN

D.IDS

93.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（ A ），应立即处理。

A.各种声光告警

B.噪音

C.声响

D.辐射

94.下面（ D ）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

95.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（ A ）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

96.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（ C ）。

A.攻防演练

B.打补丁

C.安全测评

D.漏洞扫描

97.数据库是由逻辑相关的（ B ）组成。

A.记录

B.文件

C.数据

D.信息

98.下列哪一项与数据库的安全有直接关系( A )

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

99.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 ）。

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

100.下列（ A ）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

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 ）

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

102.有关NTFS文件系统优点的描述中，（ C ）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

103.以下那个解决可以帮助减少物理硬件成本？（ B ）

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）

104.微软推荐的有关域中组的使用策略是（ D ）。

A.A-G-P

B.DL-P

C.A-DL-G-P

D.A-G-DL-P

105.应实现设备特权用户的（ A ），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

106.雨天在户外操作电气设备时，操作杆的绝缘部分应有（ A ），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

107.逻辑强隔离装置采用代理模式，也称为（ A ）

A.SQL代理

B.TNS代理

C.ORACLE代理

D.OCI代理

108.如果需要创建一个RAID 10的RAID组，至少需要（ C ）块硬盘？

A.2

B.3

C.4

D.5

109.下列方法（ A ）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

310.boot.ini文件是一个文本文件，其作用是（ A ）。

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

111.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（ B ）措施。

A.修复

B.恢复

C.格式化

D.备份

112.（ A ）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

113.《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（ B ）级。

A.4

B.5

C.6

D.7

114.在Windows操作系统中可以通过安装（ A ）组件创建FTP站点。

A.IIS

B.IE

C.WWW

D.DNS

115.一个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 )

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

116.以下哪个不属于iis自带的服务（ A ）。

A.telnet服务

B.web服务

C.ftp服务

D.smtp服务

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

A.ActiveDirectoryuserandcomputer

B.ActiveDirectorySiteandService

C.ActiveDirectorydomainandtrust

D.GPMC

118.下面不属于虚拟化平台的是（ D ）。

A.Vmware

B.Hyper-v

C.Citrix

D.DOS

119.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？( B )

A.缓冲区溢出

B.地址欺骗

C.拒绝服务

D.暴力攻击

120.破解双方通信获得明文是属于（ A ）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

121.信息安全等级保护的5个级别中，（ B ）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

122.防火墙能够（ B ）。

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

123.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 ）

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

124.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 )

A.Sniffer

B.IDS

C.防火墙

D.路由器

125.风险评估不包括以下哪个活动?( A )

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

126.在"选项"对话框的"文件位置"选项卡中可以设置（ B ）。

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

127.下列RAID技术无法提高读写性能的是（ B ）。

A.RAID0

B.RAID1

C.RAID3

D.RAID5

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

A.4

B.6

C.8

D.12

129.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

130.以下对于拒绝服务攻击描述错误的是：( A )

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

131.信息安全风险的三要素是指:( A )

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

132.从系统结构上来看，入侵检测系统可以不包括（ C ）。

A.数据源

B.分析引擎

C.审计

D.响应

133.依据数据包的基本标记来控制数据包的防火墙技术是( A )

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

134.溢出攻击的核心是（ A ）。

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

135.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（ D ）。

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

136.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 ）。

A.机密性

B.完整性

C.可用性

D.可控性

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

A.通风

B.密闭

C.封闭

D.阴凉

138.电子邮件客户端通常需要用（ A ）协议来发送邮件。

A.仅 SMTP

B.仅 POP

C.SMTP 和 POP

D.以上都不正确

139.DNS在计算机术语中是（A ）？

A.域名服务器

B.邮局协议

C.文件传输服务

D.网页服务器

140.数据安全主要包含（ B ）。

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

141.IIS写权限漏洞是由于开启了IIS上的哪项服务引起的（ B ）。

A.FastCGI

B.Webdav

C.PHP-fpm

D.IIS URL Rewite

142.设备的硬件维护操作时必须戴（ C）。

A.安全帽

B.安全带

C.防静电手套

D.针织手套

143.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 ）。

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

144.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 ）。

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

145.公钥密码基础设施PKI解决了信息系统中的问题。( A )

A.身份信任

B.权限管理

C.安全审计

D.加密

146.下面RAID级别中，数据冗余能力最弱的是？（ A ）

A.RAID 0

B.RAID 1

C.RAID 3

D.RAID 5

147.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（ B ）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

148.更换部件或设备工作变更时，全程工作必须至少有（ B ）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

149.不能防范ARP欺骗攻击的是（ A ）

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

150.简单包过滤防火墙主要工作在( B )

A.链路层/网络层

B.网络层/传输层

C.应用层

D.会话层

151. A.B类计算机机房的空调设备应尽量采用（ A ）。

A.风冷式空调

B.立式的

C.分体的

D.规定中没有要求

152.对DMZ区的描述错误的是（ A ）

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

153.一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 )

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

154.（ A ）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

155.2011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（ A ）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

156.数据保密性指的是（ A ）。

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

157.下面哪种方法不能够更新针对计算机的组策略设定（ B ）。

A.重启机器

B.当前用户重新登陆

C.gpupdate

D.后台更新

158.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：（ B ）。

A.216.12.128.0/24

B.216.12.128.0/20

C.216.12.0.0/16

D.216.12.128.0/11

159.计算机病毒是指（ C ）。

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

160.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（ B ）。

A.可靠性

B.可用性

C.连续性

D.有效性

161.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（ A ）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

162.终端涉密检查的文件动态监控是指（ A ）。

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

163.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（ B ）。

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

164.Internet信息服务在Windows的哪个组件下（ D ）。

A.索引服务

B.网络服务

C.应用程序服务器

D.Windows网络服务

165.SA指的是（ A ）

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

166.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（ B ）。

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

167.以下代码中存在（ A ）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

168.在下面的NT/2K安全模型的空白处，应该是哪个安全组件？( B )

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）

169.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（ C ）使用。

A.领导

B.机房管理员

C.系统管理员

D.系统操作员

170.（ A ）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

171.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（ A ）次全备，保留周期为30天。

A.一

B.二

C.三

D.无

172.冯.诺伊曼机工作方式的基本特点是（ B ）。

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

173.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（ A ）生产中心。

A.低于

B.相当

C.高于

D.不能衡量

174.不属于信息安全与信息系统的“三个同步”的是（ A ）

A.同步管理

B.同步建设

C.同步规划

D.同步投入

175.下列不属于URL的是（ B ）。

A.http://www.163.com

B.www.163.com

C.ftp://www.163.com

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

176.一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（ C ）关系。

A.一对一

B.一对多

C.多对多

D.多对一

177.要使用默认选项安装 WSUS，不须在计算机上安装的软件是（ D ）。

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

178.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：( B )

A.透明模式

B.路由模式

C.代理模式

D.以上都不对

179.下列（ A ）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

180.网页挂马是指（ A ）

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

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

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

182.关于安全风险，下列说法不正确的是（ B ）。

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。

183.使用数据库的主要目的之一是为了解决数据的（ D ）问题。

A.可靠性

B.传输

C.保密

D.共享

184.为了防御网络监听，最常用的方法是：( B )

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

185.目前使用的防病毒软件的作用是（ D ）。

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

186.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( B )

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

187.内容过滤技术的应用领域不包括( B )

A.防病毒

B.网页防篡改

C.防火墙

D.入侵检测

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

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

189.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。（ B ）

A.1，3

B.2，4

C.2，5

D.1，4

190.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？( B )

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

191.Windows 系统下，哪项不是有效进行共享安全的防护措施?( A )

