# 1.当前我国的信息安全形势为（ ）

A、遭受敌对势力的入侵、攻击、破坏。

B、针对基础信息网络和重要信息系统的违法犯罪持续上升。

C、全社会的信息安全等级保护意识仍需加强。

D、总体情况尚可，少量的基础信息网络和重要信息系统安全隐患严重。

**正确答案：** ABC

# 2.以下对信息系统安全建设整改工作的复杂性和艰巨性说法正确的是（ ）

A、政策性和技术性很强。

B、涉及范围广。

C、信息系统安全加固改造，需要国家在经费上予以支持

D、跨省全国联网的大系统结构复杂运行实时保障性高、数据重要，加固改造周期长。

**正确答案：** ABCD

# 3.访问控制列表可实现下列哪些要求（ ）

A、允许202.38.0.0/16网段的主机可以使用协议HTTP访问129.10.10.1

B、不让任何机器使用Telnet登录

C、使某个用户能从外部远程登录

D、让某公司的每台机器都可经由SMTP发送邮件

E、允许在晚上8:00到晚上12:00访问网络

**正确答案：** ABDE

# 4.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（ ）。

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

**正确答案：** AC

# 5.如果只对主机地址为172.16.30.55进行访问列表的设置，下面各项正确的有（ ）

A、172.16.30.55 0.0.0.255

B、172.16.30.55 0.0.0.0Oracle中的三种系统文件分别是.数据文件 DBF

C、any 172.16.30.55

D、host 172.16.30.55

**正确答案：** BD

# 6.Oracle中的三种系统文件分别是（ ）

A、数据文件 DBF

B、控制文件 CTL

C、日志文件 LOG

D、归档文件 ARC

**正确答案：** ABC

# 7.关于表分区的说法正确的有（ ）

A、表分区存储在表空间中

B、表分区可用于任意的数据类型的表

C、表分区不能用于含有自定义类型的表

D、表分区的每个分区都必须具有明确的上界值

**正确答案：** AC

# 8.HASH加密使用复杂的数字算法来实现有效的加密,其算法包括（ ）

A、MD2;

B、MD4;

C、MD5;

D、Cost256

**正确答案：** ABC

# 9.根据《关于信息安全等级保护的实施意见》，信息系统安全等级保护应当遵循什么原则？（ ）

A、明确责任，共同保护

B、依照标准，自行保护

C、同步建设，动态调整

D、指导监督，保护重点

**正确答案：** ABCD

# 10.根据《信息安全等级保护管理办法》，关于信息系统安全保护等级的划分，下列表述正确的是（ ）。

A、第一级，信息系统受到破坏后，会对公民、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、第四级，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

