一、1 单项选择题（1-605）

1、 Chinese Wall 模型的设计宗旨是：（A）。

A、用户只能访问哪些与已经拥有的信息不冲突的信息　　B、用户可以访问所有信息

C、用户可以访问所有已经选择的信息　　D、用户不可以访问哪些没有选择的信息

2、 安全责任分配的基本原则是：（C）。

A、“三分靠技术，七分靠管理”　　B、“七分靠技术，三分靠管理”

C、“谁主管，谁负责”　　D、防火墙技术

3、 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（B）不属于信息运行安全技术的范畴。

A、风险分析　　B、审计跟踪技术　　C、应急技术　　D、防火墙技术

4、 从风险的观点来看，一个具有任务紧急性，核心功能性的计算机应用程序系统的开发和维护项目应该（A）。

A、内部实现　　B、外部采购实现　　C、合作实现　　D、多来源合作实现

5、 从风险分析的观点来看，计算机系统的最主要弱点是（B）。

A、内部计算机处理　　B、系统输入输出　　C、通讯和网络　　D、外部计算机处理

6、 从风险管理的角度，以下哪种方法不可取？（D）

A、接受风险　　B、分散风险　　C、转移风险　　D、拖延风险

7、 当今 IT 的发展与安全投入，安全意识和安全手段之间形成（B）。

A、安全风险屏障　　B、安全风险缺口　　C、管理方式的变革　　D、管理方式的缺口

8、 当为计算机资产定义保险覆盖率时，下列哪一项应该特别考虑？（D）。

A、已买的软件　　B、定做的软件　　C、硬件　　D、数据

9、 当一个应用系统被攻击并受到了破坏后，系统管理员从新安装和配置了此应用系统，在该系统重新上线前管理员不需查看：（C）

A、访问控制列表　　B、系统服务配置情况

C、审计记录　　D、用户账户和权限的设置

10、根据《计算机信息系统国际联网保密管理规定》，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行（B）。

A、 逻辑隔离　　B、物理隔离　　C、安装防火墙　　D、VLAN 划分

11、根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素

决定？（D）

A、威胁、脆弱性　　B、系统价值、风险

C、信息安全、系统服务安全　　D、受侵害的客体、对客体造成侵害的程度业务

12、公司应明确员工的雇佣条件和考察评价的方法与程序，减少因雇佣不当而产生的安全风险。人员考察的内容不包括（B）。

A、身份考验、来自组织和个人的品格鉴定　　B、家庭背景情况调查

C、学历和履历的真实性和完整性　　D、学术及专业资格

13、计算机信息的实体安全包括环境安全、设备安全、（B）三个方面。

A 运行安全　　B、媒体安全　　C、信息安全　　D、人事安全

14、目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（B）

A、公安部　　B、国家保密局

C、信息产业部　　D、国家密码管理委员会办公室

15、目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（B）

A、GB/T 18336-2001 信息技术安全性评估准则

B、GB 17859-1999 计算机信息系统安全保护等级划分准则

C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构

D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

16、确保信息没有非授权泄密，即确保信息不泄露给非授权的个人、实体或进程，不为其所用，是指（C）。

A、完整性　　B、可用性　　C、保密性　　D、抗抵赖性

17、如果对于程序变动的手工控制收效甚微，以下哪一种方法将是最有效的？（A）

A、自动软件管理　　B、书面化制度　　C、书面化方案　　D、书面化标准

18、如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？（A）

A、计算风险　　B、选择合适的安全措施

C、实现安全措施　　D、 接受残余风险

19、软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（A）

A、软件中止和黑客入侵　　B、远程监控和远程维护

C、软件中止和远程监控　　D、远程维护和黑客入侵

20、 管理审计指（C）

A、保证数据接收方收到的信息与发送方发送的信息完全一致

B、防止因数据被截获而造成的泄密

C、对用户和程序使用资源的情况进行记录和审查

D、保证信息使用者都可

21、为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（A）

A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B、进行离职谈话，禁止员工账号，更改密码

C、让员工签署跨边界协议

D、列出员工在解聘前需要注意的所有责任

22、为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（D）

A、人际关系技能　　B、项目管理技能　　C、技术技能　　D、沟通技能

23、我国的国家秘密分为几级？（A）

A、3　　B、4　　C、5　　D、6

24、系统管理员属于（C）。

A、决策层　　B、管理层

C、执行层　　D、既可以划为管理层，又可以划为执行层

25、下列哪一个说法是正确的？（C）

A、风险越大，越不需要保护　　B、风险越小，越需要保护

C、风险越大，越需要保护　　D、越是中等风险，越需要保护

26、下面哪类访问控制模型是基于安全标签实现的？（B）

A、自主访问控制　　B、强制访问控制

C、基于规则的访问控制　　D、基于身份的访问控制

27、下面哪项能够提供最佳安全认证功能？（B）

A、这个人拥有什么　　B、这个人是什么并且知道什么

C、这个人是什么　　D、这个人知道什么

28、下面哪一个是国家推荐性标准？（A）

A、GB/T 18020-1999　　应用级防火墙安全技术要求

B、SJ/T 30003-93　　电子计算机机房施工及验收规范

C、GA243-2000　　计算机病毒防治产品评级准则

D、ISO/IEC 15408-1999　信息技术安全性评估准则

29、下面哪一项关于对违反安全规定的员工进行惩戒的说法是错误的？（C）

A、对安全违规的发现和验证是进行惩戒的重要前提

B、惩戒措施的一个重要意义在于它的威慑性

C、处于公平，进行惩戒时不应考虑员工是否是初犯，是否接受过培训

D、尽管法律诉讼是一种严厉有效的惩戒手段，但使用它时一定要十分慎重

30、下面哪一项最好地描述了风险分析的目的？（C）

A、识别用于保护资产的责任义务和规章制度

B、识别资产以及保护资产所使用的技术控制措施

C、识别资产、脆落性并计算潜在的风险

D、识别同责任义务有直接关系的威胁

31、下面哪一项最好地描述了组织机构的安全策略？（A）

A、定义了访问控制需求的总体指导方针

B、建议了如何符合标准

C、表明管理意图的高层陈述

D、表明所使用的技术控制措施的高层陈述

32、下面哪一种风险对电子商务系统来说是特殊的？（D）

A、服务中断　　B、应用程序系统欺骗

C、未授权的信息泄露　　D、确认信息发送错误

33、下面有关我国标准化管理和组织机构的说法错误的是？（C）

A、国家标准化管理委员会是统一管理全国标准化工作的主管机构

B、国家标准化技术委员会承担国家标准的制定和修改工作

C、全国信息安全标准化技术委员负责信息安全技术标准的审查、批准、编号和发布

D、全国信息安全标准化技术委员负责统一协调信息安全国家标准年度技术项目

34、项目管理是信息安全工程师基本理论，以下哪项对项目管理的理解是正确的？（A）

A、项目管理的基本要素是质量，进度和成本

B、项目管理的基本要素是范围，人力和沟通

C、项目管理是从项目的执行开始到项目结束的全过程进行计划、组织

D、项目管理是项目的管理者，在有限的资源约束下，运用系统的观点，方法和理论，

对项目涉及的技术工作进行有效地管理

35、信息安全的金三角是（C）。

A、可靠性，保密性和完整性　　B、多样性，冗余性和模化性

C、保密性，完整性和可用性　　D、多样性，保密性和完整性

36、信息安全风险缺口是指（A）。

A、IT 的发展与安全投入，安全意识和安全手段的不平衡

B、信息化中，信息不足产生的漏洞

C、计算机网络运行，维护的漏洞

D、计算中心的火灾隐患

37、信息安全风险应该是以下哪些因素的函数？（A）

A、信息资产的价值、面临的威胁以及自身存在的脆弱性等

B、病毒、黑客、漏洞等

C、保密信息如国家密码、商业秘密等

D、网络、系统、应用的复杂的程度

38、信息安全工程师监理的职责包括？（A）

A、质量控制，进度控制，成本控制，合同管理，信息管理和协调

B、质量控制，进度控制，成本控制，合同管理和协调

C、确定安全要求，认可设计方案，监视安全态势，建立保障证据和协调

D、确定安全要求，认可设计方案，监视安全态势和协调

39、信息安全管理最关注的是？（C）

A、外部恶意攻击　　B、病毒对 PC 的影响

C、内部恶意攻击　　D、病毒对网络的影响

40、信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（C）

A、信息的价值　　B、信息的时效性

C、信息的存储方式　　D、法律法规的规定

41、信息网络安全的第三个时代是（A）

A、主机时代，专网时代，多网合一时代　　B、主机时代，PC 时代，网络时代

C、PC 时代，网络时代，信息时代　　D、2001 年，2002 年，2003 年

42、一个公司在制定信息安全体系框架时，下面哪一项是首要考虑和制定的？（A）

A、安全策略　　B、安全标准　　C、操作规程　　D、安全基线

43、以下哪个不属于信息安全的三要素之一？（C）

A、机密性　　B、完整性　　C、抗抵赖性　　D、可用性

44、以下哪一项安全目标在当前计算机系统安全建设中是最重要的？（C）

A、目标应该具体　　B、目标应该清晰

C、目标应该是可实现的　　D、目标应该进行良好的定义

45、以下哪一项计算机安全程序的组成部分是其它组成部分的基础？（A）

A、制度和措施　　B、漏洞分析

C、意外事故处理计划　　D、采购计划

46、以下哪一项是对信息系统经常不能满足用户需求的最好解释？（C）

A、没有适当的质量管理工具　　B、经常变化的用户需求

C、用户参与需求挖掘不够　　D、项目管理能力不强

47、以下哪一种人给公司带来了最大的安全风险？（D）

A、临时工　　B、咨询人员　　C、以前的员工　　D、当前的员工

48、以下哪种安全模型未使用针对主客体的访问控制机制？（C）

A、基于角色模型　　B、自主访问控制模型

C、信息流模型　　D、强制访问控制模型

49、以下哪种措施既可以起到保护的作用还能起到恢复的作用？（C）

A、对参观者进行登记　　B、备份

C、实施业务持续性计划　　D、口令

50、以下哪种风险被定义为合理的风险？（B）

A、最小的风险　　B、可接受风险

C、残余风险　　D、总风险

51、以下人员中，谁负有决定信息分类级别的责任？（B）

A、用户　　B、数据所有者　　C、审计员　　D、安全官

52、有三种基本的鉴别的方式：你知道什么，你有什么,以及（C）。

A、你需要什么　B、你看到什么　　C、你是什么　　D、你做什么

53、在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（B）

A、自下而上　　B、自上而下　　C、上下同时开展　　D、以上都不正确

54、在风险分析中，下列不属于软件资产的是（D）

A、计算机操作系统　　B、网络操作系统

C、应用软件源代码　　D、外来恶意代码

55、在国家标准中，属于强制性标准的是：（B）

A、GB/T　XXXX-X-200X　　B、GB XXXX-200X

C、DBXX/T　XXX-200X　　D、QXXX-XXX-200X

56、在任何情况下，一个组织应对公众和媒体公告其信息系统中发生的信息安全事件？（A）

A、当信息安全事件的负面影响扩展到本组织意外时

B、只要发生了安全事件就应当公告

C、只有公众的什么财产安全受到巨大危害时才公告

D、当信息安全事件平息之后

57、在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？（A）

A、标准（Standard）　　B、安全策略（Security policy）

C、方针（Guideline）　　D、流程(Proecdure)