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

192.关于屏蔽子网防火墙，下列说法错误的是（ D ）。

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

193.分布式拒绝服务攻击的简称是（ A ）

A.DDOS

B.DROS

C.LAND

D.SDOS

194.在安全编码中，应该按照（ A ）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

195.入侵检测应用的目的：( D )

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

196.以下能有效预防计算机病毒的方法是（ B ）。

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

197.路由器的路由表包括目的地址，下一站地址以及（ B ）。

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

198.RAID6级别的RAID组的磁盘利用率（N：成员盘个数）为（ C ）。

A.N/（N-2）

B.1

C.（N-2）/N

D.1/2N

199.信息系统安全中应用安全方面不包括（ B ）。

A.安全评估

B.强制访问控制

C.身份鉴别

D.应用通信安全

200.计算机病毒是指编制或者在（ A ）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

201.下面的网络协议中，面向连接的协议是：（ A ）。

A.传输控制协议

B.用户数据报协议

C.网际协议

D.网际控制报文协议

202.在/etc/fstab文件中指定的文件系统加载参数中，参数一般用于CD-ROM等移动设备（ D ）。

A.defaults

B.sw

C.rw和ro

D.noauto

203.Linux文件权限一共10位长度，分成四段，第三段表示的内容是（ C ）。

A.文件类型

B.文件所有者的权限

C.文件所有者所在组的权限

D.其他用户的权限

204.具有很多C语言的功能，又称过滤器的是（ C ）。

A.csh

B.tcsh

C.awk

D.sed

205.一台主机要实现通过局域网与另一个局域网通信，需要做的工作是（ C ）。

A.配置域名服务器

B.定义一条本机指向所在网络的路由

C.定义一条本机指向所在网络网关的路由

D.定义一条本机指向目标网络网关的路由

206.下列关于链接描述，错误的是（ B ）。

A.硬链接就是让链接文件的i节点号指向被链接文件的i节点

B.硬链接和符号连接都是产生一个新的i节点

C.链接分为硬链接和符号链接

D.硬连接不能链接目录文件

207.在局域网络内的某台主机用ping命令测试网络连接时发现网络内部的主机都可以连同，而不能与公网连通，问题可能是（ C ）。

A.主机IP设置有误

B.没有设置连接局域网的网关

C.局域网的网关或主机的网关设置有误

D.局域网DNS服务器设置有误

208.下列文件中，包含了主机名到IP地址的映射关系的文件是：（ B ）。

A./etc/HOSTNAME

B./etc/hosts

C./etc/resolv.conf

D./etc/networks

208.在shell中变量的赋值有四种方法，其中，采用name=12的方法称（ A ）。

A.直接赋值

B.使用read命令

C.使用命令行参数

D.使用命令的输出

209.命令可以从文本文件的每一行中截取指定内容的数据（ D ）。

A.cp

B.dd

C.fmt

D.cut

210.在日常管理中，通常CPU会影响系统性能的情况是：（ A ）。

A.CPU已满负荷地运转

B.CPU的运行效率为30%

C.CPU的运行效率为50%

D.CPU的运行效率为80%

211.在安装Linux的过程中的第五步是让用户选择安装方式，如果用户希望安装部分组件（软件程序），并在选择好后让系统自动安装，应该选择的选项是（ D ）。

A.full

B.expert

C.newbie

D.menu

212.下列信息是某系统用ps –ef命令列出的正在运行的进程，进程是运行Internet超级服务器，它负责监听Internet sockets上的连接，并调用合适的服务器来处理接收的信息（ D ）。