E、第五级，信息系统受到破坏后，会对国家安全造成特别严重损害

**正确答案：** ABCDE

# 11.根据《计算机信息系统安全保护条例》，计算机信息系统（ ）应当同步落实相应的安全措施。

A、规划

B、设计

C、建设

D、维护

**正确答案：** ABCD

# 12.经测评，计算机信息系统安全状况未达到国家有关规定和标准的要求的（ ）

A、委托单位应当根据测评报告的建议，完善计算机信息系统安全建设

B、重新提出安全测评委托

C、另行委托其他测评机构进行测评

D、自行进行安全测评

**正确答案：** AB

# 13.根据《信息安全等级测评工作细则》，关于测评和自查工作，以下表述正确的是（ ）。

A、第三级计算机信息系统应当每年至少进行一次安全自查和安全测评

B、第四级计算机信息系统应当每半年至少进行一次安全自查和安全测评

C、第五级计算机信息系统应当依据特殊安全要求进行安全自查和安全测评

D、自查报告连同测评报告应当由计算机信息系统运营、使用单位报地级以上市公安机关公共信息网络安全监察部门

**正确答案：** ABCD

# 14.根据《公安厅关于计算机信息系统安全保护的实施办法》，关于公安机关的进行安全检查的要求，下列表述正确的是（ ）。

A、对第三级计算机信息系统每年至少检查一次

B、对第四级计算机信息系统每半年至少检查一次

C、对第五级计算机信息系统，应当会同国家指定的专门部门进行检查

D、对其他计算机信息系统应当不定期开展检查

**正确答案：** ABCD

# 15.根据《计算机信息系统安全保护条例》，计算机信息系统的运营、使用单位接到公安机关要求整改的通知后拒不按要求整改的，由公安机关处以（ ）。

A、罚款5000元

B、拘留15日

C、警告

D、停机整顿

**正确答案：** CD

# 16.根据《计算机信息系统安全保护条例》规定，第二级以上计算机信息系统的运营、使用单位计算机信息系统投入使用前未经符合国家规定的安全等级测评机构测评合格的 ，由公安机关（ ）。

A、责令限期改正，给予警告

B、逾期不改的，对单位的主管人员、其他直接责任人员可以处五千元以下罚款，对单位可以处一万五千元以下罚款

C、有违法所得的，没收违法所得

D、情节严重的，并给予六个月以内的停止联网、停机整顿的处罚

E、必要时公安机关可以建议原许可机构撤销许可或者取消联网资格

**正确答案：** ABCDE

# 17.根据《公安厅关于计算机信息系统安全保护的实施办法》，信息安全等级测评机构申请备案（ ）

A、一般应当向地级以上市公安机关公共信息网络安全监察部门提出申请

B、承担省直和中央驻粤单位信息安全等级测评工作的机构，直接向省公安厅公共信息网络安全监察部门提出申请

C、一般应当向公安部公共信息网络安全监察部门提出申请

D、一般应当向县级以上市公安机关公共信息网络安全监察部门提出申请

**正确答案：** AB

# 18.根据《信息安全等级保护管理办法》，安全保护等级为第三级以上的计算机信息系统应当选用符合下列条件的安全专用产品（ ）

A、产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格

B、产品的核心技术、关键部件具有我国自主知识产权

C、产品研制、生产单位及其主要业务、技术人员无犯罪记录

D、产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能

E、对国家安全、社会秩序、公共利益不构成危害

**正确答案：** ABCDE

# 19.《计算机信息网络国际联网安全保护管理办法》规定，任何单位和个人不得从事下列危害计算机信息网络安全的活动：（ ）

A、故意制作、传播计算机病毒等破坏性程序的

B、未经允许，对计算机信息网络功能进行删除、修改或者增加的

C、未经允许，对计算机信息网络中存储、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

D、未经允许，进入计算机信息网络或者使用计算机信息网络资源的

**正确答案：** ABCD

# 20.我国信息安全等级保护的内容包括（ ）

A、对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输和处理这些信息的信息系统分等级实行安全保护

B、对信息系统中使用的信息安全产品实行按等级管理

C、对信息安全从业人员实行按等级管理

D、对信息系统中发生的信息安全事件按照等级进行响应和处置

E、对信息安全违反行为实行按等级惩处

**正确答案：** ABCD

# 21.目前，我国在对信息系统进行安全等级保护时，划分了5个级别，包括（ ）

A、专控保护级

B、强制保护级

C、监督保护级

D、指导保护级

E、自主保护级

**正确答案：** ABCDE

# 22.等级保护对象受到破坏时所侵害的客体包括的三个方面为：（ ）

A、公民、法人和其他组织的合法权益

B、社会秩序、公共利益

C、国家安全

D、个人利益

**正确答案：** ABC

# 23.等级保护对象受到破坏后对客体造成侵害的程度归结为哪三种（ ）

A、造成轻微损害

B、造成一般损害

C、造成严重损害

D、造成特别严重损害

**正确答案：** BCD

# 24.根据定级指南，信息系统安全包括哪两个方面的安全：（ ）

A、业务信息安全

B、系统服务安全

C、系统运维安全

D、系统建设安全

**正确答案：** AB

# 25.作为定级对象的信息系统应具有如下基本特征：（ ）

A、具有唯一确定的安全责任单位

B、具有信息系统的基本要素

C、承载单一或相对独立的业务应用

D、单位具有独立的法人

**正确答案：** ABC

# 26.信息安全和系统服务安全受到破坏后，可能产生以下危害后果（ ）

A、影响行使工作职能

B、导致业务能力下降

C、引起法律纠纷

D、导致财产损失

**正确答案：** ABCD

# 27.安全保护等级为第三级以上的计算机信息系统应当选用符合下列条件的安全专用产品：（ ）

A、产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格。

B、产品的核心技术、关键部件具有我国自主知识产权。

C、产品研制、生产单位及其主要业务、技术人员无犯罪记录。

D、产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能。

**正确答案：** ABCD

# 28.三级及以上信息系统的物理访问控制应满足以下要求：（ ）

A、机房出入口应安排专人值守，控制、鉴别和记录进入的人员。

B、需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

C、应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

D、重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

**正确答案：** ABCD

# 29.三级及以上信息系统的网络安全审计应满足以下（ ）要求：

A、应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

B、审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

C、应能够根据记录数据进行分析，并生成审计报表；

D、应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

**正确答案：** ABCD

# 30.三级及以上信息系统的应用安全身份鉴别应满足以下（ ） 要求：

A、应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

B、应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

C、应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

D、应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

**正确答案：** ABCD

# 31.三级及以上信息系统的应用安全资源控制应满足以下（ ）要求：

A、应能够对一个时间段内可能的并发会话连接数进行限制。

B、应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。