58、在信息安全管理工作中“符合性”的含义不包括哪一项？（C）

A、对法律法规的符合　　B、对安全策略和标准的符合

C、对用户预期服务效果的符合　　D、通过审计措施来验证符合情况

59、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

60、职责分离是信息安全管理的一个基本概念。其关键是权利不能过分集中在某一个人手中。职责分离的目的是确保没有单独的人员（单独进行操作）可以对应用程序系统特征或控制功能进行破坏。当以下哪一类人员访问安全系统软件的时候，会造成对“职责分离”原则的违背？（D）

A、数据安全管理员　　B、数据安全分析员

C、系统审核员　　D、系统程序员

61、中国电信的岗位描述中都应明确包含安全职责，并形成正式文件记录在案，对于安全职责的描述应包括（D）。

A、落实安全政策的常规职责　　B、执行具体安全程序或活动的特定职责

C、保护具体资产的特定职责　　D、以上都对

62、终端安全管理目标：规范支撑系统中终端用户的行为，降低来自支撑系统终端的安全威

胁，重点解决以下哪些问题？（A）。

A、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

B、终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理；终端防病毒管理

C、终端接入和配置管理；桌面及主机设置管理；终端防病毒管理

D、终端接入和配置管理；终端账号、秘密、漏洞补丁等系统安全管理；桌面及主机设置管理

63、著名的橘皮书指的是（A）。

A、可信计算机系统评估标准(TCSEC)　　B、信息安全技术评估标准（ITSEC）

C、美国联邦标准（FC）　　D、通用准则（CC）

64、资产的敏感性通常怎样进行划分？（C）

A、绝密、机密、敏感　　B、机密、秘密、敏感和公开

C、绝密、机密、秘密、敏感和公开等五类

D、绝密、高度机密、秘密、敏感和公开等五类

65、重要系统关键操作操作日志保存时间至少保存（C）个月。

A、1　　B、2　　C、3　　D、4

66、安全基线达标管理办法规定：BSS 系统口令设置应遵循的内控要求是（C）

A、数字+字母　　B、数字+字母+符号

C、数字+字母+字母大小写　　D、数字+符号

67、不属于安全策略所涉及的方面是（D）。

A、物理安全策略　　B、访问控制策略

C、信息加密策略　　D、防火墙策略

68、“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（C）。

A、“普密”、“商密”两个级别　　B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别

D、“一密”、“二密”，“三密”、“四密”四个级别

69、对 MBOSS 系统所有资产每年至少进行（A）次安全漏洞自评估。

A、1　　B、2　　C、3　　D、4

70、下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（A）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

71、中国电信各省级公司争取在 1-3 年内实现 CTG-MBOSS 系统安全基线“达标”（C）级以上。

A、A 级　　B、B 级　　C、C 级　　D、D 级

72、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（C）

A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定

B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级

C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案

D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

73、获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息（B）组以上的可以被《中华人民共和国刑法》认为是非法获取计算机信息系统系统认定的“情节严重”。

A、5　　B、10　　C、-15　　D、20

74、基准达标项满（B）分作为安全基线达标合格的必要条件。

A、50　　B、60　　C、70　　D、80

75、《国家保密法》对违法人员的量刑标准是（A）。

A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑

B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑

C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑

D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

76、$HOME/.netrc 文件包含下列哪种命令的自动登录信息？（C）

A、rsh　　B、ssh　　C、ftp　　D、rlogin

77、/etc/ftpuser 文件中出现的账户的意义表示（A）。

A、该账户不可登录 ftp　　B、该账户可以登录 ftp　　C、没有关系　　D、缺少

78、按 TCSEC 标准，WinNT 的安全级别是（A）。

A、C2　　B、B2　　C、C3　　D、B1

79、Linux 系统/etc 目录从功能上看相当于 Windows 的哪个目录？（B）

A、program files　B、Windows　　C、system volume information　　D、TEMP

80、Linux 系统格式化分区用哪个命令？（A）

A、fdisk　　B、mv　　C、mount　　D、df

81、在 Unix 系统中，当用 ls 命令列出文件属性时，如果显示-rwxrwxrwx,意思是（A）。

A、前三位 rwx 表示文件属主的访问权限；中间三位 rwx 表示文件同组用户的访问权限；后三位 rwx 表示其他用户的访问权限

B、前三位 rwx 表示文件同组用户的访问权限；中间三位 rwx 表示文件属主的访问权限；后三位 rwx 表示其他用户的访问权限

C、前三位 rwx 表示文件同域用户的访问权限；中间三位 rwx 表示文件属主的访问权限；后三位 rwx 表示其他用户的访问权限

D、前三位 rwx 表示文件属主的访问权限；中间三位 rwx 表示文件同组用户的访问权限；后三位 rwx 表示同域用户的访问权限

82、Linux 系统通过（C）命令给其他用户发消息。

A、less　　B、mesg　　C、write　　D、echo to

83、Linux 中，向系统中某个特定用户发送信息，用什么命令？（B）

A、wall　　B、write　　C、mesg　　D、net send

84、防止系统对 ping 请求做出回应，正确的命令是：（C）。

A、echo 0>/proc/sys/net/ipv4/icmp_ehco_ignore_all

B、echo 0>/proc/sys/net/ipv4/tcp_syncookies

C、echo 1>/proc/sys/net/ipv4/icmp_echo_ignore_all

D、echo 1>/proc/sys/net/ipv4/tcp_syncookies

85、NT/2K 模型符合哪个安全级别？（B）

A、B2　　B、C2　　C、B1　　D、C1

86、Red Flag Linux 指定域名服务器位置的文件是（C）。

A、etc/hosts　　B、etc/networks　　C、etc/rosolv.conf　　D、/.profile

87、Solaris 操作系统下，下面哪个命令可以修改/n2kuser/.profile 文件的属性为所有用户可读、科协、可执行？（D）

A、chmod 744 /n2kuser/.profile　　B、 chmod 755 /n2kuser/.profile

C、 chmod 766 /n2kuser/.profile　　D、 chmod 777 /n2kuser/.profile

88、如何配置，使得用户从服务器 A 访问服务器 B 而无需输入密码？（D）

A、利用 NIS 同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhost 文件

C、在两台服务器上创建并配置$HOME/.netrc 文件

D、在两台服务器上创建并配置/etc/hosts.equiv 文件

89、Solaris 系统使用什么命令查看已有补丁列表？（C）

A、uname –an　　B、showrev　　C、oslevel –r　　D、swlist –l product ‘PH??’

90、Unix 系统中存放每个用户信息的文件是（D）。

A、/sys/passwd　　B、/sys/password　　C、/etc/password　　D、/etc/passwd

91、Unix 系统中的账号文件是（A）。

A、/etc/passwd　　B、/etc/shadow　　C、/etc/group　　D、/etc/gshadow

92、Unix 系统中如何禁止按 Control-Alt-Delete 关闭计算机？（B）

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

93、Unix 中。可以使用下面哪一个代替 Telnet，因为它能完成同样的事情并且更安全？（）

A、S-TELNET　　B、SSH　　C、FTP　　D、RLGON

94、Unix 中，默认的共享文件系统在哪个位置？（C）

A、/sbin/　　B、/usr/local/　　C、/export/　　D、/usr/

95、Unix 中，哪个目录下运行系统工具，例如 sh,cp 等？（A）

A、/bin/　　B、/lib/　　C、/etc/　　D、/

96、U 盘病毒依赖于哪个文件打到自我运行的目的？（A）

A、autoron.inf　　B、autoexec.bat　　C、config.sys　　D、system.ini

97、Windows 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

98、Windows 2000 目录服务的基本管理单位是（D）。

A、用户　　B、计算机　　C、用户组　　D、域

99、Windows 2000 系统中哪个文件可以查看端口与服务的对应？（D）

A、c:\winnt\system\drivers\etc\services　　B、c:\winnt\system32\services

C、c:\winnt\system32\config\services　　D、c:\winnt\system32\drivers\etc\services

100、Windows NT/2000 SAM 存放在（D）。

A、WINNT　　B、WINNT/SYSTEM32

C、WINNT/SYSTEM　　D、WINNT/SYSTEM32/config

101、 Windows NT/2000 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

102、Windows NT 的安全标识（SID）串是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是什么？（C）

A、击键速度　　B、用户网络地址

C、处理当前用户模式线程所花费 CPU 的时间　　D、PING 的响应时间

103、Windows NT 和 Windows 2000 系统能设置为在几次无效登录后锁定账号，可以防止：（B）。

A、木马　　B、暴力破解　　C、IP 欺骗　　D、缓冲区溢出攻击

104、Windows 主机推荐使用（A）格式。

A、NTFS　　B、FAT32　　C、FAT　　D、Linux

105、XP 当前的最新补丁是（C）。

A、SP1　　B、SP2　　C、SP3　　D、SP4

106、按 TCSEC 标准，WinNT 的安全级别是（A）。

A、C2　　B、B2　　C、C3　　D、B1

107、当你感觉到你的 Win2003 运行速度明显减慢，当打开任务管理器后发现 CPU 使用率达到了 100%，你认为你最有可能受到了（D）攻击。

A、缓冲区溢出攻击　　B、木马攻击　　C、暗门攻击　　D、DOS 攻击

108、档案权限 755，对档案拥有者而言，是什么含义？（A）

A、可读，可执行，可写入　　B、可读

C、可读，可执行　　D、可写入

109、如何配置，使得用户从服务器 A 访问服务器 B 而无需输入密码（D）。

A、利用 NIS 同步用户的用户名和密码

B、在两台服务器上创建并配置/.rhosts 文件

C、在两台服务器上创建并配置$HOME/.netrc 文件

D、在两台服务器上创建并配置/et/hosts.equiv 文件

110、要求关机后不重新启动，shutdown 后面参数应该跟（C）。

A、–k　　B、–r　　C、-h　　D、 –c

111、一般来说，通过 web 运行 http 服务的子进程时，我们会选择（D）的用户用户权限方式，这样可以保证系统的安全。

A、root　　B、httpd　　C、guest　　D、nobody

112、以下哪项技术不属于预防病毒技术的范畴？（A）

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

113、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？（B）

A、缓冲区溢出攻击　　B、钓鱼攻击　　C、暗门攻击　　D、DDos 攻击

114、与另一台机器建立 IPC$会话连接的命令是（D）。

A、net user \\192.168.0.1\IPC$

B、net use \\192.168.0.1\IPC$ user:Administrator / passwd:aaa

C、net user \192.168.0.1IPC$　　D、net use \\192.168.0.1\IPC$

115、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

116、在 NT 中，怎样使用注册表编辑器来严格限制对注册表的访问？（C）

A、HKEY_CURRENT_CONFIG,连接网络注册、登录密码、插入用户 ID

B、HKEY_CURRENT_MACHINE,浏览用户的轮廓目录，选择 NTUser.dat

C、HKEY_USERS,浏览用户的轮廓目录，选择 NTUser.dat

D、HKEY_USERS,连接网络注册，登录密码，插入用户 ID

117、在 Solaris 8 下，对于/etc/shadow 文件中的一行内容如下“root:3vd4NTwk5UnLC:9038::::::”，以下说法正确的是：（E）。