A.root 1 4.0 0.0 344 204? S 17:09 0:00 init

B.root 2 0.0 0.1 2916 1520? S 17:09 0:00 /sbin/getty

C.root 3 0.0 0.2 1364 632? S 17:09 0:00 /usr/sbin/syslogd

D.root 4 0.0 1344 1204? S 17:09 0:10 /usr/sbin/inetd

213.在TCP/IP模型中，应用层包含了所有的高层协议，在下列的一些应用协议中，是能够实现本地与远程主机之间的文件传输工作（ B ）。

A.telnet

B.FTP

C.SNMP

D.NFS

214.当我们与某远程网络连接不上时，就需要跟踪路由查看，以便了解在网络的什么位置出现了问题，满足该目的的命令是（ C ）。

A.ping

B.ifconfig

C.traceroute

D.netstat

215.对名为fido的文件用chmod 551 fido 进行了修改，则它的许可权是（ D ）。

A.-rwxr-xr-x

B.-rwxr--r—

C.-r--r--r—

D.-r-xr-x—x

216.在i节点表中的磁盘地址表中，若一个文件的长度是从磁盘地址表的第1块到第11块，则该文件共占有块号（ B ）。

A.256

B.266

C.11

D.256×10

217.用ls –al 命令列出下面的文件列表，文件是符号连接文件（ D ）。

A.-rw-rw-rw- 2 hel-s users 56 Sep 09 11:05 hello

B.-rwxrwxrwx 2 hel-s users 56 Sep 09 11:05 goodbey

C.drwxr--r-- 1 hel users 1024 Sep 10 08:10 zhang

D.lrwxr--r-- 1 hel users 2024 Sep 12 08:12 cheng

218.DNS域名系统主要负责主机名和之间的解析（ A ）。

A.IP地址

B.MAC地址

C.网络地址

D.主机别名

219.WWW服务器是在Internet上使用最为广泛，它采用的是结构（ B ）。

A.服务器/工作站

B.B/S

C.集中式

D.分布式

220.Linux系统通过命令给其他用户发消息（ C ）。

A.less

B.mesg y

C.write

D.echo to

221.NFS是系统（ C ）。

A.文件

B.磁盘

C.网络文件

D.操作

222.命令可以在Linux的安全系统中完成文件向磁带备份的工作（ B ）。

A.cp

B.tr

C.dir

D.cpio

223.Linux文件系统的文件都按其作用分门别类地放在相关的目录中，对于外部设备文件，一般应将其放在目录中（ C ）。

A./bin

B./etc

C./dev

D./lib

224.在重新启动Linux系统的同时把内存中的信息写入硬盘，应使用命令实现（ D ）。

A.# reboot

B.# halt

C.# reboot

D.# shutdown –r now

225.网络管理具备以下几大功能：配置管理、、性能管理、安全管理和计费管理等（ A ）。

A.故障管理

B.日常备份管理

C.升级管理

D.发送邮件

226.关于代理服务器的论述，正确的是（ A ）。

A.使用internet上已有的公开代理服务器，只需配置客户端。

B.代理服务器只能代理客户端http的请求。

C.设置好的代理服务器可以被网络上任何主机使用。

D.使用代理服务器的客户端没有自己的ip地址。

227.在vi编辑器中的命令模式下，删除当前光标处的字符使用命令（ A ）。

A.＜x＞

B.＜d＞;＜w＞

C.＜D＞

D.＜d＞;＜d＞

228.删除文件命令为：（ D ）。

A.mkdir

B.rmdir

C.mv

D.rm

229.在下列的名称中，不属于DNS服务器类型的是：（ C ）。

A.Primary Master Server

B.Secondary Master Server

C.samba

D.Cache\_only Server

230.网络管理员对WWW服务器进行访问、控制存取和运行等控制，这些控制可在文件中体现（ A ）。

A.http D.conf

B.lilo.conf

C.inet D.conf

D.resolv.conf

231.邮件转发代理也称邮件转发服务器，它可以使用SMTP协议，也可以使用协议（ C ）。

A.FTP

B.TCP

C.UUCP

D.POP

232.启动samba服务器进程，可以有两种方式：独立启动方式和父进程启动方式，其中前者是在文件中以独立进程方式启动（ C ）。

A./usr/sbin/smbd

B./usr/sbin/nmbd

C.r C.samba

D./etc/inet D.conf

233.DHCP是动态主机配置协议的简称，其作用是可以使网络管理员通过一台服务器来管理一个网络系统，自动地为一个网络中的主机分配地址（ D ）。

A.网络

B.MAC

C.TCP

D.IP

234.为了保证在启动服务器时自动启动DHCP进程，应将文件中的dhcpd=no改为dhcpd=yes（ A ）。

A.r C.inet1

B.lilo.conf

C.inet D.conf

D.http D.conf

235.对文件进行归档的命令为（ D ）。

A.dd

B.cpio

C.gzip

D.tar

236.改变文件所有者的命令为（ C ）。

A.chmod

B.touch

C.chown

D.cat

237.（ A ）下面关于i节点描述错误的是？（inode是一种数据结构，vfs中描述文件的相关参数）

A.i节点和文件是一一对应的

B.i节点能描述文件占用的块数

C.i节点描述了文件大小和指向数据块的指针

D.通过i节点实现文件的逻辑结构和物理结构的转换

238.建立一个新文件可以使用的命令为（ D ）。

A.chmod

B.more

C.cp

D.touch(指令改变档案的时间记录。)

239.在下列命令中，不能显示文本文件内容的命令是：（ D ）。

A.more

B.less

C.tail

D.join

240.在使用匿名登录ftp时，用户名为（ B ）。

A.users

B.anonymous

C.root

D.guest

241.在实际操作中，想了解命令logname 的用法，可以键入得到帮助（ D ）。

A.logname --man

B.logname/？

C.help logname

D.logname --help

242.如果LILO被安装在MBR，使用命令即可卸载LILO（ A ）。

A.lilo –u

B.lilo –c

C.lilo –v

D.lilo -V

243.当用命令ls –al查看文件和目录时，欲观看卷过屏幕的内容，应使用组合键（ D ）。

A.Shift+Home

B.Ctrl+ PgUp

C.Alt+ PgDn

D.Shift+ PgUp

244.mc是UNIX风格操作系统的（ C ）。

A.文件编辑器/程序编译器

B.配置网络的窗口工具

C.目录浏览器/文件管理器

D.Samba服务器管理工具

245.i节点是一个长的表，表中包含了文件的相关信息（ D ）。

A.8字节

B.16字节

C.32字节

D.64字节

246.Linux 文件名的长度不得超过个字符（ C ）。

A.64

B.128

C.256

D.512

247.不是邮件系统的组成部分（ B ）。

A.用户代理

B.代理服务器

C.传输代理

D.投递代理

248.在Shell脚本中，用来读取文件内各个域的内容并将其赋值给Shell变量的命令是（ D ）。

A.fold

B.join

C.tr

D.read

249.用ftp进行文件传输时，有两种模式：（ C ）。

A.Word和binary

B.txt和Word Document

C.ASCII和binary

D.ASCII和Rich Text Format

250.某文件的组外成员的权限为只读；所有者有全部权限；组内的权限为读与写，则该文件的权限为（ D ）。

A.467

B.674

C.476

D.764

251.在DNS系统测试时，设named进程号是53，命令通知进程重读配置文件（ D ）。

A.kill –USR2 53

B.kill –USR1 53

C.kill -INT 63

D.kill –HUP 53

252.Apache服务器默认的接听连接端口号是（ C ）。

A.1024

B.800

C.80 (http)

D.8

253.PHP和MySQL的联合使用解决了（ C ）。

A.在Proxy上处理数据库的访问问题

B.在WWW服务器上处理黑客的非法访问问题

C.在WWW服务器上处理数据库的访问问题

D.在Sendmail邮件系统上处理数据库的访问问题

254.OpenSSL是一个（ A ）。

A.加密软件

B.邮件系统

C.数据库管理系统

D.嵌入式脚本编程语言

255.Samba服务器的配置文件是（ D ）。

A.http D.conf

B.inet D.conf

C.r C.samba

D.sm B.conf

256.关于DNS服务器，叙述正确的是（ D ）。

A.DNS服务器配置不需要配置客户端

B.建立某个分区的DNS服务器时只需要建立一个主DNS服务器

C.主DNS服务器需要启动named进程，而辅DNS服务器不需要

D.DNS服务器的root.cache文件包含了根名字服务器的有关信息

257.将Windows C:盘(hda1)安装在Linux文件系统的/winsys目录下，命令是（ B ）。

A.[email=root@l04.edu.cn:%7E#mount]root@l04.edu.cn:~#mount[/email]dev/had1 /winsys

B.[email=root@l04.edu.cn:%7E#mount]root@l04.edu.cn:~#mount[/email]/dev/had1 /winsys

C.[email=root@l04.edu.cn:%7E#mount]root@l04.edu.cn:~#mount[/email]/dev/had1 winsys

D.[email=root@l04.edu.cn:%7E#mount]root@l04.edu.cn:~#mount[/email]dev/had1 winsys

258.设超级用户root当前所在目录为：/usr/local，键入cd命令后，用户当前所在目录为（ B ）。

A./home

B./root

C./home/root

D./usr/local

259.字符设备文件类型的标志是（ B ）。

A.p

B.c

C.s

D.1

260.将光盘CD-ROM（hdc）安装到文件系统的/mnt/cdrom目录下的命令是（ C ）。

A.mount /mnt/cdrom

B.mount /mnt/cdrom /dev/hdc

C.mount /dev/hdc /mnt/cdrom

D.mount /dev/hdc

261.将光盘/dev/hdc卸载的命令是（ C ）。

A.umount /dev/hdc

B.unmount /dev/hdc

C.umount /mnt/cdrom /dev/hdc

D.unmount /mnt/cdrom /dev/hdc

262.在DNS配置文件中，用于表示某主机别名的是：（ B ）。

A.NS

B.CNAME

C.NAME

D.CN

263.可以完成主机名与IP地址的正向解析和反向解析任务的命令是：（ A ）。

A.nslookup

B.arp

C.ifconfig

D.dnslook

264.你的网络有3台DHCP Server 如何手动压缩DHCP数据库：在命令行使用压缩命令，并（ A ）：

A.停止DHCP Server服务，使用Jetpack工具压缩，重新启动DHCP。

B.停止DHCP Server服务，使用Compact命令压缩，重新启动DHCP。

C.备份DHCP数据，使用Jetpack工具压缩，对备份做授权恢复。

D.停止DHCP Server服务, 使用winzip命令压缩，重新启动DHCP

265.作为公司的网络管理员，你在一台安装Windows Server 2008 操作系统的计算机上创建了一个FTP 站点，该站点的主目录位于一个NTFS 分区上。你设置该站点允许用户下载，并可以匿名访问，可是用户报告说他们不能下载服务器上的文件。通过检查你发现这是由于没有设置用户对FTP 站点主目录NTFS 权限造成的，为了让用户能够下载这些文件并最大限度的实现安全性，你应该将FTP 站点主目录的NTFS 权限设置为（ B ）。

A.Everyone 组有完全控制的权限

B.用户帐号IUSR\_Computername 具有读取的权限

C.用户帐号IUER\_Computername 具有安全控制的权限

D.用户帐号IUER\_Computername 具有读取和写入的权限

266.你想查看某台计算机的TCP/IP 连接状态，可以使用（ A ）命令。

A.netstat

B.nbtstat

C.nslookup

D.ipconfig/all

267.为了节省公共网络的IP 地址，你作为网络管理员想利用NAT 服务实现网络地址转换服务。你希望公司局域网内的50 台计算机在连接Internet 时都使用一个相同的 IP 地址，你应该使用NAT 的（ C ）翻译类型。