C、应能够对系统服务水平降低到预先规定的最小值进行检测和报警。

D、应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

**正确答案：** ABCD

# 32.三级信息系统的人员录用应满足以下要求：（ ）。

A、应指定或授权专门的部门或人员负责人员录用。

B、应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核。

C、应签署保密协议。

D、可从所有人员中选拔从事关键岗位的人员，并签署岗位安全协议。

**正确答案：** ABCD

# 33.三级信息系统的管理制度包括如下（ ）内容。

A、应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

B、应对安全管理活动中的各类管理内容建立安全管理制度；

C、应对要求管理人员或操作人员执行的日常管理操作建立操作规程；

D、应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

**正确答案：** ABCD

# 34.三级信息系统的系统定级包括如下（ ）内容。

A、应明确信息系统的边界和安全保护等级。

B、应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由。

C、应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。

D、应确保信息系统的定级结果经过相关部门的批准。

**正确答案：** ABCD

# 35.三级信息系统的外包软件开发包括如下（ ）内容。

A、应根据开发需求检测软件质量。

B、应在软件安装之前检测软件包中可能存在的恶意代码。

C、应要求开发单位提供软件设计的相关文档和使用指南。

D、应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

**正确答案：** ABCD

# 36.三级信息系统的恶意代码防范管理包括如下（ ）内容。

A、应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

B、应指定专人对网络和主机进行恶意代码检测并保存检测记录。

C、应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

D、应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

**正确答案：** ABCD

# 37.对三级信息系统的人员配备包括如下（ ）内容。

A、应配备一定数量的系统管理员、网络管理员、安全管理员等。

B、应配备专职安全管理员，不可兼任。

C、关键事务岗位应配备多人共同管理。

D、应配备系统审计员，加强对管理员工作的监督。

**正确答案：** ABCD

# 38.三级信息系统的测试验收包括如下（ ）内容。

A、应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；

B、在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

C、应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；

D、应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

**正确答案：** ABCD

# 39.三级信息系统的等级测评包括如下（ ）内容

A、在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。

B、应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。

C、应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

D、应指定或授权专门的部门或人员负责等级测评的管理。

**正确答案：** ABCD

# 40.三级信息系统的安全服务商选择包括如下（ ）内容

A、应确保安全服务商的选择符合国家的有关规定。

B、应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。

C、应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

D、应确保选定的安全服务商提供质量保证。

**正确答案：** ABCD

# 41.近年来，网络信息安全备受大家关注。其中，网络信息安全的基本属性包括（ ）。

A、保密性

B、完整性

C、可用性

D、可控性

E、抗否认性

**正确答案：** ABCD

# 42.信息安全等级保护测评工作原则，主要包括：（ ）。

A、规范性原则

B、整体性原则

C、最小影响原则

D、保密性原则

**正确答案：** ABCD

# 43.某信息系统1被定为3级，测评的指标选择可能有：（ ）。

A、S3A3G3

B、S3A1G3

C、S3A2G3

D、S1A3G3

**正确答案：** ABCD

# 44.等级保护测评准则的作用，主要有：（ ）。

A、指导系统运营使用单位进行自查

B、指导评估机构进行检测评估

C、监管职能部门参照进行监督检查

D、规范测评内容和行为

**正确答案：** ABCD

# 45.网络空间成为（ ）之外的第五空间，是国家主权延伸的新疆域。

A、领土

B、领海

C、领空

D、太空

E、河流

**正确答案：** ABCD

# 46.如何实现技术突破？（ ）

A、明确国家信息安全产业发展主管部门，加大经费投入力度，确立发展方向

B、加快实施可信计算应用示范工程，有序推进国产化替代

C、整合现有资金渠道，支持核心技术和关键产品研发

D、联合产业上下游企业，组建自主技术产品联合工作组，推进产品整合

E、坚持以应用促发展，带动信息安全产品和系统具有完全自主知识产权

**正确答案：** ABCDE

# 47.我国互联网发展有哪些特征？（ ）

A、互联网经济快速发展

B、互联网的社会影响逐步加深

C、互联网规模持续扩大

D、互联网应用更新换代不断加快

**正确答案：** ABCD

# 48.领导人在推特上开通微博的国家包括（ ）。

A、美国

B、中国

C、朝鲜

D、德国

E、俄罗斯

**正确答案：** ABDE

# 49.下列属于自媒体时代发展的历程的是（ ）。

A、书信媒体

B、网络媒体

C、传统媒体

D、新媒体

E、自媒体

**正确答案：** CDE

# 50.当一个舆情事件爆发时，我们应该哪些角度的网评类稿子？（ ）

A、直接解读

B、官方文章

C、花絮评论

D、情感倾诉

E、以上都是

**正确答案：** ABCDE

# 51.以下属于传统犯罪手法与网络技术相融合的案例的是（ ）。

A、借助淫秽色情网站传播木马程序进而实施网络盗窃

B、借助实施黑客攻击进而进行敲诈勒索

C、借助盗窃QQ号码实施视频诈骗

D、借助技术操控的赌博活动实施诈骗

E、借助网络钓鱼盗窃信用卡信息实施信用卡犯罪

**正确答案：** ABCDE

# 52.以互联网和手机为信息载体的新媒体有（ ）。

A、Facebook

B、Twitter

C、MSN

D、人民日报

E、QQ

**正确答案：** ABCDE

# 53.发展中国家互联网发展的相关问题有哪些？（ ）

A、垃圾邮件

B、网络安全

C、知识产权

D、网络犯罪

E、电子商务

**正确答案：** ABCDE

# 54.电子政务安全保障体系包括安全技术系统、安全管理系统两部分。下列各项中，属于安 全技术系统的包括（ ） 。

A、物理安全

B、安全标准

C、网络基础平台安全

D、信息资源层安全

E、业务应用层安全

**正确答案：** ACDE

# 55.信息安全给当今信息化社会中的每一个人、每一个组织、每一个机构、每一个国家都带 来了相当大的困惑。其中，信息安全的特征包括（ ） 。

A、网络信息安全是系统的安全

B、网络信息安全是动态的安全

C、网络信息安全是静态的安全

D、网络信息安全是跨时空、无边界的安全

E、网络信息安全是非传统的安全

**正确答案：** ABDE

# 56.我国信息安全攻防能力不足表现在（ ） 。

A、产品普遍“带病上岗”