A、这里的 3vd4NTwk5UnLC 是可逆的加密后的密码

B、这里的 9038 是指从 1970 年 1 月 1 日到现在的天数

C、这里的 9038 是指从 1980 年 1 月 1 日到现在的天数

D、这里的 9038 是指从 1980 年 1 月 1 日到最后一次修改密码的天数

E-以上都不正确

118、在 Solaris 8 下，对于/etc/shadow 文件中的一行内容如下：root:3vd4NTwk5UnLC:0:1:Super-User:/:”，以下说法正确的是：（A）。

A、是/etc/passwd 文件格式　　B、是/etc/shadow 文件格式

C、既不是/etc/passwd 也不是/etc/shadow 文件格式

D、这个 root 用户没有 SHELL，不可登录

E、这个用户不可登录，并不是因为没有 SHELL

119、在 Solaris 系统中，终端会话的失败登录尝试记录在下列哪个文件里面?(D)

A、-/etc/default/login　　B、/etc/nologin

C、/etc/shadow　　D、var/adm/loginlog

120、在 Windows 2000 中，以下哪个进程不是基本的系统进程:(D)

A、smss. exe　　B、csrss. Exe　　C、winlogon. exe　　D、-conime.exe

121、在 Windows 2000 中可以察看开放端口情况的是:(D)。

A、nbtstat　　B、net　　C、net show　　D、netstat

122.、在 Windows 2003 下 netstat 的哪个参数可以看到打开该端口的 PID?(C)（格式到此）

A、a　　B、n　　C、o　　D 、p

123.、在使用影子口令文件(shadowedpasswords)的 Linux 系统中，/etc/passwd 文件和/etc/shadow 文件的正确权限分别是(C)。

A、rw-r-----,-r--------　　B、rw-r--r--,-r--r--r—

C、rw-r--r--,-r--------　　Drw-r--rw-,-r-----r--

124.、制定数据备份方案时，需要重要考虑的两个因素为适合的备份时间和(B)。

A、备份介质　　B、备份的存储位置

C、备份数据量　　D、恢复备份的最大允许时间

125.、周期性行为，如扫描，会产生哪种处理器负荷?(A)

A、Idle Ioad　　B、Usage Ioad　　C、Traffic load　　D、以上都不对

126、主要由于(D)原因，使 Unix 易于移植

A、Unix 是由机器指令书写的　　B、Unix 大部分由汇编少部分用 C 语言编写

C、Unix 是用汇编语言编写的　　D、Unix 小部分由汇编大部分用 C 语言编写

127.、HP-UX 系统中，使用(A)命令查看系统版本、硬件配置等信息。

A、uname -a　　B、ifconfig　　C、netstat　　D、ps -ef

128.、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

129、在云计算虚拟化应用中，VXLAN 技术处于 OS 工网络模型中 2-3 层间，它综合了 2 层交换的简单性与 3 层路由的跨域连接性。它是通过在 UDP/IP 上封装 Mac 地址而实现这一点的。在简单应用场合，vxLAN 可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?(C)

A、惠普　　B、Juniper　　C、Cisco 与 Vmware　　D、博科 Brocade

130.、Linux 中，什么命令可以控制口令的存活时间了(A)。

A、chage　　B、passwd　　C、chmod　　D、umask

131.、Qfabric 技术是使用市场上现成的计算和存储网元并利用行业标准的网络接口将它们连接后组建大规模的数据中心，以满足未来云计算的要求。该技术概念是哪个厂家主推的概念?(B)

A、惠普　　B、uniper　　C、Cisco 与 Vmware　　D、博科 Brocade

132、为了检测 Windows 系统是否有木马入侵，可以先通过()命令来查看当前的活动连接端口。

A、ipconfig　　B、netstat -rn　　C、tracert –d　　D、netstat -an

133、网络营业厅提供相关服务的可用性应不低于（A）。

A、99.99%　　B、99.9%　　C、99%　　D、98.9%

134.、IRF(Intelligent Resilient Framework)是在该厂家所有数据中心交换机中实现的私有技术，是应用在网络设备控制平面的多虚拟技术。该技术属于哪个厂家?(A)

A、惠普　　B、Juniper　　C、Cisco 与 Vmware　　D、博科 Brocade

135.、Windows NT 的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:(D)。

A、击键速度　　B、当前用户名

C、用户网络地址　　D、处理当前用户模式线程所花费 CPU 的时间

136、脆弱性扫描，可由系统管理员自行进行检查，原则上应不少于(B)。

A、每周一次　　B、每月一次　　C、每季度一次　　D、每半年一次

137、下面哪一个情景属于身份验证(Authentication)过程?(A)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

138、下面哪一个情景属于授权(Authorization)过程?(B)

A、用户依照系统提示输入用户名和口令

B、用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改

C、用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

139、下列哪一条与操作系统安全配置的原则不符合?(D)

A、关闭没必要的服务　　B、不安装多余的组件

C、安装最新的补丁程序　　D、开放更多的服务

140、关于 DDoS 技术，下列哪一项描述是错误的(D)。

A、一些 DDoS 攻击是利用系统的漏洞进行攻击的

B、黑客攻击前对目标网络进行扫描是发功 DDoS 攻击的一项主要攻击信息来源

C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的 DDoS 攻击入侵

D、DDoS 攻击不对系统或网络造成任何影响

141、关于 PPP 协议下列说法正确的是:(C)。

A、PPP 协议是物理层协议

B、PPP 协议是在 HDLC 协议的基础上发展起来的

C、PPP 协议支持的物理层可以是同步电路或异步电路

D、PPP 主要由两类协议组成:链路控制协议族 CLCP)和网络安全方面的验证协议族(PAP 和 CHAP)

142、接口被绑定在 2 层的 zone，这个接口的接口模式是（C）。

A、NAT mode　　B、Route mode

C、-Transparent mode　　D、NAT 或 Route mode

143、接入控制方面，路由器对于接口的要求包括：（D）。

A、串口接入　　B、局域网方式接入　　C、Internet 方式接入　　D、VPN 接入

144、局域网络标准对应 OSI 模型的哪几层？（C）。

A、上三层　　B、只对应网络层　　C、下三层　　D、只对应物理层

145、拒绝服务不包括以下哪一项？（D）。

A、DDoS　　B、畸形报文攻击　　C、Land 攻击　　D、ARP 攻击

146、抗 DDoS 防护设备提供的基本安全防护功能不包括（A）。

A、对主机系统漏洞的补丁升级　　B、检测 DDoS 攻击

C、DDoS 攻击警告　　D、DDoS 攻击防护

147、路由器产品提供完备的安全架构以及相应的安全模块，在软、硬件层面设置重重过滤，保护路由器业务安全。其中不对的说法是：（C）。--》缺少 D 选项

A、路由器产品支持 URPF，可以过滤大多数虚假 IP 泛洪攻击

B、路由器产品支持 CAR 功能，可以有效限制泛洪攻击

C、路由器产品不支持 ACL 配置功能，不能定制过滤规则

D、

148、路由器对于接入权限控制，包括：（D）。

A、根据用户账号划分使用权限　　B、根据用户接口划分使用权限

C、禁止使用匿名账号　　D、以上都是

149、路由器启动时默认开启了一些服务，有些服务在当前局点里并没有作用，对于这些服务：（C）。缺少 D 选项

A、就让他开着，也耗费不了多少资源　　B、就让他开着，不会有业务去访问

C、必须关闭，防止可能的安全隐患　　D、

150、设置 Cisco 设备的管理员账号时，应（C）。

A、多人共用一个账号　　B、多人共用多个账号

C、一人对应单独账号　　D、一人对应多个账号

151、什么命令关闭路由器的 finger 服务？（C）

A、disable finger　　B、no finger　　C、no finger service　　D、no service finger

152、什么是 IDS？（A）

A、入侵检测系统　　B、入侵防御系统　　C、网络审计系统　　D、主机扫描系统

153、实现资源内的细粒度授权，边界权限定义为：（B）。

A、账户　　B、角色　　C、权限　　D、操作

154、使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（A）

A、拒绝服务　　B、文件共享　　C、BIND 漏洞　　D、远程过程调用

155、使用 TCP 79 端口的服务是：（D）。

A、telnet　　B、SSH　　C、Web　　D、Finger

156、使用一对一或者多对多方式的 NAT 转换，当所有外部 IP 地址均被使用后，后续的内网用户如需上网，NAT 转换设备会执行什么样的动作？（C）

A、挤掉前一个用户，强制进行 NAT 转换　　B、直接进行路由转发

C、不做 NAT 转换　　D、将报文转移到其他 NAT 转换设备进行地址转换

157、私网地址用于配置本地网络、下列地址中属于私网地址的是？（C）

A、100.0.0.0　　B、172.15.0.0　　C、192.168.0.0　　D、244.0.0.0

158、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、日志分析工作

C、攻击检测和报警　　D、对访问行为实施静态、固定的控制

159、随着安全要求的提高、技术的演进，（D）应逐步实现物理隔离，或者通过采用相当于物理隔离的技术（如 MPLSVPN）实现隔离。

A、局域网　　B、广域网及局域网　　C、终端　　D、广域网

160、通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，请问这种攻击属于何种攻击？（D）

A、拒绝服务（DoS）攻击　　B、扫描窥探攻击

C、系统漏洞攻击　　D、畸形报文攻击

161、通信领域一般要求 3 面隔离，即转发面、控制面、用户面实现物理隔离，或者是逻辑隔离，主要目的是在某一面受到攻击的时候，不能影响其他面。路由器的安全架构在实现上就支持：（D）