A.静态NAT

B.动态NAT

C.端口NAT

D.端口映射

268.如果父域的名字是ACME.COM，子域的名字是DAFFY，那么子域的DNS 全名是（ C ）。

A.ACME.COM

B.DAFFY

C.DAFFY.ACME.COM

D.DAFFY.COM

269.小李公司的办公网中没有 DNS 服务器和网关服务器，则小李可以使用（ A ）方法进行互联网中的网页浏览。

A.通过办公网中网页代理服务器

B.通过互联网中的网页代理服务器

C.没有办法实现该功能

D.通过更换网页浏览器

270.GPO（组策略对象）不能链接到哪一个Active Directory对象上（ D ）。

A.域

B.计算机

C.组织单元

D.站点

271.公司需要使用域控制器来集中管理域账户公司，你装域控制器必须具备以下条件（ D ）。

A.操作系统版本是Windows server 2008或者Windows XP

B.本地磁盘至少有一个NTFS分区

C.本地磁盘必须全部是NTFS分区

D.有相应的DNS 服务器支持

272.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。下列关于工作组的叙述中正确的是（ C ）。

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

273.如果想显示计算机ip地址的详细信息，用（ B ）命令。

A.ipconfig

B.ipconfig/all

C.ipconfig/renew

D.showipinfo/all

274.你是一台Windows Server 2008计算机的系统管理员，你可以使用（ C ）工具来管理该计算机中的组帐号。

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

275.在windows server 2008系统中，默认的密码最长使用时间是（ C ）。

A.30天

B.35天

C.42天

D.48天

276.在Windows 2008系统上，可以通过右击文件夹，选择“共享”来创建共享文件夹，以下（ B ）权限级别不属于通过该种方式创建共享应有的权限。

A.读者

B.所有者

C.共有者

D.参与者

277.安装windows server 2008 操作系统后，第一次登录使用的账户是（ A ）。

A.只能使用administrator 登录

B.任何一个用户账户

C.在安装过程中创建用户账号

D.Guest

278.以下哪个不是设置组策略的选项（ A ）。

A.组策略的启用

B.组策略的继承

C.组策略的优先顺序调整

D.组策略的应用

279.SSH的“加密通道”是指在本地端口和远程服务端口之间建立一条加密的通道，保证向该服务器传送的数据是通过加密的。一旦加密通道建立以后，应用程序只需要直接与（ B ）连接，就可以实现向远程服务加密发送数据的功能。

A.远程端口

B.本地端口

C.本地服务

D.远程服务

280.（ C ）代表网络的物理结构。

A.域

B.子网

C.站点

D.域控制器

281.在用Windows2008 Server 实现DNS 时，DNS 区域中下列（ C ）资源记录对于活动目录服务的正常运行是必须的。

A.SOA

B.PTR

C.SRV

D.NS

282.以下有关操作主机描述不正确的是（ C ）。

A.在每个林中，至少有5个指派给一个或多个域控制器的操作主机角色

B.在每个林中，林范围的操作主机角色必须只出现一次

C.在林中的每个域中，域范围的5个操作主机角色必须在每个域中只出现一次

D.在林中，只能传送操作主机，不能查封操作主机

283.在一个域目录树中，父域与其子域具有（ B ）。

A.单向不可传递信任关系

B.双向可传递信任关系

C.双向不可传递信任关系

D.以上都不正确

284.VPN与专线相比最大的优势是（ C ）。

A.可管理性

B.安全性

C.经济性

D.稳定性

285.Windows 2008下诊断DNS故障时，最常用的命令是：（ B ）。

A.NETSTAT

B.NSLOOKUP

C.ROUTE

D.NBTSTAT

286.小明在公司要查询www.xap C.edu.cn这个DNS名称对应的IP地址时，其正确的查询过程是（ A ） ①查询公司默认的DNS服务器 ②查询ROOT DNS服务器 ③查询.CN 域的DNS服务器 ④查询.EDU.CN 域的DNS服务器 ⑤查询.XAP C.EDU.CN 域的DNS服务器。

A.①②③④⑤

B.①③④⑤②

C.①⑤

D.⑤④③②①

287.在DNS的记录类型中MX表示（ C ）。

A.起始授权机构

B.主机地址

C.邮件交换器资源记录

D.指针

288.下列哪一项策略可以用来约束密码的长度不小于7个字符（ B ）。

A.密码最短存留期

B.密码长度最小值

C.强制密码历史

D.密码必须符合复杂性要求

289.在 Windows2008中，下列（ B ）主机负责域的增加和删除。

A.架构主机

B.域命名主机

C.RID主机

D.PDC仿真主机

290.用户名最长可以达到（ C ）个字符。

A.10

B.15

C.20

D.25

291.（ D ）帐户默认情况下是禁用的。

A.Administrators

B.Power users

C.Administrator

D.Guest

292.管理员在Windows Server 2008 系统上配置动态磁盘，他希望配置的卷读写效率最高，应该创建（ B ）卷。

A.简单

B.带区----条带区

C.镜像

D.RAID-5

293.公司处在单域的环境中，你是域的管理员，公司有两个部门：销售部和市场部，每个部门在活动目录中有一个相应的OU，分别是SALES和MARKET。有一个用户TOM要从市场部调动到销售部工作。TOM的账户原来存放在组织单位MARKET里，你想将TOM的账户存放到组织单位SALES里，应该通过（ B ）来实现此功能 。

A.在组织单位MARKET里将TOM的账户删除，然后在组织单位SALES里新建

B.直接将TOM的账户拖动到组织单位SALES里

C.将TOM使用的计算机重新加入域

D.复制TOM的账户到组织单位里，然后将MARKET里TOM的账户删除

294.小黑是公司的网管，公司的计算机处于单域环境中，小胡因病请了3个月病假。出于安全考虑，小黑希望在这三个月内小胡的域用户账户不能使用，三个月后可以再使用，那么小黑应该（ B ）。

A.锁定小胡的域用户账户，三个月后再启用

B.禁用小胡的域用户账户，三个月后再启用

C.将小胡的域用户账户有效期设置为3个月

D.将小胡的域用户账户登录时间设置为3个月后允许登录

295.Windows 2003的NTFS文件系统具有对文件和文件夹加密的特性。域用户user1加密了自己的一个文本文件myfile.txt。他没有给域用户user2授权访问该文件。下列叙述正确的是（ A ）。

A.对文件加密后可以防止非授权用户访问，所以user不能读取该文件

B.User1需要解密文件myfile.txt才能读取

C.User2如果对文件myfile.txt具有NTFS完全控制权限，就可以读取该文件

D.User2如果对文件myfile.txt具有NTFS完全控制权限，就可以读取该文件

296.公司的网络采用单域结构进行管理，管理员在DC上为销售部建立组账户的时候发现他不能将组账户设置为通用组，如下所示，产生这种现象最可能的原因是（ C ）。

A.管理员没有以Administrator账户登录DC

B.管理员选择的组类型为安全组

C.域的模式为混合模式

D.管理员不是Enterprise Admins组中的成员

297.你公司的办公网络是Windows 2003域环境。你想使员工无论使用哪台计算机都能获得他在前一次登录使用的桌面环境，该员工可以修改并保存桌面环境。你使用（ B ）能实现。

A.本地配置文件

B.漫游配置文件

C.强制配置文件

D.临时配置文件

298.某公司所有的计算机都处在工作组环境下，并且利用DHCP动态分配主机的IP地址。一天早上，管理员接到一个员工小黑打来的电话，员工说他使用的Windows XP计算机无法访问公司局域网里面的其它计算机，而昨天还是可以的。管理员在该员工的Windows XP计算机上登录，并使用ipconfig /all命令查看网络配置信息，发现IP地址是169.254.25.38。你知道这可能是由于（ C ）原因导致的。