B、我国不能有效抵御西方国家的网络攻击

C、在 X86 架构下，我国发现美国的攻击

D、重要信息系统对外依赖严重

E、骨干网络 20%-30%的网络设备都来自于思科

**正确答案：** ABC

# 57.（ ）造成了我国信息安全技术实力较弱。

A、缺乏自主技术体系

B、对新兴技术信息安全反应过慢

C、对网络犯罪技术缺乏有效应对

D、没有掌握核心技术

E、对新兴技术信息盲目跟风

**正确答案：** ABCDE

# 58.当今，我国的网络安全工作面临新的复杂形势， 网络安全面临新的挑战，体现在 （ ） 。

A、网上、微博中的大 V、造谣、煽动

B、贫富差距已经就业住房等问题

C、社会发展不平衡

D、人们的思想意识、价值观、道德观多元化

E、重要的系统风险管理滞后，非常态化

**正确答案：** ACDE

# 59.我国网络不良信息治理存在的问题有（ ） 。

A、法律建设不完善

B、管理体制效率不高

C、非正式的管制方式导致管制成本高昂

D、行业自律不到位

E、没有监管

**正确答案：** ABCD

# 60.在寻找治理与网络言论自由的平衡点时决不能触碰的底线有（ ） 。

A、法律法规的底线

B、社会主义这个制度的底线

C、国家利益的底线

D、公民合法权益的底线

E、社会公共秩序的底线

**正确答案：** ABCDE

# 61.以下关于我国当前网络违法犯罪情况的描述中正确的是（ ） 。

A、网络淫秽色情、赌博、诈骗依然呈高发态势

B、各类传统违法犯罪向网上扩散蔓延

C、黑客攻击破坏活动十分猖獗

D、境内外敌对势力的破坏活动突出

E、侵犯人权等违法犯罪十分突出

**正确答案：** ABCD

# 62.当前网络违法犯罪活动的特点包括（ ） 。

A、形成分工合作的利益链条

B、跨地域作案

C、隐蔽性强

D、规模缩小

E、传统犯罪手法与网络技术相融合

**正确答案：** ABCE

# 63.电子政务和电子商务网络的基本安全需求有（ ）。

A、严格的保密要求

B、信息交换：准确.及时

C、严格的权限管理

D、严格的程序和流程要求

E、确保责任明确

**正确答案：** ABCDE

# 64.信息安全是保障信息化顺利推行的基础性.战略性的工作，它关系到国家的（ ）。

A、经济安全

B、政治安全

C、文化安全

D、国防安全

E、社会的稳定

**正确答案：** ABCDE

# 65.70%-80%的网络设备都来自于思科，同时几乎所有的（ ）都由思科掌握。

A、超级核心节点

B、移动网络节点

C、国际交换节点

D、国际汇聚节点

E、互联互通节点

**正确答案：** ACDE

# 66.我国互联网治理的目标包括（ ）。

A、积极发展互联网，推进现代化建设

B、依法保护社会公众互联网言论自由

C、依法保护集团政治利益不受侵害

D、互联网要成为传播社会主义先进文化的前沿阵地

E、以上都是正确的

**正确答案：** ABE

# 67.下列观点错误的有（ ）。

A、网络审查出于特定的政治目的

B、网络审查影响网络经济的发展

C、网络审查影响了司法的公正

D、网络审查侵犯了个人隐私

E、网络审查影响了我国网民的工作学习

**正确答案：** ABCDE

# 68.计算机病毒的主要来源有（ ）

A、黑客组织编写

B、计算机自动产生

C、恶意编制

D、恶作剧

**正确答案：** ACD

# 69.发现感染计算机病毒后，应采取哪些措施（ ）

A、断开网络

B、使用杀毒软件检测、清除

C、如果不能清除，将样本上报国家计算机病毒应急处理中心

D、格式化系统

**正确答案：** ABC

# 70.我国移动化转型刚刚起步，需要具备（ ）。

A、移动化的舆情处理能力

B、移动化的舆情回应能力

C、移动化的舆情感应能力

D、移动化的舆情评估能力

E、以上都是正确的

**正确答案：** ABD

# 71.终端安全有三大目标，分别是（ ）。

A、数据安全

B、技术安全

C、账户安全

D、连接安全

E、支付安全

**正确答案：** ACE

# 72.根据冯·诺依曼体系结构，计算机由（ ）构成。

A、运算器

B、控制器

C、存储器

D、输入设备

E、输出设备

**正确答案：** ABC

# 73.计算机网络具有（ ）等特点。

A、资源共享

B、数据通信能力

C、均衡负载互相协作

D、分布处理

E、提高计算机可靠性

**正确答案：** ABCDE

# 74.按照网络规模和所跨越的地理位置分类，计算机网络分为（ ）。

A、局域网

B、外围网

C、有线网

D、城域网

E、广域网

**正确答案：** ABCDE

# 75.管理信息系统开发的原则有（ ）。

A、完整性

B、相关性

C、适应性

D、可靠性

E、自主开发

**正确答案：** ABCDE

# 76.管理的基本职能有（ ）。

A、计划

B、组织

C、领导

D、控制

E、协调

**正确答案：** ABCD

# 77.市场营销组合过程中的四个变量是（ ）。

A、产品

B、用户

C、价格

D、销售渠道

E、促销

**正确答案：** ACDE

# 78.MIS需求调查常用的方法有（ ）。

A、开调查会或个别访问

B、收集报表资料

C、书面调查

D、参加业务实践

E、技能大赛

**正确答案：** ABCD

# 79.系统测试过程中，如果按照“自底向上”原则进行测试，需要完成（ ）三个阶段。

A、模块测试

B、功能测试

C、子系统测试

D、系统总测试

E、黑盒测试

**正确答案：** ACD

# 80.按照应用分类，网络服务器分为（ ）。

A、数据库服务器

B、WEB服务器

C、VOD服务器

D、邮件服务器

E、文件服务器

**正确答案：** ABCDE

# 81.计算机病毒传播的途径有（ ）。

A、不可移动的硬件设备，如ASIC

B、移动存储设备，如U盘

C、网络

D、点对点通信系统

E、无线通信系统

**正确答案：** ABCDE

# 82.作为信息系统评价指标的有（ ）。

A、可靠性

B、经济性

C、正确性

D、准时性

**正确答案：** ABCD

# 83.下面哪些属于开发信息系统的生命周期（ ）。

A、可行性研究与战略规划

B、系统分析

C、系统实现与测试

D、系统更换

**正确答案：** ABC

# 84.按照不同的管理对象和管理职能将企业（系统）划分为子系统的数量多少与（ ）有关。

A、产品品种的多少

B、产品复杂程度

C、工艺特点

D、生产设备

**正确答案：** ABC

# 85.专家系统的核心部分是（ ）。

A、知识库子系统

B、知识获取子系统

C、咨询解释子系统

D、推理子系统

**正确答案：** ABCD

# 86.企业信息系统的开发工作小组的开发人员有（ ）。

A、管理人员

B、程序设计人员

C、系统分析设计人员

D、最高层领导

**正确答案：** ABC

# 87.企业信息系统硬件的逻辑配置方案有（ ）。

A、多用户系统

B、单机

C、计算机网络

D、工作站方案

**正确答案：** ABCD

# 88.数据库的物理设计的主要内容是（ ）。

A、建立逻辑模型

B、确定存储结构

C、确定数据存放位置

D、确定存储分配

**正确答案：** BCD

# 89.绘制系统结构图时要遵循模块设计的原则是（ ）。

A、低耦合

B、高聚合

C、作用范围要在控制范围之中

D、独立性

**正确答案：** ABC

# 90.企业信息系统开发的四个阶段是（ ）。

A、系统设计

B、系统评价

C、系统分析

D、系统实施

**正确答案：** ABCD

# 91.离散型生产制造的主要类型有（ ）。

A、大量生产

B、成批生产

C、单件生产

D、客户化生产

E、多品种生产

**正确答案：** ABC

# 92.企业信息化投资过程中，了解相关产品信息时，可以从以下（ ）方面入手。

A、性价比

B、市场占有率

C、先进性

D、适用性

E、兼容性

**正确答案：** ABCDE

# 93.网络管理的功能主要包括（ ）。

A、配置管理

B、性能管理

C、计费管理

D、故障管理

E、安全管理

**正确答案：** ABCDE

# 94.数据物理备份的方法有（ ）。

A、利用SQL语言提取数据

B、适用恢复管理器备份

C、热备份

D、数据库冷备份

E、操作系统备份

**正确答案：** BCDE

# 95.以下关于对称加密的说法正确的是（ ）

A、在对称加密中，只有一个密钥用来加密和解密信息

B、在对称加密中，用到了二个密钥来加密和解密信息，分别是公共密钥和私用密钥

C、对称加密是一个简单的过程，双方都必需完全相信对方，并持有这个密钥的备份

D、对称加密的速度非常快，允许你加密大量的信息而只需要几秒钟

**正确答案：** ACD

# 96.在建网时，设计IP地址方案首先要（ ）。

A、给每一硬件设备分配一个IP地址

B、选择合理的IP寻址方式

C、保证IP地址不重复

D、动态获得IP地址时可自由安排

**正确答案：** BD

# 97.网络按通信方式分类，可分为（ ）。

A、点对点传输网络

B、广播式传输网络

C、数据传输网

D、对等式网络

**正确答案：** AB

# 98.下列说法中属于ISO/OSI七层协议中应用层功能的是（ ）。

A、拥塞控制

B、电子邮件

C、防止高速的发送方的数据把低速的接收方淹没

D、目录查询

**正确答案：** BD

# 99.如果发现网络变得很慢，经过观察，发现网络冲突增加很多，以下哪些情况会引起此类故障（ ）。

A、电缆太长

B、有网卡工作不正常

C、网络流量增大

D、电缆断路

**正确答案：** ABC

# 100.下列关于中继器的描述正确的是（ ）。

A、扩展局域网传输距离

B、放大输入信号

C、检测到冲突，停止传输数据到发生冲突的网段

D、增加中继器后，每个网段上的节点数可以大大增加

**正确答案：** ABC

# 101.从技术角度看，网络信息安全与保密的技术特征主要表现在系统的（ ）

A、可靠性

B、可用性

C、保密性

D、完整性

E、不可抵赖性

**正确答案：** ABCDE

# 102.拒绝服务攻击的后果是（ ）

A、信息不可用

B、应用程序不可用

C、系统宕机

D、带宽增加

E、阻止通信

**正确答案：** ABCE

# 103.网络安全是在分布网络环境中对（ ）提供安全保护。

A、信息载体

B、信息的处理、传输

C、硬件

D、软件

E、信息的存储、访问

**正确答案：** ABE

# 104.计算机安全级别包括（ ）。

A、D级

B、C1级

C、C2级

D、C3级

E、B1级

**正确答案：** ABCE

# 105.网络安全应具有以下特征（ ）。

A、保密性

B、可靠性

C、完整性

D、可用性

E、可控性

**正确答案：** ABCDE

# 106.屏蔽子网防火墙体系结构中的主要组件有（ ） 。

A、参数网络

B、堡垒主机

C、内部路由器

D、外部路由器

E、内部主机

**正确答案：** CDE

# 107.数字签名方案主要包括的阶段有（ ） 。

A、系统初始化

B、签名产生

C、签名验证

D、加密阶段

E、解密阶段

**正确答案：** ABC

# 108.在设计因特网防火墙时，网络管理员必须做出几个决定（ ）

A、防火墙的姿态

B、机构的整体安全策略

C、防火墙的经济费用

D、防火墙系统的组件或构件

E、机构的地理环境

**正确答案：** ABCD

# 109.网络安全工作的目标包括（ ）

A、信息机密性;

B、信息完整性;

C、服务可用性;