A、转发面和控制面物理隔离　　B、控制面和用户面逻辑隔离

C、转发面和用户面逻辑隔离　　D、以上都支持

162、网管人员常用的各种网络工具包括 telnet、ftp、ssh 等，分别使用的 TCP 端口号是（B）。

A、21、22、23　　B、23、21、22　　C、23、22、21　　D、21、23、22

163、网络安全工作的目标包括：（D）。

A、信息机密性　　B、信息完整性　　C、服务可用性　　D、以上都是

164、网络安全在多网合一时代的脆弱性体现在（C）。

A、网络的脆弱性　　B、软件的脆弱性　　C、管理的脆弱性　　D、应用的脆弱性

165、应限制 Juniper 路由器的 SSH（A），以防护通过 SSH 端口的 DoS 攻击。

A、并发连接数和 1 分钟内的尝试连接数　　B、并发连接数

C、1 分钟内的尝试连接数　　D、并发连接数和 3 分钟内的尝试连接数

166、应用网关防火墙的逻辑位置处在 OSI 中的哪一层？（C）

A、传输层　　B、链路层　　C、应用层　　D、物理层

167、应用网关防火墙在物理形式上表现为？（B）

A、网关　　B、堡垒主机　　C、路由　　D、交换机

168、用来追踪 DDoS 流量的命令式：（C）

A、ip source-route　　B、ip cef　　C、ip source-track　　D、ip finger

169、用于保护整个网络 IPS 系统通常不会部署在什么位置？（D）

A、网络边界　　B、网络核心　　C、边界防火墙内　　D、业务终端上

170、用于实现交换机端口镜像的交换机功能是：（D）

A、PERMIT LIST　　B、PVLAN　　C、VTP　　D、SPAN

171、有关 L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（D）。

A、L2TP 是由 PPTV 协议和 Cisco 公司的 L2F 组合而成

B、L2TP 可用于基于 Internet 的远程拨号访问

C、为 PPP 协议的客户建立拨号连接的 VPN 连接

D、L2TP 只能通过 TCP/IP 连接

172、有关 PPTP（Point-to-Point Tunnel Protocol）说法正确的是（C）。

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

173、有一些应用，如微软 Out look 或 MSN。它们的外观会在转化为基于 Web 界面的过程中丢失，此时要用到以下哪项技术：（B）

A、Web 代理　　B、端口转发　　C、文件共享　　D、网络扩展

174、预防信息篡改的主要方法不包括以下哪一项？（A）

A、使用 VPN 技术　　B、明文加密　　C、数据摘要　　D、数字签名

175、域名服务系统（DNS）的功能是（A）。

A、完成域名和 IP 地址之间的转换　　B、完成域名和网卡地址之间的转换

C、完成主机名和 IP 地址之间的转换　　D、完成域名和电子邮件地址之间的转换

176、源 IP 为 100.1.1.1，目的 IP 为 100.1.1.255，这个报文属于什么攻击？（B）（假设该网段掩码为 255.255.255.0）

A、LAND 攻击　　B、SMURF 攻击　　C、FRAGGLE 攻击　　D、WINNUKE 攻击

177、在 AH 安全协议隧道模式中，新 IP 头内哪个字段无需进行数据完整性校验？（A）

A、TTL　　B、源 IP 地址　　C、目的 IP 地址　　D、源 IP 地址+目的 IP 地址

178、在 C/S 环境中，以下哪个是建立一个完整 TCP 连接的正确顺序？（D）

A、SYN，SYN/ACK，ACK　　B、Passive Open,Active Open,ACK,ACK

C、SYN,ACK/SYN,ACK　　D、Active Open/Passive Open,ACK,ACK

179、在 L2TP 应用场景中，用户的私有地址分配是由以下哪个组建完成？（B）

A、LAC　　B、LNS　　C、VPN Client　　D、用户自行配置

180、在 OSI 模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（A）

A、应用层　　B、物理层　　C、会话层　　D、网络层

181、在 OSI 参考模型中有 7 个层次，提供了相应的安全服务来加强信息系统的安全性。以下哪一层提供了抗抵赖性？（B）

A、表示层　　B、应用层　　C、传输层　　D、数据链路层

182、在安全策略的重要组成部分中，与 IDS 相比，IPS 的主要优势在哪里？（B）

A、产生日志的数量　　B、攻击减少的速度

C、较低的价格　　D、假阳性的减少量

183、在安全审计的风险评估阶段，通常是按什么顺序来进行的？（A）

A、侦查阶段、渗透阶段、控制阶段　　B、渗透阶段、侦查阶段、控制阶段

C、控制阶段、侦查阶段、渗透阶段　　D、侦查阶段、控制阶段、渗透阶段

184、在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（D）

A、IETF 因特网工程工作小组　　B、ISO 国际标准组织

C、IANA 因特网地址指派机构　　D、OSI 开放系统互联

185、在传输模式 IPSec 应用情况中，以下哪个区域数据报文可受到加密安全保护？（D）

A、整个数据报文　　B、原 IP 头　　C、新 IP 头　　D、传输层及上层数据报文

186、在点到点链路中，OSPF 的 Hello 包发往以下哪个地址？（B）

A、127.0.0.1　　B、224.0.0.5　　C、233.0.0.1　　D、255.255.255.255

187、在建立堡垒主机时，（A）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

188、在进行 Sniffer 监听时，系统将本地网络接口卡设置成何种侦听模式？（D）

A、unicast 单播模式　　B、Broadcast 广播模式

C、Multicast 组播模式　　D、Promiscuous 混杂模式

189、在零传输（Zone transfers）中 DNS 服务使用哪个端口？（A）

A、TCP 53　　B、UDP 53　　C、UDP 23　　D、TCP23

190、在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（C）

A、入网访问控制　　B、权限控制　　C、网络检测控制　　D、防火墙控制

191、在思科设备上，若要查看所有访问表的内容，可以使用的命令式（B）

A、show all access-lists　　B、show access-lists

C、show ip interface　　D、show interface

192、在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的这是对（A）。

A、可用性的攻击　　B、保密性的攻击　　C、完整性的攻击　　D、真实性的攻击

193、在一个局域网环境中，其内在的安全威胁包括主动威胁和被动威胁。以下哪一项属于被动威胁？（C）

A、报文服务拒绝　　B、假冒　　C、数据流分析　　D、报文服务更改

194、在以下 OSI 七层模型中，synflooding 攻击发生在哪层？（C）

A、数据链路层　　B、网络层　　C、传输层　　D、应用层

195、在以下哪类场景中，移动用户不需要安装额外功能（L2TP）的 VPDN 软件？（B）

A、基于用户发起的 L2TP VPN　　B、基于 NAS 发起的 L2TP VPN

C、基于 LNS 发起的 L2TP VPN　　D、以上都是

196、账户口令管理中 4A 的认证管理的英文单词为：（B）

A、Account　　B、Authentication　　C、Authorization　　D、Audit

197、只具有（A）和 FIN 标志集的数据包是公认的恶意行为迹象。

A、SYN　　B、date　　C、head　　D、标志位

198、主从账户在 4A 系统的对应关系包含：（D）

A、1 -N　　B、1 -1　　C、N -1　　D、以上全是

199、主动方式 FTP 服务器要使用的端口包括（A）。

A、TCP 21 TCP 20　　B、TCP21 TCP 大于 1024 的端口

C、TCP 20、TCP 大于 1024 端口　　D、都不对

200、下列（D）因素不是影响 IP 电话语音质量的技术因素。

A、时延　　B、抖动　　C、回波　　D、GK 性能

201、下列安全协议中使用包括过滤技术，适合用于可信的 LAN 到 LAN 之间的 VPN（内部 VPN）的是（D）。

A、PPTP　　B、L2TP　　C、SOCKS v5　　D、IPSec

202、下列不是抵御 DDoS 攻击的方法有（D）。

A、加强骨干网设备监控　　B、关闭不必要的服务

C、限制同时打开的 Syn 半连接数目　　D、延长 Syn 半连接的 time out 时间

203、下列措施不能增强 DNS 安全的是（C）。

A、使用最新的 BIND 工具　　B、双反向查找

C、更改 DNS 的端口号　　D、不要让 HINFO 记录被外界看到

204、下列各种安全协议中使用包过滤技术，适合用于可信的 LAN 到 LAN 之间的 VPN，即内部网 VPN 的是（）。

A、PPTP　　B、L2TP　　C、SOCKS v5　　D、IPSec

205、下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适？（D）

A、回应的比例　　B、被动的防御　　C、主动的防御　　D、都不对

206、下列哪项是私有 IP 地址？（A）

A、10.5.42.5　　B、172.76.42.5　　C、172.90.42.5　　D、241.16.42.5

207、下列哪一项能够提高网络的可用性？（B）

A、数据冗余　　B、链路冗余　　C、软件冗余　　D、电源冗余

208、下列哪一种攻击方式不属于拒绝服务攻击：（A）。

A、LOphtCrack　　B、Synflood　　C、Smurf　　D、Ping of Death

209、下列哪一项是 arp 协议的基本功能？（A）

A、通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的进行

B、对局域网内的其他机器广播路由地址

C、过滤信息，将信息传递个数据链路层　　D、将信息传递给网络层

210、最早的计算机网络与传统的通信网络最大的区别是什么？（A）

A、计算机网络采用了分组交换技术　　B、计算机网络采用了电路交换技术

C、计算机网络的可靠性大大提高　　D、计算机网络带宽和速度大大提高

211、以下哪个属于 IPS 的功能？（A）

A、检测网络攻击　　B、网络流量检测　　C、实时异常告警　　D、以上都是

212、以下说法错误的是（C）。

A、安全是一个可用性与安全性之间的平衡过程　　B、安全的三要素中包含完整性