A.用户自行指定了IP地址

B.IP地址冲突

C.动态申请地址失败

D.以上都不正确

299.公司有一台文件服务器，管理员已经对Windows Server 2003上的用户数据进行了每周备份，他还想对注册表、引导文件、com+对象也进行备份。最好应该（ D ）来实现该目的。

A.配置Windows Server2003备份来备份系统分区

B.使用BackSys.exe命令进行备份

C.使用VBSCRIPT脚本语言编写一个备份脚本

D.配置Windows Server 2003备份来备份系统状态数据

300.通常情况下当DHCP客户的IP地址租用期满后，客户机会（ D ）。

A.继续使用该IP地址

B.使用专用IP自动编址

C.广播DHCPREQUEST消息请求续租

D.重新启动租用过程来租用新的IP地址

**一、判断(第1题～第180题。对下列语句进行判断，将相应的√或× 填入题内的括号中。每题1分，满分180分。)**

1.ICMP协议数据单元封装在IP数据报中传送。（√ ）

2.地址池是作用域除保留外剩余的IP地址（× ）

3.专用移动存储介质交换区与保密区的登录密码可以一致。（× ）

4.防火墙采用何种通讯方式是由用户的网络环境决定的，用户需要根据自己的网络情况，合理的确定防火墙的通讯模式。（√ ）

5.Telnet的端口号为23（√ ）

6.weblogic server的缺省安全策略中，对口令的长度做了约束。（√ ）

7.所有的信息系统与数据网络运行设备，任何人不得随意拆除、损坏或移动，设备的更换、拆卸和移动必须填报作业计划，并经批准后方可实施。（√ ）

8.有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。（√ ）

9.在Windows操作系统中，cookie文件可以帮助域名解析（× ）

10.提供电子邮件安全服务的协议是SET（× ）

11.RAID 5最大的好处是在一块盘掉线的情况下，RAID照常工作，相对于RAID 0必须每一块盘都正常才可以正常工作的状况容错性能好多了。（√ ）

12.P2V 将正在运行的虚拟机从一台物理计算机迁移到另一台物理计算机上。（× ）

13.信息运维部门应制定信息系统定检计划（包括巡检项目及周期），定期对机房环境、服务器、数据库、中间件、应用系统、网络设备、安全设备等信息系统进行巡检，及时发现存在的各种安全隐患。（√ ）

14.备份最常用的3种备份策略：完全备份、差别备份、增量备份。（√ ）

15.重新格式化硬盘可以清除所有病毒（× ）

16.向有限的空间输入超长的字符串是缓冲区益出攻击手段。（√ ）

17.在linux操作系统中，install命令的作用是安装或升级软件或备份数据。（√ ）

18.网络安全是保护网络系统的硬件、软件及系统中的数据，防止因偶然或恶意的原因而遭到破坏、更改、泄露，保证网络系统的正常运行，服务不中断。（√ ）

19.修改系统错误文件是防病毒软件的一项基本功能。（× ）

20.文件压缩变换是一个单项加密过程。（× ）

21.关闭默认共享不符合公司桌面终端管理要求。（× ）

22.RAID 1其磁盘的利用率却只有50%，是所有RAID级别中最低的。（√ ）

23.组策略无法实现仅允许使用指定U盘。（× ）

24.不定期对设备及应用系统运行情况进行统计分析，对设备及应用系统的缺陷及故障进行登记，并做好运行维修记录，每月、每年提供运行报告报送信息部门。（× ）

25.ICMP协议属于因特网中的网络层协议（√ ）

26.RIP协议引入路由保持机制的作用是防止网络中形成路由环路。（√ ）

27.组策略中包含两部分:“计算机配置”、“用户配置”。其中“用户配置”是针对用户的配置，只在所有用户帐户上生效。（√ ）

28.网络安全策略主要包括两大部分，即访问控制策略、信息加密策略。（√ ）

29.CiSco 公司只做防火墙产品。（× ）

30.B/S结构具有分布性特点，业务扩展简单方便，维护简单方便，共享性强。（√ ）

31.计算机木马不具有自我复制性和传染性，不会像病毒那样自我复制、刻意感染其他文件。（√ ）

32.一般缺陷：短时间内不会恶化成危急或严重的缺陷，应列入月检修计划进行处理。（√ ）

33.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内容、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。（√ ）