D、可审查性

**正确答案：** ABCD

# 110.智能卡可以应用的地方包括（ ）

A、进入大楼；

B、使用移动电话；

C、登录特定主机；

D、执行银行和电子商务交易

**正确答案：** ABCD

# 111.计算机信息系统安全保护的目标是要保护计算机信息系统的（ ）

A、实体安全

B、运行安全

C、信息安全

D、人员安全

**正确答案：** ABCD

# 112.计算机信息系统的运行安全包括（ ）

A、系统风险管理

B、审计跟踪

C、备份与恢复

D、电磁信息泄漏

**正确答案：** ABC

# 113.实施计算机信息系统安全保护的措施包括（ ）

A、安全法规

B、安全管理

C、组织建设

D、制度建设

**正确答案：** AB

# 114.计算机信息系统安全管理包括（ ）

A、组织建设

B、事前检查

C、制度建设

D、人员意识

**正确答案：** ACD

# 115.公共信息网络安全监察工作的性质（ ）

A、是公安工作的一个重要组成部分

B、是预防各种危害的重要手段

C、是行政管理的重要手段

D、是打击犯罪的重要手段

**正确答案：** ABCD

# 116.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

**正确答案：** ABCD

# 117.安全员应具备的条件: （ ）

A、具有一定的计算机网络专业技术知识

B、经过计算机安全员培训，并考试合格

C、具有大本以上学历

D、无违法犯罪记录

**正确答案：** ABD

# 118.网络操作系统应当提供哪些安全保障（ ）

A、验证(Authentication)

B、授权(Authorization)

C、数据保密性(Data Confidentiality)

D、数据一致性(Data Integrity)

E、数据的不可否认性(Data Nonrepudiation)

**正确答案：** ABCD

# 119.Windows NT的"域"控制机制具备哪些安全特性？（ ）

A、用户身份验证

B、访问控制

C、审计(日志)