C、可以做到绝对的安全　　D、网络安全是信息安全的子集

213、以下属于 4A 策略管理模块可以管理的为（C）。

A、访问控制策略　　B、信息加密策略　　C、密码策略　　D、防火墙策略

214、最早研究计算机网络的目的是什么？（B）

A、共享硬盘空间、打印机等设备　　B、共享计算资源

C、直接的个人通信　　D、大量的数据交换

215、防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为（C）。

A、内容过滤　　B、地址转换　　C、透明代理　　D、内容中转

216、可以通过哪种安全产品划分网络结构，管理和控制内部和外部通讯（A）。

A、防火墙　　B、CA 中心　　C、加密机　　D、防病毒产品

217、网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（D）。

A、多重安全网关　　B、防火墙　　C、Vlan 隔离　　D、物理隔离

218、下列哪项不是 Tacacs+协议的特性。（A）

A、扩展记账　　B、加密整个数据包　　C、使用 TCP　　D、支持多协议

219、一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（A）

A、最小特权　　B、阻塞点　　C、失效保护状态　　D、防御多样化

220、包过滤防火墙工作的好坏关键在于？（C）

A、防火墙的质量　　B、防火墙的功能　　C、防火墙的过滤规则设计　　D、防火墙的日志

221、对于日常维护工作，连接路由器的协议通常使用：（B）。缺少 D 选项

A、TELNET，简单，容易配置　　B、SSH &SSHv2 加密算法强劲，安全性好

C、TELNET 配置 16 位长的密码，加密传输，十分安全　　D、

222、BOTNET 是（C）。

A、普通病毒　　B、木马程序　　C、僵尸网络　　D、蠕虫病毒

223、监听的可能性比较低的是（B）数据链路。

A、Ethernet　　B、电话线　　C、有线电视频道　　D、无线电

224、当 IPS 遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（B）。

A、pass　　B、bypass　　C、watchdog　　D、HA

225、网络环境下的 security 是指（A）。

A、防黑客入侵，防病毒，窃取和敌对势力攻击

B、网络具有可靠性，可防病毒，窃密和敌对势力攻击

C、网络具有可靠性，容灾性，鲁棒性

D、网络的具有防止敌对势力攻击的能力

226、某一案例中，使用者已将无线 AP 的 SSID 广播设置为禁止，并修改了默认 SSID 值，但仍有未经授权的客户端接入该无线网络，这是因为（D）

A、禁止 SSID 广播仅在点对点的无线网络中有效

B、未经授权客户端使用了默认 SSID 接入

C、无线 AP 开启了 DHCP 服务

D、封装了 SSID 的数据包仍然会在无线 AP 与客户端之间传递

227、为了保护 DNS 的区域传送（zone transfer），应该配置防火墙以阻止（B）。

1.UDP

2.TCP

3.53

4.52

A、1,3　　B、2,3　　C、1,4　　D、2,4

228、以下不属于代理服务技术优点的是（D）。

A、可以实现身份认证　　B、内部地址的屏蔽盒转换功能

C、可以实现访问控制　　D、可以防范数据驱动侵袭

229、应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（C）。

A、60%　　B、70%　　C、80%　　D、90%

230、TCP 协议与 UDP 协议相比，TCP 是（B），UDP 是（）。

A、设置起来麻烦；很好设置　　B、容易；困难

C、面向连接的；非连接的　　D、不可靠的；可靠的

231、交换机转发以太网的数据基于：（B）。

A、交换机端口号　　B、MAC 地址　　C、IP 地址　　D、数据类别

232、HTTP，FTP，SMTP 建立在 OSI 模型的哪一层？（D）

A、2 层-数据链路层　　B、3 层-网络层　　C、4 层-传输层　　D、7 层-应用层

233、网络安全的基本属性是（D）。

A、机密性　　B、可用性　　C、完整性　　D、以上都是

234、网络安全的主要目的是保护一个组织的信息资产的（A）。

A、机密性、完整性、可用性　　B、参照性、可用性、机密性、

C、可用性、完整性、参照性　　D、完整性、机密性、参照性

235、DBS 是采用了数据库技术的计算机系统。DBS 是一个集合体，包含数据库、计算机硬件、软件和（C）。

A、系统分析员　　B、程序员　　C、数据库管理员　　D、操作员

236、MySQL -h host -u user -p password 命令的含义如下，哪些事正确的？（D）

A、-h 后为 host 为对方主机名或 IP 地址　　B、-u 后为数据库用户名

C、-p 后为密码　　D、以上都对

237、Oracle 当连接远程数据库或其它服务时，可以指定网络服务名，Oracle9i 支持 5 中命名方法，请选择错误的选项。（D）

A、本地命名和目录命名　　B、Oracle 名称（Oracle Names）

C、主机命名和外部命名　　D、DNS 和内部命名

238、Oracle 的数据库监听器（LISTENER）的默认通讯端口是？（A）

A、TCP 1521　　B、TCP 1025　　C、TCP 1251　　D、TCP 1433

239、Oracle 默认的用户名密码为（A）。

A、Scote/tiger　　B、root　　C、null　　D、rootroot

240、Oracle 数据库中，物理磁盘资源包括哪些（D）。

A、控制文件　　B、重做日志文件　　C、数据文件　　D、以上都是

241、Oracle 中启用审计后，查看审计信息的语句是下面哪一个？（C）

A、select * from SYS.AUDIT$　　B、select * from syslogins

C、select * from SYS.AUD$　　D、AUDIT SESSION

242、SMTP 的端口？（A）

A、25　　B、23　　C、22　　D、21

243、SQL Server 的登录账户信息保存在哪个数据库中？（C）

A、model　　B、msdb　　C、master　　D、tempdb

244、SQL Sever 的默认 DBA 账号是什么？（B）

A、administrator　　B、sa　　C、root　　D、SYSTEM

245、SQL Sever 的默认通讯端口有哪些？（B）

A、TCP 1025　　B、TCP 1433　　C、UDP 1434　　D、TCP 14333　　E、TCP 445

246、SQL Sever 中可以使用哪个存储过程调用操作系统命令，添加系统账号？（B）

A、xp_dirtree　　B、xp_cmdshell　　C、xp_cmdshell　　D、xpdeletekey

247、SQL Sever 中下面哪个存储过程可以执行系统命令？（C）

A、xp_regread　　B、xp_command　　C、xp_cmdshell　　D、sp_password

248、SQL 的全局约束是指基于元祖的检查子句和（C）。

A、非空值约束　　B、域约束子句　　C、断言　　D、外键子句

249、SQL 数据库使用以下哪种组件来保存真实的数据？（C）

A、Schemas　　B、Subschemas　　C、Tables　　D、Views

250、SQL 语句中，彻底删除一个表的命令是（B）。

A、delete　　B、drop　　C、clear　　D、remore

251、SQL 语言可以（B）在宿主语言中使用，也可以独立地交互式使用。

A、-极速　　B、-嵌入　　C、-混合　　D、-并行

252、SSL 安全套接字协议所用的端口是（B）。

A、80　　B、443　　C、1433　　D、3389

253、不属于数据库加密方式的是（D）。

A、库外加密　　B、库内加密　　C、硬件/软件加密　　D、专用加密中间件

254、测试数据库一个月程序主要应对的风险是（B）。

A、非授权用户执行“ROLLBACK”命令　　B、非授权用户执行“COMMIT”命令

C、非授权用户执行“ROLLRORWARD”命令　　D、非授权用户修改数据库中的行

255、查看 Oracle　8i 及更高版本数据库的版本信息的命令是（C）。----缺少 CD 选项

A、cd $Oracle_HOME/orainst　B、C-cd $Oracle_HIME/orainst　　C、　　D、

256、从安全的角度来看，运行哪一项起到第一道防线的作用？（C）

A、远端服务器　　B、WEB 服务器　　C、防火墙　　D、使用安全 shell 程序

257、从下列数据库分割条件中，选出用于抵御跟踪器攻击和抵御对线性系统攻击的一项。（B）。

A、每个分割区 G 有 g=|G|记录，其中 g=0 或 g>=n，且 g 为偶数，

B、记录必须成对地加入 G 或从 G 中删除

C、查询集虚报口各个分割区，如果查询含有一个以上记录的统计信息是从 m 各分割区 G1，G2，… …Gm 中每一个分割区而来的，则统计信息 g（G1VG2V… …VGm）是允许发布

D、记录必须不对地加入 G 或从 G 中删除

258、单个用户使用的数据库视图的描述为（A）。

A、外模式　　B、概念模式　　C、内模式　　D、存储模式

259、对于 IIS 日志记录，推荐使用什么文件格式？（D）

A、Microsoft　IIS 日志文件格式　　B、NCSA 公用日志文件格式

C、ODBC 日志记录格式　　D、W3C 扩展日志文件格式

260、对于 IIS 日志文件的存放目录，下列哪项设置是最好的？（D）----缺少 D 选型

A、%WinDir%\System32\LogFiles　　B、C:\Inetpub\wwwroot\LogFiles

C、C:\LogFiles..)-F:\LogFiles　　D、

261、对于 IIS 日志文件的访问权限，下列哪些设置是正确的？（D）

A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）

B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）

C、SYSTEM（完全控制）Administrator（完全控制）Inernet 来宾账户（读取和运行）

D、SYSTEM（完全控制）Administrator（完全控制）

262、对于数据库的描述一下哪项说法是正确的？（A）

A、数据和一系列规则的集合　　B、一种存储数据的软件

C、一种存储数据的硬件　　D、是存放人量数据的软件

263、攻击者可能利用不必要的 extproc 外部程序调用功能获取对系统的控制权，威胁系统安全。关闭 Extproc 功能需要修改 TNSNAMES.ORA 和 LISTENER.ORA 文件删除一下条目，其中有一个错误的请选择出来（A）。