34.中间件处于操作系统与应用软件之上。（× ）

35.支持端口认证的协议是IEEE802.1x（√ ）

36.在外包服务商合作协议中要求关键岗位的外协驻场人员备用机制以保证服务连续；对于必要的岗位变更和人员退出，无需提前提出人员申请。（× ）

37.同一台计算机加入域的同时也可以加入工作组。（× ）

38.在Windows环境下，租约期满后，DHCP客户端可以向DHCP服务器发送一个Dhcprequest报文来请求重新租用IP地址（√ ）

39.关于Windows 2003系统DHCP服务器，客户机的地址租约续订是由客户端软件自动完成的。（√ ）

40.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。（√ ）

41.报文摘要算法SHA-1输出的位数是160位（√ ）

42.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。（√ ）

43.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。（× ）

44.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。（√ ）

45.防火墙技术是一种主动式安全模型（× ）

46.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。（√ ）

47.以太网可以传送最大的TCP段为1480 字节（√ ）

48.NTFS文件系统中,磁盘配额可以限制用户对磁盘的使用量。（√ ）

49.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。（√ ）

50.在Linux 中，可以使用.ip-config命令为计算机配置 IP地址（× ）

51.业务恢复人员在完成对应用系统的切换工作后，不需要进行应用验证，确保应用正常运行，可以直接上线。（× ）

52.用命令行方式可以将计算机加入域。（√ ）

53.新增应用系统接入网络前不必进行病毒例行检测。（× ）

54.FTP服务的主要问题是登陆的用户名口令是明文方式发送给服务器。（√ ）

55.若通过桌面系统对终端施行 IP、MAC 地址绑定，该网络 IP 地址分配方式应为静态。（√ ）

56.IBM小型机列出网卡状态及路由信息的命令是：#netstat -rn 。（√ ）

57.就算用户手动删除了某张用户表，也有机会找回。（√ ）

58.在RIP协议中，默认60秒更新一次路由（× ）

59.sqlserver应该社会自日志审核无法追踪回溯安全事件。（√ ）

60.在网络拥塞的情况下，发送电子邮件后，接收者可能过几个小时后才能收到。（√ ）

61.采用FDM技术进行多路复用时，复用后的信号的带宽通常大于复用前所有信号的带宽之和。（√ ）

62.操作系统分三类:批处理系统、分时系统、实时系统。（√ ）

63.外部合作单位人员进行开发、测试工作要先与公司签署保密协议。（√ ）

64.切实按照有关规范要求，做好机房的防雷工作，确保网络设备和各类服务器的安全。（√ ）

65.网络管理员调试网络，使用（ping目标地址-a）命令来持续查看网络连通性（× ）

66.信息系统应急预案既要制定、修订和完善，更需要演练与处理（√ ）

67.若一直得不到回应，DHCP客户端总共会广播4次请求（√ ）

68.使用IEEE 802.lq协议，最多可以配置4094个VLAN（√ ）

69.在unix操作系统中，cp这个指令的意义是复制（"COPY"）,也就是将一个或多个档案复制成另一个档案或者是将其复制到另一个目录去。（√ ）

70.3DES的密钥长度为128（× ）

71.应配备集中运行监控系统实现对所有服务器、网络设备、安全设备、数据库、中间件、应用系统的集中监控。（√ ）

72.如果内部网络的地址网段为 192. 168. 1. 0/24 ， 需要用到防火墙的地址映射才能使用户上网。（× ）

73.ICMP不属于路由协议。（√ ）

74.快速生成树协议的是IEEE802.1d（× ）

75.知识库一级目录由各个知识管理员负责建立，二级目录由知识专家建立。（× ）

76.数据库系统的数据共享是指多个用户共享一个数据文件。（√ ）

77.web攻击面不仅仅是浏览器中可见的内容（√ ）

78.磁盘阵列有硬件磁盘阵列和软件磁盘阵列之分，目前市面上的磁盘阵列系统大部份是软件磁盘阵列,硬件盘阵列较少。（× ）

79.数据库系统的基本特征是数据共享性、数据独立性和冗余度小。（√ ）

80.地址池是作用域应用排除范围之后剩余的IP地址（√ ）

81.优先级为中的事件响应与解决时限要求是：响应时限要求为1小时，解决时限要求为2天。（√ ）

82.领网权是国家主权在网络空间的继承和延伸。（√ ）

83.透明模式下的防火墙多端口接在同一交换机会形成环路。（√ ）

84.客户端采用DhcpDecline报文来拒绝DHCP服务器提供的IP地址（√ ）

85.各单位对业务相对独立、安全要求高的管理信息系统，应为其单独分配IP地址段，也可与其他管理信息系统共用地址段。（× ）

86.入侵检测系统可以替代防火墙进行网络安全防护。（× ）

87.优先级为紧急的事件响应与解决时限要求是：响应时限要求为20分钟，解决时限要求为4小时。（√ ）

88.国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。（√ ）

89.能够支持突发通信流量的广域网协议是帧中继。（√ ）

90.IBM小型机故障定位方法包括小型机I/O柜上的显示面板上的Checkpoints信息Error Code和SRNs。（√ ）

91.IPSEC不可以做到签发证书。（√ ）

92.在无线局域网中，AP（无线接入点）工作在OSI模型的数据链路层 。（√ ）

93.应定期或不定期对网络与服务器主机进行安全扫描和检测，对扫描结果及时进行分析，采取相应补救措施。（√ ）

94.由发布实施人员验证发布的信息是否完整准确并审批授权进行发布。（× ）

95.基本磁盘包括扩展分区和逻辑分区。（× ）

96.在Linux系统中，在etc/hostname文件中查看一台主机的名称和完整域名（√ ）

97.对于外委开发项目，在信息系统的开发、维护过程中，为保障企业有关信息的安全，项目主管单位必须要求施工方（开发商或系统集成商）签订保密协议。（√ ）

98.《网络安全法》开始施行的时间是2017 年6月1日（√ ）

99.OSPF网络被划分为各种区域，其中作为区域之间交换路由信息的是主干区域 （√ ）

100.在RIP协议中，如果判定路由的去向，依据的参数是路由跳数。（√ ）

101.TCP协议使用3次握手机制建立连接,当请求方发出SYN连接请求后,等待对方回答SYN,ACK,这样可以防止建立错误的连接。（√ ）

102.驻留在多个网络设备上的程序在短时间内同时产生大量的请求消息冲击某Web服务器,导致该服务器不堪重负,无法正常响应其他合法用户的请求,这属于DDoS攻击。（√ ）

103.WINDOWS注册表是WINDOWS的核心,通过修改注册表,可以对系统进行限制和优化。（√ ）

104.在活动目录用户和计算机中,在“查看”菜单上,单击“高级功能”,在对象的属性中出现安全标签。（√ ）

105.安全组提供了一种有效方式来指派网上资源的访问权。（√ ）

106.DDOS是指集中式拒绝服务攻击。（× ）

107.典型的Web服务器配置缺陷包括使用默认证书、保留默认内容、启用目录列表功能、启用危险的HTTP方法、启用Web代理功能和虚拟主机的默认主机配置缺陷。（√ ）

108.Web应用安全的核心问题在于用户可以提交任意输入。（√ ）

109.影响Web安全的关键因素可以归纳为不成熟的安全意识、独立的开发过程、欺骗性的简化、迅速发展的威胁形势、资源与时间限制、在技术上强其所难这六个因素。（√ ）

110.上传检查文件扩展名和检查文件类型是同一种安全检查机制。（× ）

111.禁止不需要的端口和禁用不需要的协议可以有效地减少Web服务器的攻击面。（√ ）

112.web漏洞发掘方式主要分为黑盒模式和白盒模式。 （√ ）

113.XSS跨站脚本漏洞主要影响的是客户端浏览用户。（√ ）

114.对于只提供万维网服务的Windows服务器而言,443端口是需要禁止的（× ）。

115.WAF指的是web防火墙。（√ ）

116.SSL不仅保证连接的安全性,它本身也参与HTTP事务。 (B )

117.网页文件最好放在NTFS的磁盘分区内,是因为利用NTFS权限增加网页安全性（√ ）。118.SQL注入攻击不会威胁到操作系统的安全。（× ）

119.SQL注入一般可通过网页表单直接输入。 （√ ）

120.Nmap是一款优秀的端口扫描工具。（√ ）

121.网络边界保护中主要采用防火墙系统,为了保证其有效发挥作用,应当避免在内网和外网之间存在不经过防火墙控制的其他通信连接。 （√）

122.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。 （√）

123.增量备份是备份从上次进行完全备份后更改的全部数据文件 （×）

124.已经联网的用户有对计算机信息信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的权利。 （×）

125.TCP FIN属于典型的端口扫描类型。 （√）

126.用于描述DNS数据库段的数据是一种ASCII文本数据。 （√）

127.SOCKS是一种Socket的实现机制。 （×）

128.区分服务也叫分用服务,传输层用于向上传送通信数据。 （×）

129.RIPv2最多有15个网络直径,OSPFv2最多有128个网络直径。 （×）

130.DHCP响应消息包含DHCP请求消息。 （√）

131.ARPA是一种与Mac地址及IP地址相关的一种协议。 （×）

132.地址请求是一种ARP服务请求。 （×）

133.权威服务器是PKI中一种发放安全证书的服务器。 （×）

134.带宽是一种跨网络信息数量的评估数据。 （√）

135.绑定确认是一种必选数据。 （×）

136.桌面终端管理系统为了发现机器名和MAC地址,必须在部署之前打开UDP端口161。 （×）

137.SMTP服务的默认端口号是23,POP3服务的默认端口号是110。 （×）

138.TCP/IP协议中,UDP比TCP协议开销少。 （√）

139.网络通信协议中存在安全上的缺陷,攻击者有可能不必攻破密码体制即可获得所需要的信息或服务。这种安全问题称为系统缺陷。 （×）

140.利用ARP协议可以进行跨网段主机发现。 （×）

141.半连接扫描也需要完成TCP协议的三次握手过程。 （×）

142.IPSEC 协议族通过AH 和ESP 两种模式完成数据的验证功能,同时ESP 还可以完成数据的加密功能。 （√）

143.GRE 是Generic Routing Encapsulation 通用路由封装的简称。 （√）

144.标准GRE 协议配置时,虚拟Tunnel 接口的源端、目的端不一定要为固定公网IP 地址。（√）

145.VPN与专线相比最大的优势是经济性。 （√）

146.IPSec VPN为保证通过公用网络平台传输数据的专用性和安全性主要VPN主要采用4项技术来保证安全,这4种技术分别是隧道技术、加解密技术、密钥管理技术和入侵检测技术。（×）