D、数据通讯的加密

**正确答案：** ABC

# 120.从系统整体看，下述那些问题属于系统安全漏洞（ ）

A、产品缺少安全功能

B、产品有Bugs

C、缺少足够的安全知识

D、人为错误

E、缺少针对安全的系统设计

**正确答案：** ABCDE

# 121.应对操作系统安全漏洞的基本方法是什么？（ ）

A、对默认安装进行必要的调整

B、给所有用户设置严格的口令

C、及时安装最新的安全补丁

D、更换到另一种操作系统

**正确答案：** ABC

# 122.严格的口令策略应当包含哪些要素（ ）

A、满足一定的长度，比如8位以上

B、同时包含数字，字母和特殊字符

C、系统强制要求定期更改口令

D、用户可以设置空口令

**正确答案：** ABCD

# 123.计算机安全事件包括以下几个方面（ ）

A、重要安全技术的采用

B、安全标准的贯彻

C、安全制度措施的建设与实施

D、重大安全隐患、违法违规的发现事故的发生

**正确答案：** ABCD

# 124.计算机案件包括以下几个内容（ ）

A、违反国家法律的行为

B、违反国家法规的行为

C、危及、危害计算机信息系统安全的事件

D、计算机硬件常见机械故障

**正确答案：** ABC

# 125.重大计算机安全事故和计算机违法案件可由（ ）受理

A、案发地市级公安机关公共信息网络安全监察部门

B、案发地当地县级（区、市）公安机关治安部门

C、案发地当地县级（区、市）公安机关公共信息网络安全监察部门

D、案发地当地公安派出所

**正确答案：** AC

# 126.现场勘查主要包括以下几个环节（ ）

A、对遭受破坏的计算机信息系统的软硬件的描述及被破坏程度

B、现场现有电子数据的复制和修复

C、电子痕迹的发现和提取，证据的固定与保全

D、现场采集和扣押与事故或案件有关的物品

**正确答案：** ABCD

# 127.计算机安全事故原因的认定和计算机案件的数据鉴定（ ）

A、是一项专业性较强的技术工作

B、必要时可进行相关的验证或侦查实验

C、可聘请有关方面的专家，组成专家鉴定组进行分析鉴定

D、可以由发生事故或计算机案件的单位出具鉴定报告

**正确答案：** ABCD

# 128.计算机病毒的特点（ ）

A、传染性

B、可移植性

C、破坏性

D、可触发性

**正确答案：** ACD

# 129.计算机病毒按传染方式分为（ ）

A、良性病毒

B、引导型病毒

C、文件型病毒

D、复合型病毒

**正确答案：** BCD

# 130.计算机病毒的危害性有以下几种表现（ ）

A、删除数据

B、阻塞网络

C、信息泄漏

D、烧毁主板

**正确答案：** ABC

# 131.计算机病毒由（ ）部分组成

A、引导部分

B、传染部分

C、运行部分

D、表现部分

**正确答案：** ABD

# 132.以下哪些措施可以有效提高病毒防治能力（ ）

A、安装、升级杀毒软件

B、升级系统、打补丁

C、提高安全防范意识

D、不要轻易打开来历不明的邮件

**正确答案：** ABCD

# 133.计算机病毒的主要传播途径有（ ）

A、电子邮件

B、网络

C、存储介质

D、文件交换

**正确答案：** ABCD

# 134.以下哪些措施可以有效预防病毒、蠕虫和特洛伊木马的感染？（ ）

A、使用最新的防病毒软件

B、定期扫描系统

C、限制用户的权限

D、教育用户识别恶意软件

**正确答案：** ABCD

# 135.病毒、蠕虫和特洛伊木马的攻击方式有哪些不同？（ ）

A、病毒通常感染文件，蠕虫自我复制，特洛伊木马隐藏在合法软件中

B、病毒和蠕虫可以通过网络传播，而特洛伊木马通常需要用户执行

C、病毒和特洛伊木马可能会导致系统崩溃，而蠕虫主要消耗网络资源

D、所有上述描述都是正确的

**正确答案：** ABC

# 136.如何应对恶意软件的变异？（ ）

A、使用具有启发式检测的防病毒软件

B、定期更新病毒数据库

C、实施强制性的系统更新

D、使用沙箱技术进行测试

**正确答案：** ABCD

# 137.以下哪些行为可能会导致恶意软件的感染？（ ）

A、下载不明来源的软件

B、点击电子邮件中的不明链接

C、从不更新操作系统和软件

D、使用弱密码

**正确答案：** ABC

# 138.恶意软件防御策略应该包括哪些方面的内容？（ ）

A、预防措施

B、检测机制

C、响应计划

D、恢复流程

**正确答案：** ABCD

# 139.恶意软件的清除过程中，哪些步骤是关键的？（ ）

A、隔离受感染的系统

B、使用防病毒软件进行深度扫描

C、移除恶意软件文件

D、恢复受影响的系统文件

**正确答案：** ABCD

# 140.如何确保恶意软件防御策略的有效性？（ ）

A、定期测试防御措施

B、监控恶意软件的活动

C、更新防御策略以适应新威胁

D、培训用户识别和应对恶意软件

**正确答案：** ABCD

# 141.恶意软件攻击的哪些方面可以作为防御的切入点？（ ）

A、攻击者的入口点

B、恶意软件的传播机制

C、攻击者的心态

D、恶意软件的执行环境

**正确答案：** ABCD

# 142.在恶意软件防御中，如何平衡安全性和系统性能？（ ）

A、使用高效的防病毒引擎

B、优化扫描和处理时间

C、监控系统性能

D、根据系统的重要性调整安全策略

**正确答案：** ABCD

# 143.恶意软件防御中，如何利用蜜罐技术？（ ）

A、收集恶意软件样本

B、分析恶意软件行为

C、吸引攻击者远离关键资产

D、测试和验证防御措施

**正确答案：** ABCD

# 144.恶意软件防御中，如何降低零日攻击的风险？（ ）

A、定期更新软件和系统

B、使用未知威胁检测技术

C、限制系统的暴露面

D、全面禁止网络访问

**正确答案：** ABCD

# 145.恶意软件防御中，如何提高用户的警觉性？（ ）

A、定期发送安全警告

B、开展安全意识培训

C、设置明显的警告标志

D、禁止所有外部电子邮件

**正确答案：** ABCD

# 146.恶意软件防御中，如何利用大数据技术提高防御能力？（ ）

A、分析异常流量模式

B、识别潜在的恶意行为

C、实时监控和警报

D、预测未来的威胁

**正确答案：** ABCD

# 147.勒索软件的主要目的是什么？（ ）

A、窃取敏感信息

B、破坏系统功能

C、迫使受害者支付赎金

D、保护自己

**正确答案：** ABC

# 148.勒索软件通常通过哪些方式传播？（ ）

A、网络共享

B、电子邮件附件

C、恶意网站

D、USB驱动器

**正确答案：** ABCD

# 149.以下哪些是勒索软件的特点？（ ）

A、加密受害者数据

B、显示勒索信息

C、要求支付赎金

D、具有自我销毁功能

**正确答案：** ABC

# 150.勒索软件防御策略应该包括哪些方面？（ ）

A、备份重要数据

B、使用防病毒软件

C、定期更新软件和系统

D、教育用户识别恶意软件

**正确答案：** ABCD

# 151.如何防止勒索软件感染？（ ）

A、避免打开不明链接和附件

B、使用强大的密码

C、启用自动更新

D、定期扫描系统

**正确答案：** ABCD

# 152.勒索软件的清除步骤通常包括哪些？（ ）

A、隔离受感染系统

B、停止勒索软件运行

C、解密被加密的数据

D、修复系统漏洞

**正确答案：** ABCD

# 153.面对勒索软件攻击，受害者应该如何应对？（ ）

A、不要支付赎金

B、立即关闭网络连接

C、通知相关安全机构

D、寻求专业帮助

**正确答案：** ABCD

# 154.以下哪些措施可以减少勒索软件攻击的风险？（ ）

A、使用最新的操作系统和软件

B、定期备份重要数据

C、限制用户权限

D、开展安全意识培训

**正确答案：** ABCD

# 155.如何确保勒索软件防御策略的有效性？（ ）

A、定期测试防御措施

B、监控勒索软件的活动

C、更新防御策略以适应新威胁

D、培训用户识别和应对勒索软件

**正确答案：** ABCD

# 156.勒索软件的赎金通常要求以哪种形式支付？（ ）

A、比特币

B、电汇

C、礼品卡

D、所有上述形式

**正确答案：** ABC

# 157.勒索软件攻击前通常会进行哪些侦察活动？（ ）

A、网络扫描

B、社会工程学攻击

C、系统测试

D、数据泄露

**正确答案：** ABC

# 158.以下哪些措施可以帮助防止勒索软件的传播？（ ）

A、使用防火墙

B、更新操作系统和应用程序

C、关闭不必要的系统服务

D、限制对内部网络的访问

**正确答案：** ABCD

# 159.勒索软件防御中，哪些实践可以提高应急响应的效率？（ ）

A、建立快速的通信渠道

B、预先准备应急响应计划

C、进行定期的应急响应演练

D、指定专门的应急响应团队