A、sys_ertproc　　B、icache_extproc

C、PLSExtproc　　D、extproc

264、关系数据库中，实现实体之间的联系是通过表与表之间的（D）。

A、公共索引　　B、公共存储

C、公共元组　　D、公共属性

265、关系型数据库技术的特征由一下哪些元素确定的？（A）

A、行和列　　B、节点和分支

C、Blocks 和 Arrows　　D、父类和子类

266、关于 WEB 应用软件系统安全，说法正确的是（D）？

A、Web 应用软件的安全性仅仅与 WEB 应用软件本身的开发有关

B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C、黑客的攻击主要是利用黑客本身发现的新漏洞

D、以任何违反安全规定的方式使用系统都属于入侵

267、目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（D）？

A、数据库系统庞大会提供管理成本　　B、数据库系统庞大会降低管理效率

C、数据的集中会降低风险的可控性　　D、数据的集中会造成风险的集中

268、哪一个是 PKI 体系中用以对证书进行访问的协议（B）？

A、SSL　　B、LDAP　　C、CA　　D、IKE

269、如果一个 SQL Server 数据库维护人员，需要具有建立测试性的数据库的权限，那么应该指派给他哪个权限（A）？

A、Database　Creators　　B、System　Administrators

C、Server　Administrators　　D、Security　Adiministrators

270、如果以 Apache 为 WWW 服务器，（C）是最重要的配置文件。

A、access.conf　　B、srm.cong　　C、httpd.conf　　D、mime.types

271、若有多个 Oracle 数据需要进行集中管理，那么对 sysdba 的管理最好选择哪种认证方式（B）？

A、系统认证　　B、password 文件认证方式　　C、域认证方式　D、以上三种都可

272、数据库管理系统 DBMS 主要由哪两种部分组成？（A）

A、文件管理器和查询处理器　　B、事务处理器和存储管理器

C、存储管理器和查询处理器　　D、文件管理器和存储管理器

273、数据库系统与文件系统的最主要区别是（B）。

A、数据库系统复杂，而文件系统简单

B、文件系统不能解决数据冗余和数据独立性问题，而数据库系统可以解决

C、文件系统只能管理程序文件，而数据库系统能够管理各宗类型的文件

D、文件系统管理的数据量较少，而数据库系统可以管理庞大的数据量

274、为了防止电子邮件中的恶意代码，应该由（A）方式阅读电子邮件。

A、纯文本　　B、网页　　C、程序　　D、会话

275、为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下

哪一项是耗费计算资源最多的一种垃圾邮件过滤机（D）？

A、SMTP 身份认证　　B、逆向名字解析　　C、黑名单过滤　　D、内容过滤

276、为什么要对数据库进行“非规范化”处理（B）？

A、确保数据完整性　B、增加处理效率　　C、防止数据重复　　D、节省存储空间

277、下列不属于 WEB 安全性测试的范畴的是（A）？

A、数据库内容安全性　　B、客户端内容安全性

C、服务器端内容安全性　　D、日志功能

278、下列操作中，哪个不是 SQL Server 服务管理器功能（A）？

A、执行 SQL 查询命令　　B、停止 SQL　Server 服务

C、暂停 SQL　Server 服务　　D、启动 SQL　Server 服务

279、下列关于 IIS 的安全配置，哪些是不正确的（C）？

A、将网站内容移动到非系统驱动程序　　B、重命名 IUSR 账户

C、禁用所有 WEB 服务扩展　　D、创建应用程序池

280、下列哪些不是广泛使用 http 服务器？（D）

A、W3C　　B、Apache　　C、IIS　　D、IE

281、下列哪些属于 WEB 脚本程序编写不当造成的（C）？

A、IIS5.0　Webdav Ntdll.dll 远程缓冲区一处漏洞

B、apache 可以通过../../../../../../../etc/passwd 方位系统文件

C、登陆页面可以用 password=’a’or’a’=’a’绕过

D、数据库中的口令信息明文存放

282、下列哪种方法不能有效的防范 SQL 进入攻击（C）？

A、对来自客户端的输入进行完备的输入检查

B、把 SQL 语句替换为存储过程、预编译语句或者使用 ADO 命令对象

C、使用 SiteKey 技术

D、关掉数据库服务器或者不使用数据库

283、下列哪种工具不是 WEB 服务器漏洞扫描工具（B）？

A、Nikto　　B、Web　Dumper　　C、paros　Proxy　　D、Nessus

284、下列哪种攻击不是针对统计数据库的（D）？

A、小查询集合大查询集攻击　B、中值攻击　　C、跟踪攻击　　D、资源解析攻击

285、下列哪项中是数据库中涉及安全保密的主要问题（A）？

A、访问控制问题　　B、数据的准确性问题

C、数据库的完整性问题　　D、数据库的安全性问题

286、下列应用服务器中，不遵循 J2EE 规范的是（C）？

A、MTS　　B、WebLogic　　C、Oracle 9iApplication Server　　D、WebSpere

287、下面关于 IIS 报错信息含义的描述正确的是（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

288、下面关于 Oracle 进程的描述，哪项是错误的（B）？

A、运行在 Windows 平台上的 Oracle 能让每个用户组程序化地打开新的进程，这是一个安全隐患

B、在 Windows 平台，除了 Oracle.exe 进程外还有其他的独立进程

C、unix 平台上有多个独立运行的进程，包括数据写进程、日志写进程、存档进程、系统监控进程、进程监控进程

D、有一个特殊的内存区域被映射为*nix 平台上的所有进程，此区域时系统全局去

289、下面哪一项是与数据库管理员（DBA）职责不相容的（C）？

A、数据管理　　B、信息系统管理　　C、系统安全　　D、信息系统规划

290、下面选型中不属于数据库安全控制的有（D）。

A、信息流控制　　B、推论控制　　C、访问控制　　D、隐通道控制

291、下面选型中不属于数据库安全模型的是（D）。

A、自主型安全模型　　B、强制型安全模型　　C、基于角色的模型　　D、访问控制矩阵

292、一般来说，通过 WEB 运行 http 服务的子进程时，我们会选择（D）的用户权限方式，这样可以保证系统的安全。

A、root　　B、httpd　　C、guest　　D、nobody

293、一下不是数据库的加密技术的是（D）。

A、库外加密　　B、库内加密　　C、硬件加密　　D、固件加密

294、一下对于 Oracle 文件系统描述错误的是（B）？

A、*nix 下 Oracle 的可执行文件在$Oracle_HOME/bin/Oracle,$Oracle_HOME/bin 也应该包含在路径环境变量内

B、Windows 下 Oracle 的可执行文件在%Oracle_HOME%\bin\Oracle.exe,其他

C、硬件加密　　D、固件加密

295、以下几种功能中，哪个是 DBMS 的控制功能（A）？

A、数据定义　　B、数据恢复　　C、数据修改　　D、数据查询

296、以下哪个安全特征和机制是 SQL 数据库所特有的（B）？

A、标识和鉴别　　B、数据恢复　　C、数据修改　　D、数据查询

297、以下哪个是数据库管理员（DBA）可以行使的职责（A）？

A、系统容量规划　　B、交易管理　　C、审计　　D、故障承受机制

298、以下哪条命令能利用“SQL 注入”漏洞动用 XP_cmdshell 存储过程，获得某个子目的清单？（A）

A、http://localhost/script?':EXEC+master..XP_cmdshell+'dir':--

B、http://localhost/script?1':EXEC+master..XP_cmdshell+'　dir':--

C、http://localhost/script?0':EXEC+master..XP_cmdshell+'　dir':--

D、http://localhost/script?1':EXEC+master..XP_cmdshell+'　dir'--

299、以下哪条命令能利用“SQL”漏洞动用 XP_cmdshell 存储过程，启动或停止某项服务？（B）

A、http://localhost/script?':EXEC+master..XP_servicecontrol+'start',+'Server'　;-

B、http://localhost/script?0':EXEC+master..XP_servicecontrol+'start',+'Server'　;--

C、http://localhost/script?1':EXEC+master..XP_servicecontrol+'start',+'Server'　; --

D、http://localhost/script?0':EXEC+master..XP_servicecontrol+'start',+'Server' --

300、以下哪项不属于访问控制策略的实施方式？（D）

A、子模式法　　B、修改查询法　　C、集合法　　D、验证法

301、以下哪一项是和电子邮件系统无关的？（）

A、PEM(Privacy enhanced mail)　　B、PGP(Pretty good privacy)

C、X.500　　D、X.400

302、以下哪种方法可以用于对付数据库的统计推论？（C）

A、信息流控制　　B、共享资源矩阵　　C、查询控制　　D、间接存取

303、以下是对层次数据库结构的描述，请选择错误描述的选项。（C）

A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来

B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据

C、它的优点是用户不需要十分熟悉数据库结构

D、层次数据库模型的结构就像是一棵倒转的树

304、以下是对单用户数据库系统的描述，请选择错误描述的选项（C）。

A、单用户数据库系统是一种早期的最简单的数据库系统

B、在单用户系统中，整个数据库系统，包括应用程序、DBMS、数据，都装在一台计算机之间不能共享数据

C、在单用户系统中，由多个用户共用，不同计算机之间能共享数据

D、单用户数据库系统已经不适用于现在的使用，被逐步淘汰了

305、以下是对分布式结构数据库系统的描述，请选择错误描述的选项。（D）

A、分布式结构的数据库系统的数据在逻辑上是一个整体，但物理地分布在计算机网络的不同节点上，每个节点上的主机又带有多个终端用户

B、网络中的每个节点都可以独立的处理数据库中的数据，执行全局应用

C、分布式结构的数据库系统的数据分布存放给数据的处理、管理和维护带来困难

D、分布式结构的数据库系统的数据只在存放在服务器端，其他节点只进行处理和执行

306、以下是对关系数据库结构的描述，请选择错误描述的选项。（D）

A、数据存储的主要载体是表，或相关数据组

B、有一对一、一对多、多对多三种表关系

C、表关联是通过引用完整性定义的，这是通过主码和外码（主键或外键约束条件实现的）

D、缺点是不支持 SQL 语言

307、以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（A）

A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力

B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行 DBMS 功能又执行应用程序

C、在网络中把某些节点的计算机专门用于执行 DBMS 核心功能，这台计算机就成为数据库服务器

D、其他节点上的计算机安装 DBMS 外围应用开发工具和应用程序，支持用户的应用，称为客户机

308、以下是对面向对象数据库结构的描述，请选择错误描述的选项。（C）

A、它允许用对象的概念来定义与关系数据库交互

B、面向对象数据库中有两个基本的结构：对象和字面量

C、优点是程序员需要掌握与面向对象概念以及关系数据库有关的存储

D、缺点是用户必须理解面向对象概念，目前还没有统一的标准，稳定性还是一个值得关注的焦点

309、以下是对主从式结构 数据库系统的描述，请选择错误描述的选项。（D）

A、主从式结构是指一个主机带多个终端的多用户结构

B、在这种结构中，数据库系统的应用程序、DBMS、数据等都集中存放在主机上

C、所有处理任务都由主机来完成，各个用户通过主机的终端并发地存取数据，能够共享数据源

D、主从式结构的优点是系统性能高，是当终端用户数目增加到一定程度后，数据的存取通道不会形成瓶颈

311、在 GRUB 的配置文件 grub.conf 中，“timeout=-1”的含义是（C）。

A、不等待用户选择，直接启动默认的系统

B、在 10 秒钟内，等待用户选择要启动的系统

C、一直等待用户选择要启动的系统

D、无效

312、在 Oracle 中，quota 可以限制用户在某个表空间上最多可使用多少字节，如果要限制 data_ts 表 500K，以下哪个是正确的命令？（B）

A、quo 500k in data_ts　　B、quota 500K on data_ts

C、quota data_ts ,imit 500K　　D、quota data_ts on 500K

313、在 Oracle 中，建表约束包括引用完整性约束、check 完整性约束，还有以下三项是正确的，请排除一个错误选项。（D）

A、非空完整性约束　　B、唯一完整性约束

C、主码完整性约束　　D、数据角色性约束

314、在 Oracle 中，将 scott 的缺省表空间改为 data2_ts，下列哪个是正确的？（A）

A、ALTER USER scott DEFAULT TABLESPACE data2_ts

B、ALTER DEFAULT TABLESPACE data2_ts USER scott

C、ALTER USER scott TABLESPACE DEFAULT data2_ts

D、ALTER scott USER DEFAULT TABLESPACE data2_ts

315、在 Oracle 中，将 scott 的资源文件改为 otherprofile，下列哪个是正确的？（C）

A、ALTER PROFILE USER scott otherprofile

B、ALTER otherprofile USER scottPROFILE

C、ALTER USER scott PROFILE otherprofile

D、ALTER scott USER PROFILE otherprofile

316、在 Oracle 中，将当前系统所有角色都授予 scott，除 Payroll 外，下列哪个是正确的？（D）

A、ALTER DEFAULT ROLLE USER scott ALL EXCEPT Payroll

B、ALTER USER DEFAULT ROLLE ALL EXCEPT Payroll

C、ALTER DEFAULT ROLLE ALL EXCEPT USER scott

D、ALTER USER scott DEFAULT ROLLE ALL EXCEPT Payroll

317、在 Oracle 中，用 ALTER 将 scott 的口令改为 hello，下列哪个是正确的？（A）

A、ALTER USER scott IDENTIFIED BY hello

B、ALTER scott USER IDENTIFIED BY hello

C、ALTER USER scott IDENTIFIED AS hello

D、ALTER USER hello IDENTIFIED BY scott

318、在 WEB 应用软件的基本结构中，客户端的基础是（A）。

A、HTML 文档　　B、客户端程序

C、HTML 协议　　D、浏览器

319、在 WEB 应用软件的系统测试技术中，下面不属于安全性测试内容的是（C）。

A、客户端的内容安全性　　B、服务器的内容安全性

C、数据库的内容安全性　　D、Cookie 安全性

320、在典型的 WEB 应用站点的层次结构中，“中间件”是在哪里运行的？（C）

A、浏览器客户端　　B、web 服务器

C、应用服务器　　D、数据库服务器

321、在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（C）

A、对话管理服务　　B、事务管理服务

C、资源管理服务　　D、控制管理服务

322、主要用于加密机制的协议时（D）。

A、HTTP　　B、FTP　　C、TELNETD　　D、SSL

323、分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？（D）

A、自主性　　B、可靠性　　C、灵活性　　D、数据备份

324、下面对 Oracle 的密码规则描述，哪个是错误的？（D）

A、Oracle 密码必须由英文字母，数值，#，下划线(_)，美元字符（$）构成，密码的最大长度为 30 字符，并不能以“$”,“#”,“_”或任何数字卡头；密码不能包含像“SELECT”,“DELETE”,“CREATE”这类的 ORACLE/SQL 关键字