147.MPLS VPN中的PE之间转发的数据包中都有两层标签,外层公网标签和内层私网标签。（√）

148.IPSec协议的AH头和ESP头可以单独或组合使用。（√）

149.IP报文头中的协议(Protocol)字段标识了其上层所使用的协议,当上层为TCP协议时该字段值为6,当上层为UDP协议时该字段值为17。 （√）

150.SYN Flood攻击是攻击者通过向服务端发送大量SYN报文,却不做第三步确认,造成服务端存在大量未完全建立的TCP连接,占用服务端的资源。 （√）

151.欧拉函数(81)=54。 （√）

152.仿射密码加密函数y??ax?b?mod26,其中a要与26互素。 （√）

153.DES的明文分组长度是位,加密时迭代次。 （×）

154.非对称密码体制也称公钥密码体制,即其所有的密钥都是公开的。 （×）

155.在GF(2)上x4+ 1可约,可写成(x + 1)4。 （√）

156.产生序列密码中的密序列的一种主工具是移位寄存器。 （√）

157.设H是一个Hash函数.如果寻找两个不同的消息x和x'使得H(x)=H(x')在.算上是不可行的.则称H是随机碰撞的。 （×）

158.在DES加密过程中,S盒对加密的强度没有影响。 （×）

159.McEliece密码体制适用于数字签名。 （√）

160.CFB模式在加密时必须有一个初始向量,而且可以用明文传给接收方。 （√）

161.加密和解密都是在计算机机控制下进行的。 （×）

162.尽管双重DES不等价于使用一个56位密钥的单重DES.但有一种被称为中途相遇攻击的破译方法会对它构成威胁。 （√）

163.公钥密码体制的理论基础是有限域上的离散对数。 （√）

164.设计序列密码体制的关键就是要设计一种产生密钥序列的方法。 （√）

165.“一次一密”属于序列密码中的一种。 （√）

166.PKI和PMI在应用中必须进行绑定,而不能在物理上分开。 （×）

167.路由器能隔离广播风暴。 （√）

168.首次配置路由器,就可以使用telnet方式登陆路由器进行管理。 （×）

169.标准访问列表ACL的编号是1到100内。 （×）

170.网络管理主要包括配置管理、故障管理、性能管理、计费管理、安全管理。 （√）

171.为了保障网络安全,防止外部网对内部网的侵犯,多在内部网络与外部网络之间设置防火墙。 （√）

172.计算机病毒只会破坏计算机的操作系统,而对其他网络设备不起作用。 （×）

173.当硬件配置相同时,代理防火墙对网络运行性能的影响要比包过滤防火墙小。 （×）

174.在传统的包过滤、代理和状态检测3类防火墙中,只有状态检测防火墙可以在一定程度上检测并防止内部用户的恶意破坏。 （√）

175.防火墙一般采用“所有未被允许的就是禁止的”和“所有未被禁止的就是允许的”两个基本准则,其中前者的安全性要比后者高。 （√）

176.用户标识码UID和组标识码GID的编号从501开始,若创建用户帐号或组群时未指定标识码,则系统会自动指定从编号501开始且尚未使用的号码。 （×）

177.Iptables不能阻止ICMP包。 （×）

178.Linux的3组权限位的顺序是“属主-属组-其他”,每组中位的次序是“执行-写-读”。（×）

179.存储在活动目录中的用户账户,启用了单点登录功能,当用户登录到工作站时输入一次账号和密码,就可以访问网络上所有授权他访问的资源。 （√）

180.我们在使用Windows Server 2008的DHCP服务时,当客户机租约使用时间超过租约的50时,客户机会向服务器发送DHCPDISCOVER数据包,以更新现有的地址租约。 （×）

**一、多项选择(第1题～第120题。选择两个或两个以上正确的答案，将相应的字母填入题内的括号中。每题1分，满分120分。)**

1.《网络安全法》规定,国家维护网络安全的主要任务是（ ABCD ）

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

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（ BC）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》

3.数字签名不能通过（ABD ）来实现的。

A.认证

B.程序

C.签字算法

D.仲裁

4.以下哪一项属于信息欺骗的范畴（ BCD ）

A.会话劫持

B.IP欺骗

C.重放攻击

D.社交工程

5.强制访问控制用户与访问的信息的读写关系正确的是（ AC ）。

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

E.下写:用户级别等于文件级别的写操作

6.在设计密码的存储和传输安全策略时应考虑的原则包括（ ABD ）。

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

7.下面说法正确的是（ BD ）

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

8.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“（ABCD ）”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

9.下列（ ABC ）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

10.（ ABCD ）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

11.日志分析重点包括（ ABCD ）

A.源

B.请求方法

C.请求链接

D.状态代码

12.《网络安全法》的网络运营者包括（ ABD ）

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

13.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（ABCD ）

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

14.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（ ACD）。

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

15.下列关于跨站请求伪造的说法正确的是（ABCD ）

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

16.对于防火墙不足之处，描述正确的是（ ABC ）

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

17.公司统一组织对（AC ）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

18.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（ ABC ）

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

19.“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（ ABCD ）

A.IP地址

B.用户名和密码

C.上网时间

D.Cookie信息

20.下列情况违反“五禁止”的有（ABCD ）。

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

21.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（ ABCD ）

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

22.静电产生方式有（ ABCD ）。

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

23.灭火的基本方法有（ ABC ）。

A.隔离法

B.窒息法

C.冷却法

D.水灭法

24.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（ AB ）。

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

25.以下有可能与计算机染上病毒有关的现象是（ ABC ）

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

26.管理信息大区内部安全域划分原则包括（ACD ）。.

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

27.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：（ ABD ）

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

28.数据传输完整性与保密性要求：（ ABD ）。

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。

29.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：（ BCD ）。

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

30.典型的拒绝服务攻击方式包括（ ABCD ）

A.Ping of death

B.SYN Flood

C.UDP Flood

D.Teardrop

31.Virtual Private Network技术可以提供的功能有：（ ABC ）

A.提供AccessControl

B.加密数据

C.信息认证和身份认证

D.划分子网

32.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、（ ABCD ）、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

33.环型拓扑结构的缺点是（ ABCD ）。.

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

34.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（ABD ）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

35.以下对交换机工作方式的描述，正确的是（ ABD ）

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

36.风险评估的内容包括（ ABCD ）

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

37.下列关于《网络安全法》的说法正确的有：（ ABCD ）

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

38.Ping本机IP地址返回有效结果说明（ AB ）。

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

39.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（ ABCD ）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

40.下列RAID技术中采用奇偶校验方式来提供数据保护的是（ BC ）。

A.RAID1

B.RAID3

C.RAID5

D.RAID10

41.下列属于系统安全的技术是（ ACD）

A.防火墙

B.加密狗

C.认证

D.防病毒

42.下列（ ABC ）属于活动目录的逻辑结构。

A.域树

B.域林

C.组

D.域控制器

43.下列哪些软件是用来接收电子邮件的客户端软件？（ ABD ）.