**正确答案：** ABCD

# 160.勒索软件防御中，如何确保防御措施适应新的威胁环境？（ ）

A、持续学习和研究

B、与安全社区合作

C、定期更新防御策略

D、保持对最新安全技术的关注

**正确答案：** ABCD

# 161.数据安全能力成熟度模型的安全能力维度包括（ ）

A、组织建设

B、制度流程

C、技术工具

D、人员能力

**正确答案：** ABCD

# 162.数据权限申请、审批、使用、展示数据需（ ）原则

A、看看就行

B、敏感信息脱敏

C、随便发生

D、遵循最小化够用

**正确答案：** BD

# 163.数据安全中的数据指什么（ ）

A、数字

B、设计文档

C、客户信息

D、企业组织机构

**正确答案：** ABCD

# 164.GB/T31168《信息安全技术云计算服务安全能力要求》提出的安全要求是通常情况下云服务商应具备的基本安全能力。在具体的应用场景下，云服务商有可能需要对这些安全要求进行调整。调整的方式有（ ）。

A、删减

B、补充

C、忽视

D、替代

**正确答案：** ABD

# 165.GB/T31168《信息安全技术云计算服务安全能力要求》规定的安全计划所包含的内容包括但不限于（ ）。

A、云平台的基本描述

B、所采取的安全措施的具体情况

C、对云服务商新增的安全目标及对应的安全措施的说明

D、对客户安全责任的说明，以及对客户应实施的安全措施的建议

**正确答案：** ABCD

# 166.在不同情况下，实施云计算安全措施的主体可能包括（ ）。

A、云服务商

B、客户

C、云服务商和客户共同承担

D、其他组织承担

**正确答案：** ABCD

# 167.去标识化的目标包括：（ ）

A、删除所有标识符

B、数据重标识风险尽可能低

C、将数据尽可能泛化处理

D、数据尽可能有用

**正确答案：** BD

# 168.重标识的主要方法有：（ ）

A、分离

B、泛化

C、关联

D、推断

**正确答案：** ACD

# 169.数据时效性一般要求包括（ ）

A、制定数据存储时效性管理策略和规程

B、明确存储数据分享、禁止使用和数据清除有效期，具备数据存储时效性授权与控制能力

C、具备数据时效性自动检测能力

D、建立过期存储数据的安全保护机制

**正确答案：** ABD

# 170.在国际标准化组织（ISO）出版物类型中，技术规范（TS）指（1），公开可用规范（PAS）指（2），技术报告（TR）指（3）。（ ）

A、当所讨论的技术主题仍在开发中，或者由于任何其他原因，将来有可能但不是立即能达成可发布的国际标准时发布的出版物

B、技术委员会或分委员会收集的数据不同于能作为国际标准正式发布的数据时发布的出版物

C、制定完整的国际标准之前作为中间规范发布的出版物

D、技术委员会或分委员会下工作组层面提交的出版物

**正确答案：** ABC

# 171.SO/IECJTC1/SC27/WG4是安全服务与控制工作组，涵盖的主题域包括（ ）等。

A、供应链安全

B、鉴别机制

C、事件管理

D、应用安全

E、网络安全

**正确答案：** ACDE

# 172.信息安全治理过程包括（ ）。

A、评价

B、指导

C、监督

D、沟通

**正确答案：** ABCD

# 173.哪些是最终发布的国际标准出版物类型？（ ）

A、TR

B、FDIS

C、Amd

D、Cor

**正确答案：** ACD

# 174.信息安全管体系（ISMS）标准族包括（ ）。

A、术语标准

B、要求标准

C、指南标准

D、行业特定指南标准

E、特定控制指南标准

**正确答案：** ABCD

# 175.根据《网络安全法》，国务院标准化行政主管部门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（ ）。

A、国家标准

B、行业标准

C、团体标准

D、地方标准

**正确答案：** AB

# 176.根据《网络安全法》，国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建（ ）的网络空间，建立多边、民主、透明的网络治理体系。

A、和平

B、安全

C、开放

D、合作

**正确答案：** ABCD

# 177.《网络安全法》要求，网络产品、服务应当符合相关国家标准的强制性要求。在此基础上，法律提出了以下具体要求（ ）。

A、网络产品、服务的提供者不得设置恶意程序

B、网络产品、服务的提供者应当为其产品、服务持续提供安全维护

C、网络产品、服务的提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即向社会公布

D、网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意

**正确答案：** ABD

# 178.根据《网络安全法》，以下产品中，（ ）不必在安全认证或者检测合格后方可销售或者提供

A、通用网络设备

B、未有国家标准的强制性要求的产品

C、不在目录中的产品

D、网络安全专用产品

**正确答案：** ABC

# 179.《网络安全态势感知技术标准化白皮书（2020版）》的编制单位包括：（ ）

A、公安部第一研究所

B、公安部第三研究所

C、新华三技术有限公司

D、中国电子技术标准化研究

**正确答案：** BCD

# 180.防火墙主要用于实现以下哪些功能？（ ）

A、访问控制

B、网络地址转换

C、端口过滤

D、数据加密

**正确答案：** ABC

# 181.以下哪些是防火墙的常见类型？（ ）

A、包过滤防火墙

B、状态检测防火墙

C、应用级网关

D、虚拟私人网络（VPN）

**正确答案：** ABCD

# 182.入侵检测系统（IDS）的主要功能包括哪些？（ ）

A、检测和报告异常行为

B、分析网络流量

C、响应潜在的安全威胁

D、发起攻击

**正确答案：** ABC

# 183.入侵检测系统可以根据检测方法的不同分为哪些类型？（ ）

A、基于签名的IDS

B、基于行为的IDS

C、基于机器学习的IDS

D、基于日志的IDS

**正确答案：** ABD

# 184.以下哪些是防火墙的基本配置参数？（ ）

A、允许/拒绝列表

B、端口转发

C、安全策略

D、虚拟私人网络（VPN）设置

**正确答案：** ABCD

# 185.以下哪些是防火墙的基本原则？（ ）

A、最小权限

B、防御深度

C、透明性

D、单一安全解决方案

**正确答案：** ABCD

# 186.入侵检测系统可以部署在哪些位置？（ ）

A、网络边界

B、内部网络

C、关键资产附近

D、所有上述位置

**正确答案：** ABC

# 187.入侵检测系统面临的主要挑战包括哪些？（ ）

A、误报

B、漏报

C、性能影响

D、复杂性

**正确答案：** ABCD

# 188.以下哪些是防火墙的常见配置错误？（ ）

A、过于宽松的安全策略

B、错误的端口转发设置

C、未更新的病毒定义文件

D、使用弱密码

**正确答案：** ABC

# 189.入侵检测系统可以采用哪些方法来减少误报？（ ）

A、签名库更新

B、行为分析

C、机器学习算法

D、关闭所有安全功能

**正确答案：** ABC

# 190.防火墙的主要局限性包括哪些？（ ）

A、无法防止内部威胁

B、无法防止应用层攻击

C、依赖正确的配置

D、无法防止所有类型的攻击

**正确答案：** ABCD

# 191.入侵检测系统可以提供哪些类型的报告？（ ）

A、实时报告

B、事件记录

C、趋势分析报告

D、配置变更报告

**正确答案：** ABC

# 192.防火墙和入侵检测系统之间的关系是（ ）

A、防火墙提供初步的安全防护

B、入侵检测系统补充防火墙的不足

C、两者共同构成防御体系

D、入侵检测系统可以替代防火墙

**正确答案：** ABCD

# 193.以下哪些是入侵检测系统的典型应用场景？（ ）

A、保护关键基础设施

B、防御分布式拒绝服务（DDoS）攻击

C、监测内部网络活动

D、防止网络钓鱼攻击

**正确答案：** ABC

# 194.防火墙的配置和管理应该遵循哪些原则？（ ）

A、最小权限原则

B、防御深度原则

C、定期审计和更新

D、文档化和标准化

**正确答案：** ABCD

# 195.入侵检测系统可以基于哪些因素来识别异常行为？（ ）

A、用户行为

B、网络流量模式

C、系统日志

D、应用程序行为

**正确答案：** ABCD

# 196.防火墙的技术发展包括哪些？（ ）

A、硬件防火墙

B、软件防火墙

C、下一代防火墙（NGFW）

D、云防火墙

**正确答案：** ABCD

# 197.入侵检测系统在应对新兴威胁方面具有哪些优势？（ ）

A、实时监控

B、灵活性

C、能够检测未知威胁