B、Oracle 的若算法加密机制（）两个相同的用户名和密码在两台不同的 ORACLE 数据库机器中，将具有相同的哈希值。这些哈希值存储在 SYS.USER 表中，可以通过像 DBA_USE 这类的试图来访问

C、Oracle 默认配置下，每个中户如果有 10 此的失败登录，此账户将会被锁定

D、SYS 账户在 Oracle 数据库中有最高权限，能够做任何事情，包括启动/关闭 Oracle 数据库，如果 SYS 被锁定，将不能访问数据库

325、无论是哪一种 Web 服务器，都会受到 HTTP 协议本身安全问题的困扰，这样的信息系统安全漏洞属于（C）。

A、设计型漏洞　　B、开发型漏洞　　C、运行型漏洞　　D、以上都不是

326、SSL 加密的过程包括以下步骤：（1）通过验证以后，所有数据通过密钥进行加密，使用 DEC 和 RC4 加密进行加密；(2)随后客户端随机生成一个对称密钥；(3)信息通过 HASH 加密，或者一次性加密（MD5SHA）进行完整性确认；（4）客户端和服务器协商建立加密通道的特定算法。正确的顺序的是（D）

A、（4）（3）（1）（2）　　B、（4）（1）（3）（2）

C、（4）（2）（3）（1）　　D、（4）（2）（3）（1）

327、影响 WEB 系统安全的因素，不包括？（C）

A、复杂应用系统代码量大、开发人员多、难免出现疏忽

B、系统屡次升级、人员频繁变更，导致代码不一致

C、历史遗留系统、试运行系统等对个 WEB 系统运行于不同的服务器上

D、开发人员未经安全编码培训

328、Oracle 通过修改用户密码策略可提高密码强度，以下哪个密码策略参数中文描述是错误的？（A）

A、PASSWORD_MAX　　登录超过有效次数锁定时间

B、FAILED_LOGIN_ATTEMPTS　　最大错误登录次数

C、PASSWORD_GRACE_TIME　　密码失效后锁定时间

D、PASSWORD_LIFE_TIME　　口令有效时间

329、SQL Server 服务有一个启动账号，默认账号是属于 administrators 组，现在为了安全需要创建一个新的服务启动账号，它需要哪些权限既能兼顾安全又能保证启动数据库成功，请排除一个错误的。（D）

A、数据库本地目录的读写权限　　B、启动本地服务的权限

C、读取注册表的权限　　D、通过 API 访问 Windows Resource

330、作为一台运行 IIS 在 Internet 发布站点的 Windows Web 服务器，下面哪项服务不是必需的？（B）

A、IIS Admin　　B、Net Logon

C、Performance Logs and Alerts　　D、World Wide Web Publishing

331、数据库中超级账户不能被锁定，其中 Oracle 的是（），mysql 的是（），SQLServer 的是（C）。

A、sa，root，sys　　B、admin，root，sa

C、sys，root，sa　　D、sys，admin，sa

332，Oracle 的安全机制，是由（A）、实体权限和角色权限这三级体系结构组成的。

A、系统权限　　B、索引权限　　C、操作权限　　D、命令控制

333、对 SQL 数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（B）

A、--　　B、-　　C、-=　　D、-+

334、在 Web 页面中增加验证码功能后，下面说法正确的是（A）。

A、可以增加账号破解等自动化软件的攻击难度　　B、可以防止文件包含漏洞

C、可以防止缓冲溢出　　D、可以防止 浏览

335、以下破解 Oracle 密码哈希值的步聚，其中哪个描述是错误的？（B）

A、用 Sqlplus 直接登录到 Oracle 数据库，使用 select username，password form dba_users 命令查看数据库中的用户名和密码，此时看到的密码是哈希值