A.Foxmail

B.TheBat

C.ICQ

D.OutlookExpress

44.防火墙有哪些部属方式？(ABC)

A.透明模式

B.路由模式

C.混合模式

D.交换模式

45.对UNIX中的trap指令，下列说法中（ AD ）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

46.活动目录安装后，管理工具里有增加（ ABC ）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

47.下列关于网络安全法的说法错误的有（ AB ）。

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。

48.以下属于计算机硬件系统的功能部件的是（ ACDE ）。

A.运算器

B.操作系统

C.存储器

D.输入\输出设备

E.控制器

49.下面关于计算机病毒说法正确的是（ABC ）

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

50.防火墙能够作到些什么？(ABCD)

A.包过滤

B.包的透明转发

C.阻挡外部攻击

D.记录攻击

51.使用中间件带来的好处有（ ABCD）。

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

52.对于远程访问VPN须制定的安全策略有：（ ABCD ）

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

53.加密技术包括两个元素 （ AD ）。

A.算法

B.编码

C.数字

D.密钥

E.字节

54.以下有助于减少收到垃圾邮件数量的是（ ABD ）

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

55.系统投运阶段的工作需遵循公司关于（ BCD ）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

56.IPSAN由（ ABD ）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

57.（ ABCD ）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

58.数字证书含有的信息包括（ ABD ）。

A.用户的名称

B.用户的公钥

C.用户的私钥

D.证书有效期

59.在数据库安全配置中，下列（ ABCD ）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

60.工作许可人安全责任包括（ ABCD ）。

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

61.以下关于计算机病毒说法，错误的是（ ABDE ）。

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

62.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（ ABCD ）

A.运营指标

B.资源使用情况

C.业务承载

D.业务承载

63.《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（ ABC ）

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

64.关于《网络安全法》以下正确的是（ ABCD ）

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

65.公共信息网络安全监察工作的一般原则:（ ABCD ）。

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

66.采用混合运维外包策略时，（ ABC ）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

67.下列可以引起安全配置错误的是（ AD ）

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

68.对于网络安全的特征,下列说法正确的有（ ABCD ）

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

69.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（ ABCD ），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

70.网络安全事件应急预案应当按照事件发生后的（ A ）、（ B ）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

71.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（ABD ）

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

72.下述描述中，正确的是（ BCD ）。

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

73.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（ ABC ）

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

74.应用系统进行设计时，设计方案应满足以下要求：（ ABCD ）。

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

75.下列情形中会引起内存溢出的有（ ABCD ）

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

76.（ ABCD ）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

77.中间件的产生是为了解决哪些关键问题（ ABCD ）。

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

78.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（ ABCD ）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

79.以下几个选项中，哪些项是对DBWR后台进程的错误描述：（ BCD）。

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

80.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（ ABCD ）等的维护。

A.基本信息

B.价值信息

C.使用信息

D.维护信息

81.（ ABD ）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

82.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(ABCD)

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

83.实体安全技术包括：（ ABD ）。

A.环境安全

B.设备安全

C.人员安全

D.媒体安全

84.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（ ABC ），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

85.木马在建立连接时必须条件的是（ ABC）

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

86.《网络安全法》的意义包括（ABCD ）

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

87.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（ ABCD ）

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

88.群集技术适用于以下场合：（ ABCD ）。

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

89.RIP（路由信息协议）作为路由协议采用方式有误的是哪几种。(BCD)

A.距离向量

B.链路状态

C.分散通信量

D.固定查表

90.计算机犯罪的主要特征包括（ ACD ）。

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

91.关于黑客攻击中肉鸡的认识，正确的是（ ABC ）

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

92.资产处置方式包括报废、盘亏、（ABCD ）、作价投资、出租、抵押、抵债等。

A.调拨

B.转让

C.置换

D.捐赠

93.未来的防火墙产品与技术应用有哪些特点：（ BCD ）。

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

94.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（ ABCD ）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

95.在IPSec中，使用IKE建立通道时使用的端口号，错误的是（ ACD ）。

A.TCP500

B.UDP500

C.TCP50

D.UDP50

96.你是一台Windows Server 2008计算机的系统管理员，你不可以使用（ABD ）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

97.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（ ABCD ）。

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

98.《网络安全法》在完善个人信息保护法律制度方面的亮点有：（ ABCD ）

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

99.信息系统建转运管理审查点审查要求包括（ ABC ）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

100.下列方法中（ ABCD ）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

101.下列对垃圾邮件说法正确的是（ BCD ）

A.用户减少电子邮件的使用完全是因为垃圾邮件的影响

B.降低了用户对Email的信任

C.邮件服务商可以对垃圾邮件进行屏蔽

D.有价值的信息淹没在大量的垃圾邮件中，很容易被误删

102.下列情况（ ABCD ）会给公司带来安全隐患

A.外部技术支持人员私自接入信息内网

B.使用无线键盘处理涉案及敏感信息

C.某业务系统数据库审计功能未开启

D.为方便将开发测试环境和业务系统运行环境置于同一机房

103.网络战的形式是（ ACD ）

A.网络情报战

B.火力攻击

C.网络舆论战

D.网络摧毁战

104.ARP欺骗的防御措施包括（ ABCD ）

A.使用静态 ARP 缓存

B.使用三层交换设备

C.IP与MAC地址绑定

D.ARP防御工具

105.Who is可以查询到的信息包括（ABCD ）

A.域名所有者

B.域名及IP地址对应信息

C.域名注册、到期日期

D.域名所使用的DNS Servers

106.设备标签标识内容应包括如下信息：（ABC ）等。

A.设备名称

B.设备编号

C.投运时间

D.设备价格

107.为保证网络系统的正常维护，及时排除故障，信息网络运行管理部门必须视具体情况配备必需的（ ABCD ）。

A.仪器

B.仪表

C.工具

D.备品备件

108.属于绝缘体的物体是（ ABC ）。

A.蜡纸

B.橡胶

C.塑料

D.人体

109.中间件基本特点有（ ABCD ）。

A.满足大量应用的需要

B.运用于多种硬件和OS平台

C.支持标准的协议

D.支持标准的接口

110.常用查看系统各项设备信息命令，以下正确的是（ ABCD ）。

A.#bdf列出已加载的逻辑卷及其大小信息

B.#mount列出已加载的逻辑卷及其加载位置

C.#uname–a列出系统ID号，OS版本及用户权限等信息

D.#hostname列出系统网络名称

111.IT硬件资产清查盘点是中国南方电网有限责任公司资产清查盘点工作的重要组成部分，清查盘点方式包括：（ ABCD ）。

A.定期清查盘点

B.不定期清查盘点

C.专项清查盘点

D.全面清查盘点

112.停电作业在作业前必须完成（ABCD ）等安全措施，以消除工作人员在工作中电击的可能性。

A.停电及验电

B.挂接地线

C.悬挂标示牌

D.设置临时遮拦

113.边界路由描述错误的是指（ ABD ）。

A.单独的一种路由器

B.次要的路由器

C.路由功能包含在位于主干边界的每一个LAN交换设备中

D.路由器放在主干网的外边

114.根据《中国南方电网有限责任公司信息运维服务体系（2015年）》，运行调度管理包括（ ABCD ）业务事项。

A.作业计划管理

B.方式安排

C.运行监测与分析

D.运维调度指挥

115.信息系统的安全保护等级的叙述，正确的有（ BC ）。

A.第五级，信息系统受到破坏后，会对南方电网公司、公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益

B.第二级，信息系统受到破坏后，会对南方电网公司、公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全

C.第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害

D.第一级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害

116.南网云设计思路包括（ ABC ）

A.统一入口

B.统一标准

C.统一运维

D.统一使用

117.下面关于计算机病毒的特征，正确的是（ ACD ）

A.任何计算机病毒都有破坏性

B.计算机病毒也是一个文件，它也有文件名

C.有些计算机病毒会蜕变，即每感染一个可执行文件，就会演变成另一种形式

D.只要是计算机病毒，就一定有传染的特征

118.服务目录内容主要包括（ ABCD ）；服务目录内容需要每年定期进行回顾和更新，确保服务目录的内容符合公司业务需求。

A.服务名称

B.服务目标

C.服务时间

D.例外情况

119.下列关于OSPF协议的说法正确的是（ ABD ）。

A.OSPF支持基于接口的报文验证

B.OSPF支持到同一目的地址的多条等值路由

C.OSPF是一个基于链路状态算法的边界网关路由协议

D.OSPF发现的路由可以根据不同的类型而有不同的优先级

120.端口扫描的扫描方式主要包括（ ABCD ）

A.全扫描

B.半打开扫描

C.隐秘扫描

D.漏洞扫描