D、自动响应

**正确答案：** ABC

# 198.网络地址转换（NAT）主要用于实现以下哪些功能？（ ）

A、内部网络地址与公网地址的映射

B、提高网络安全性

C、节约公网IP地址

D、数据加密

**正确答案：** ABC

# 199.NAT可以分为哪些类型？（ ）

A、静态NAT

B、动态NAT

C、端口转发

D、NAPT（网络地址端口转换）

**正确答案：** AB

# 200.端口转发主要用于实现哪些功能？（ ）

A、将内部网络的流量转发到公网

B、将公网的流量转发到内部网络

C、提高网络的可用性

D、数据加密

**正确答案：** ABC

# 201.NAT和端口转发在面对哪些威胁时具有一定的防御作用？（ ）

A、DDoS攻击

B、IP地址欺骗

C、端口扫描

D、恶意软件传播

**正确答案：** ABC

# 202.实施NAT和端口转发时，需要考虑哪些因素？（ ）

A、内部网络结构

B、公网IP地址资源

C、安全策略

D、性能影响

**正确答案：** ABCD

# 203.端口转发可以分为哪些类型？（ ）

A、显式端口转发

B、隐式端口转发

C、TCP端口转发

D、UDP端口转发

**正确答案：** AB

# 204.在使用NAT和端口转发时，可能遇到哪些问题？（ ）

A、内部网络设备无法访问公网

B、公网设备无法访问内部网络

C、端口冲突

D、性能下降

**正确答案：** ABC

# 205.如何解决NAT和端口转发可能带来的问题？（ ）

A、合理规划内部网络地址

B、确保公网IP地址充足

C、调整安全策略

D、使用高性能硬件

**正确答案：** ABC

# 206.NAT和端口转发在企业网络中的应用场景包括哪些？（ ）

A、远程访问

B、内部服务器提供公网服务

C、网络安全防护

D、无线网络连接

**正确答案：** ABC

# 207.实施NAT和端口转发时，哪些操作是安全的？（ ）

A、更新NAT规则

B、监控NAT日志

C、配置端口转发规则

D、关闭NAT功能

**正确答案：** ABC

# 208.在配置NAT和端口转发时，应该遵循哪些最佳实践？（ ）

A、最小权限原则

B、防御深度原则

C、透明性

D、单一安全解决方案

**正确答案：** ABC

# 209.NAT和端口转发技术的发展趋势包括哪些？（ ）

A、智能NAT

B、NAT64

C、端口转发加速

D、集成安全功能

**正确答案：** ABC

# 210.如何在NAT和端口转发中实现高性能？（ ）

A、使用高性能硬件

B、优化网络拓扑

C、并行处理

D、关闭不必要的服务

**正确答案：** ABC

# 211.在NAT和端口转发中，如何提高网络的安全性？（ ）

A、限制访问

B、使用防火墙

C、实施安全策略

D、使用加密技术

**正确答案：** ABC

# 212.NAT和端口转发在家庭网络中的应用场景包括哪些？（ ）

A、多台设备访问公网

B、家庭服务器提供公网服务

C、网络安全防护

D、无线网络连接

**正确答案：** ABC

# 213.在配置NAT和端口转发时，可能遇到哪些困难？（ ）

A、理解NAT和端口转发的原理

B、配置复杂的规则

C、处理异常情况

D、确保所有设备兼容

**正确答案：** ABC

# 214.如何测试NAT和端口转发的配置是否正确？（ ）

A、使用ping命令

B、使用traceroute命令

C、使用netstat命令

D、使用Wireshark进行抓包分析

**正确答案：** ABC

# 215.在NAT和端口转发中，如何优化网络性能？（ ）

A、合理规划IP地址

B、减少NAT转换

C、使用高性能设备

D、关闭不必要的服务

**正确答案：** ABC

# 216.在NAT和端口转发中，如何处理内部网络设备与公网设备之间的通信？（ ）

A、使用静态NAT

B、使用动态NAT

C、使用端口转发

D、关闭NAT功能

**正确答案：** ABC

# 217.数据包过滤可以基于哪些信息进行？（ ）

A、源IP地址

B、目的IP地址

C、源端口号

D、目的端口号

**正确答案：** ABCD

# 218.路由安全中，哪项措施可以防止路由欺骗？（ ）

A、使用路由器ID

B、实施路由过滤

C、使用加密路由协议

D、关闭路由器上的所有服务

**正确答案：** ABC

# 219.在实施数据包过滤时，应该如何处理SSH连接？（ ）

A、允许SSH连接

B、限制SSH连接的端口

C、记录SSH连接的日志

D、阻止所有SSH连接

**正确答案：** ABC

# 220.路由器的安全配置应该包括哪些方面？（ ）

A、启用防火墙

B、设置访问控制列表

C、更新路由器固件

D、更改默认的管理员密码

**正确答案：** ABCD

# 221.在数据包过滤和路由安全中，如何处理网络攻击？（ ）

A、检测并阻断恶意流量

B、及时更新安全策略

C、对受攻击设备进行隔离

D、分析攻击事件并报警

**正确答案：** ABCD

# 222.如何确保家庭网络中的数据包过滤和路由安全？（ ）

A、使用具有安全功能的路由器

B、定期更新路由器固件

C、设置家长控制功能

D、限制接入家庭网络的设备

**正确答案：** ABCD

# 223.以下哪些是数据包过滤的优点？（ ）

A、简单易用

B、可以防止未经授权的访问

C、有助于提升网络安全性

D、可能导致网络性能下降

**正确答案：** ABC

# 224.在配置数据包过滤规则时，应该注意哪些原则？（ ）

A、规则应该清晰明确

B、最小权限原则

C、规则应该易于管理

D、规则应该防止误报

**正确答案：** ABCD

# 225.如何在企业网络中实现有效的数据包过滤？（ ）

A、根据企业安全策略制定过滤规则

B、定期审查和更新过滤规则

C、使用高级 filtering 技术，如正则表达式

D、提供过滤规则的培训和指导

**正确答案：** ABCD

# 226.路由器的安全配置错误可能导致哪些风险？（ ）

A、未经授权的访问

B、网络拥塞

C、数据泄露

D、服务中断

**正确答案：** ABCD

# 227.如何确保数据包过滤和路由安全策略的执行？（ ）

A、使用强化的认证机制

B、实施严格的访问控制

C、监控和记录网络活动

D、定期进行安全评估

**正确答案：** ABCD

# 228.在处理数据包过滤和路由安全事件时，哪些步骤是标准的？（ ）

A、隔离受影响的系统

B、分析攻击模式

C、记录详细的日志信息

D、通知相关的利益相关者

**正确答案：** ABCD

# 229.恶意软件可以分为哪些类型？（ ）

A、病毒

B、蠕虫

C、木马

D、勒索软件

**正确答案：** ABCD

# 230.恶意软件的传播途径主要包括哪些？（ ）

A、网络共享

B、电子邮件

C、恶意网站

D、蓝牙

**正确答案：** ABC

# 231.恶意软件防御技术的发展趋势包括哪些？（ ）

A、更先进的检测算法

B、更快的响应时间

C、集成人工智能和机器学习

D、更广泛的使用云技术

**正确答案：** ABCD

# 232.在处理恶意软件事件时，哪些步骤是关键的？（ ）

A、立即隔离受感染系统

B、收集证据

C、清除恶意软件

D、防止未来的感染

**正确答案：** ABCD

# 233.恶意软件的哪些特征可以帮助安全专家进行识别？（ ）

A、异常的文件属性

B、加密或混淆的代码

C、恶意软件作者的签名

D、恶意软件的传播方式

**正确答案：** ABCD

# 234.特洛伊木马的典型特征有哪些？（ ）

A、隐藏在合法软件中

B、没有明显的界面

C、执行非预期功能

D、难以检测和清除

**正确答案：** ABCD

# 235.防止恶意软件感染的最佳实践包括哪些？（ ）

A、使用最新的操作系统和软件

B、定期备份重要数据

C、启用自动更新

D、保持对安全威胁的关注

**正确答案：** ABCD

# 236.恶意软件的检测和防御技术有哪些最新发展？（ ）

A、行为分析

B、机器学习

C、云安全服务

D、集成安全平台

**正确答案：** ABCD

# 237.面对勒索软件攻击，企业应该如何制定应对策略？（ ）

A、制定应急预案

B、确保数据备份

C、加强内部沟通

D、定期进行安全演练

**正确答案：** ABCD

# 238.勒索软件攻击的趋势有哪些？（ ）

A、攻击者使用更复杂的加密算法

B、攻击者倾向于针对企业而非个人

C、勒索金额不断增加

D、攻击者利用人工智能技术

**正确答案：** ABCD

# 239.以下哪些行为可能导致勒索软件的感染？（ ）

A、下载不明来源的软件

B、点击电子邮件中的不明链接

C、从不更新操作系统和软件

D、使用弱密码

**正确答案：** ABC