B、在 Cain 的 Cracker 菜单点击导入用户名和哈希值，可直接显示用户密码明文

C、在 Cain 的 Cracker 菜单点解导入用户名和哈希值，只能通过字典破解

D、在 Cain 的 Rainbow 生成的表会占用大量的硬盘空间和内存，可是破解速度和效率

很高

336、在数据库向因特网开放前，哪个步聚是可以忽略的？（B）

A、安全安装和配置操作系统和数据库系统

B、应用系统应该在内网试运行 3 个月

C、对应用软件如 Web 也没、ASP 脚本等进行安全性检查

D、网络安全策略已经生效

337、如果不设置必要的日志审核，就无法追踪回朔安全事件，检查是否启用通用查询日志，打开/etcmy.cnf 文件，查看是否包含如下设置，选出一个正确的（D）。

A、audit=filename　　B、sys=filename　　C、event=filename　　D、log=filename

338、针对一台对外提供 Web 服务的 Windows 服务器，下列关于账户权限控制，哪些项是不合理的？（C）

A、限制匿名账户对 Web 内容的目录写权限

B、从 Everyone 组中删除“从网络访问此计算机”用户权限

C、禁用 IUSR-MACHE 和 IWAN_MACHINE 账户

D、本地登录时必须使用 Administrators 账户

339、网上营业中间件如果启用了 SSl，应采用不低于（C）版本的 SSL，采用经国家密码管理局认可的密码算法。

A、2.0　　B、2.5　　C、3.0　　D、3.1

340、SQL　Server 默认的具有 DBA 权限的账号是什么？（C）

A、root　　B、admin　　C、sa　　D、system

341、（A）是指电子系统或设备在自己正常工作产生的电磁环境下，电子系统或设备之间的相互之间的相互不影响的电磁特性。

A、电磁兼容性　　B、传导干扰　　C、电磁干扰　　D、辐射干扰

342、（C）是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。

A、电磁兼容性　　B、传导干扰　　C、电磁干扰　　D、辐射干扰

343、《计算机信息系统雷电电磁脉冲安全防护规范》的标准编号是（B）。

A、GA 163-1997　　B、GA 267-2000

C、GA 243-2000　　D、GB 17859-1999

344、安装了合格防雷保安器的计算机信息系统，还必须在（C）雷雨季节前对防雷保安器、

保护接地装置进行一次年度检查，发现不合格时，应及时修复或更换。

A、第三年　　B、第二年　　C、每年　　D、当年

345、使用 IIalon 灭火的工作原理是什么？（C）

A、降低温度　　B、隔绝氧气和可燃物

C、破坏氧气和可燃物之间的化学反应　　D、减少氧气

346、白炽灯、高压汞灯与可燃物、可燃结构之间的距离不应小于（C）cm。

A、30　　B、40　　C、50　　D、60

347、被电击的人能否获救，关键在于（D）。

A、触电的方式　　B、人体电阻的大小

C、触电电压的高底　　D、能否尽快脱离电源和施行紧急救护

348、布置电子信息系统信号线缆的路由走向时，以下做法错误的是（A）。

A、可以随意弯折　　B、转弯是，弯曲半径应大于导线直径的 10 倍

C、尽量直线、平整　　D、尽量减小由线缆自身形成的感应环路面积

349、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法　　B、隔离灭火法　　C、冷却灭火法

350、长期在高频电磁场作用下，操作者会有什么不良反应？（B）

A、呼吸困难　　B、神经失常　　C、疲劳无力

351、触电事故中，绝大部分是由于（A）导致人身伤亡的。

A、人体接受电流遭到电击　　B、烧伤　　C、触电休克

352、从业人员发现直接危及人身安全的紧急情况时，例如气体灭火系统开始开启时，应（A）。

A、停止作业，立即撤离危险现场　　B、继续作业

C、向上级汇报，等待上级指令

353、从业人员既是安全生产的保护对象，又是实现安全生产的（C）。

A、关键　　B、保证　　C、基本要素

354、低压验电笔一般适用于交、直流电压未（C）伏以下。

A、220　　B、380　　C、500

355、电流为（B）毫安是，称为致命电流。

A、50　　B、100　　C、120　　D、150

356、电器的保险丝只能装在（B）上。

A、零线　　B、火线　　C、底线

357、电器着火是不能用（C）灭火。

A、四氧化碳或 1211 灭火　　B、沙土　　C、水

358、对不符合防雷标准、规范防雷工程专业设计方案，以下（B）应当按照审核结论进行修改并重新报批。

A、建设单位　　B、防雷工程专业设计单位　　C、工程施工单位

359、发现人员触电时，应（B），使之脱离电源。

A、立即用手拉开触电人员　　B、用绝缘物体拨开电源或触电者

C、用铁棍拨开电源线

360、凡设在年平均雷电日大于（C）的地区的计算机信息系统，原则上均应装设计算机信息系统防雷保安器，以防止雷电电磁脉冲过电压和过电流侵入计算机信息系统设备。

A、40　　B、45　　C、5　　D、15

361、废电池随处丢弃会造成（B）的污染。

A、白色污染　　B、重金属污染　　C、酸雨

362、干粉灭火器多长时间检查一次？（A）

A、半年　　B、一年　　C、三个月　　D、两年

363、根据国家相关规定，电压（D）以下不必考虑防止电击的安全？

A、48 伏　　B、36 伏　　C、65 伏　　D、25 伏

364、根据作业环境的不同，安全帽的颜色也不同，如在爆炸性作业场所工作宜戴（A）安全帽。

A、红色　　B、黄色　　C、白色

365、关于空气的正向压力，下面哪项描述是正确的？（B）

A、当门打开时，空气向内流动　　B、当门打开，空气向外流动

C、当发生火灾，系统自动切断电源　　D、当发生火灾，烟雾向另外一间房间流动

366、国家颁布的《安全色》标准中，表示警告、主要的颜色为（C）。

A、红色　　B、蓝色　　C、黄色

367、火灾中对人员威胁最大的是（B）。

A、火　　B、烟气　　C、可燃物

368、机房内电源馈线不得与计算机信号传输线靠近或并排敷设。空间不允许时，两者间距应不少于（B）m。

A、0.1　　B、0.6　　C、1.2　　D、0.3

369、计算机电源系统的所有节点均应镀铅锡处理（B）连接。

A、热压　　B、冷压　　C、焊锡　　D、直接

370、计算机系统接地应采用（A）。

A、专用底线　　B、和大楼的钢筋专用网相连

C、大楼的各种金属管道相连　　D、没必要

371、采取适当的措施，使燃烧因缺乏或隔绝氧气而熄灭，这种方法称作（A）。

A、窒息灭火法　　B、隔离灭火法　　C、冷却灭火法

372、计算机系统应选用（A）电缆。

A、铜芯　　B、铅芯

C、铁芯　　D、没有要求

373、进行腐蚀品的装卸作业应戴（B）手套。

A、帆布　　B、橡胶　　C、棉布

374、人体在电磁场作用下，由于（C）将使人体受到不同程度的伤害。

A、电流　　B、电压　　C、棉布

375、身上着火后，下列哪种灭火方法是错误的（C）。

A、就地打滚　　B、用厚重衣物覆盖压灭火苗　　C、迎风快跑

376、生产经营单位必须为从业人员提供符合国家标准或（C）标准的劳动防护用品。

A、当地　　B、本单位　　C、行业

377、使用新设备，必须了解、掌握其安全技术特征，采取有效的安全防护措施，并对从业人员进行专门的安全生产。（B）

A、当地　　B、本单位　　C、行业

378.实验地点相对湿度大于 75%时，则此实验环境属于易触电的环境：（A）

A、危险　　B、特别危险　　C、一般

379、通过人身的安全交流电流规定在(A)以下。

A、10mA　　B、30mA　　C、50mA

380、下列不属于对物理层信息窃取的是(D)

A、对存储介质的盗取　　B、对监视器的窃听

C、对网络线路的窃听　　D、对设备屏蔽电磁干扰

381、新、改、扩建项目的安全设施投资应当纳入(C)。

A、企业成本　　B、安措经费　　C、建设项目概算

382、液体表面的蒸汽与空气形成可燃气体，遇到点火源时，发生一闪即灭的现象称为(C)

A、爆炸　　B、蒸发　　C、闪燃

383、防雷保安器：防止(B)破坏计算机信息系统的保安装置，可分为两大类：电源线防雷保安器(简称电源防雷保安器)和信号传输线防雷保安器(简称通道防雷保安器)。

A、直击雷　　B、感应雷　　C、雷暴　　D、雷电电磁脉冲

384、EMC 标准是为了保证(D)正常工作而制走的。

A、网络　　B、媒体　　C、信息　　D、系统和设备

385、以下不符合防静电要求的是(B)。

A、穿合适的防静电衣服和防静电鞋　　B、在机房内直接更衣梳理

C、用表面光滑平整的办公家具　　D、经常用湿拖布拖地

386、以下哪些属于系统的物理故障？(A)

A、硬件故障与软件故障　　B、计算机病毒

C、人为的失误　　D、网络故障和设备环境故障

387、用灭火器灭火时，灭火器的喷射口应该对准火焰的(C)。

A、上部　　B、中部　　C、根部

388、运输、携带、邮寄计算机信息媒体进出靖的，应当如实向(A)申报。

A、海关　　B、工商

C、税务　　D、边防

389、在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ (B)

A、产生静电　　B、计算机部件腐蚀

C、有污染物　　D、B+A

390、在空气不流通的狭小地方使用二氧化碳灭火器可能造成的危险是(B)。

A 中毒　　B 缺氧　　C 爆炸

391、在雷雨天不要走近高压电杆、铁塔、避雷针、远离至少(C)米以外。

A、IO 米　　B、15 米　　C、20 米

392、在易燃易爆场所穿(C)最危险。

A、布鞋　　B、胶鞋　　C、带钉鞋

393、在遇到高压电线断落地面时，导线断落点(B)m 内，禁止人员进入。

A、IO　　B、20　　C、30

394、数据处理中心的物理环境中，最佳湿度应该保持在什么样的程度？(C)

A、30%-40%　　B、40%-50%　　C、45%-60%　　D、50%-70%

395、计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所以防雷保安器必须有合理的(B)。

A、屏蔽配置　　B、接地配置

C、分流配置　　D、均压配置

396、计算站场地宜采用(A)蓄电池。

A、封闭式　　B、半封闭式

C、开启式　　D、普通任意的

397、多层的楼房中，最适合做数据中心的位置是(D)。

A、楼　　B、地下室

C、顶楼　　D、除以上外的任何楼层

398、计算机机房是安装计算机信息系统主体的关键场所，是(A)工作的重点，所以对计算机机房要加强安全管理。

A、实体安全保护　　B、人员管理

C、媒体安全保护　　D、设备安全保护

399、区域安全，首先应考虑（B），用来识别来访问的用户的身份，并对其合法性进行验证，主要通过特殊标示符、口令、指纹等来实现。

A、来访者所持物　　B、物理访问控制　　C、来访者所具有的特征　　D、来访者所知信息

400、在计算机房出入口处或值班室，应设置（D）和应急断电装置。

A、 电视　　B、电扇　　C、报警器　　D、应急电话

401、下列（A）灭火器是扑救精密仪器火灾的最佳选择。

A、二氧化碳灭火剂　　B、干粉灭火剂　　C、泡沫灭火剂

402、电气安全主要包括人身安全、（B）安全。

A、照明　　B、设备　　C、电器　　D、空调

403、（C）基于 IDEA 算法。

A、S/MIME　　B、SET　　C、PGP　　D、SSL

404、(C）类型的加密，使得不同的文档和信息进行运算以后得到一个唯一的 128 位编码。

A、对称加密　　B、非对称加密　　C、哈希加密　　D、强壮加密

405、(C)是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。

A、公开密钥体制　　B、对称加密体制　　C、PKI（公开密钥基础设施）　　D、数字签名

406、(D)是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。

A、认证机构　　B、密码　　C、票据　　D、数字证书

407、（D）协议主要用于加密机制。

A、HTTP　　B、FTP　　C、TELNET　　D、SSL

408、（A）原则保证只有发送方与接收方能访问消息内容。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

409、（D）原则允许某些用户进行特定访问。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

410、（B）增加明文冗余度。

A、混淆　　B、扩散　　C、混淆与扩散　　D、都不是

411、3DES 加密算法的密钥长度是：（A）。

A、168　　B、128　　C、56　　D、256

412、AES 密钥长度不能是（D）。

A、128 位　　B、192 位　　C、256 位　　D、512 位

413、AES 算法是哪种算法？（A）。

A、对称密钥加密　　B、非对称密钥加密　　C、哈希算法　　D、流加密

414、AES 属于哪种加密方式？（B）。

A、流加密　　B、分组加密　　C、异或加密　　D、认证加密

415、CA 指的是（A）。

A、证书授权　　B、加密认证　　C、虚拟专用网　　D、安全套接层

416、DES 经过（A）轮运算后，左右两部分合在一起经过一个末置换，输出一个 64 位的密文。（A）

A、16　　B、8　　C、32　　D、4

417、DES 算法是哪种算法？（A）

A、对称密钥加密　　B、非对称密钥加密　　C、哈希算法　　D、流加密

418、DES 属于哪种加密方式？（B）

A、流加密　　B、块加密　　C、异或加密　　D、认证加密

419、DNSSec 中并未采用（C）。

A、数字签名技术　　B、公钥加密技术　　C、地址绑定技术　　D、报文摘要技术

420、ECB 指的是（D）。

A、密文链接模式　　B、密文反馈模式　　C、输出反馈模式　　D、电码本模式

421、EC-DSA 复杂性的程度是（D）。

A、简单　　B、最简单　　C、困难　　D、最困难

422、EFS 可以用在什么文件系统下（C）。

A、FAT16　　B、FAT32　　C、NTFS　　D、以上都可以

423、IDEA 的密钥长度是多少 bit？（D）。

A、56　　B、64　　C、96　　D、128

424、Kerberos 是 80 年代中期，麻省理工学院为 Athena 项目开发的一个认证服务系统，其目标是把认证、记账和（B）的功能扩展到网络环境。

A、访问控制　　B、审计　　C、授权　　D、监控

425、Kerberos 是为 TCP/IP 网络设计的基于（B）的可信第三方鉴别协议，负责在网络上进行仲裁及会话密钥的分配。

A、非对称密钥体系　　B、对称密钥体系　　C、公钥体系　　D、私钥体系

426、Kerberos 是一种网络认证协议。它采用的加密算法是（C）。

A、RSA　　B、PGP　　C、DES　　D、MD5

427、Kerberos 算法是一个（B）。

A、面向访问的保护系统　　B、面向票据的保护系统

C、面向列表的保护系统　　D、面向门与锁的保护系统

428、Kerberos 提供的最重要的安全服务是？（A）。

A、鉴别　　B、机密性　　C、完整性　　D、可用性

429、MD5 产生的散列值是多少位？（C）。

A、56　　B、64　　C、128　　D、160

430、MD5 是按每组 512 位为一组来处理输入的信息，经过一系列变换后，生成一个（B）为散列值。

A、64　　B、128　　C、256　　D、512

431、MD5 是以 512 位分组来处理输入的信息，每一分组又被划分为（A）32 位子分组。

A、16 个　　B、32 个　　C、64 个　　D、128 个

432、MD5 算法将输入信息 M 按顺序每组（D）长度分组，即：M1，M2，...，Mn-1，Mn。

A、64 位　　B、128 位　　C、256 位　　D、512 位

433、PKI（公共密钥基础结构）中应用的加密方式为（B）。

A、对称加密　　B、非对称加密　　C、HASH 加密　　D、单向加密

434、PKI 的全称是（D）。

A、Private Key Intrusion　　B、Public Key Intrusion

C、Private Key Infrastructure　　D、Public Key Infrastructure

435、PKI 无法实现（D）。

A、身份认证　　B、数据的完整性　　C、数据的机密性　　D、权限分配

436、RC4 是由 RIVEST 在 1987 年开发的一种流式的密文，就是实时地把信息加密成一个整体，它在美国一般密钥长度是 128 位，因为受到美国出口法的限制，向外出口时限制到多少位？（C）。

A、64 位　　B、56 位　　C、40 位　　D、32 位

437、RSA 公钥加密系统中，他想给她发送一份邮件，并让她知道是他发出，应选用的加密秘钥是（C）。

A、他的公钥　　B、她的公钥　　C、他的私钥　　D、她的私钥

438、RSA 使用不方便的最大问题是（A）。

A、产生密钥需要强大的计算能力　　B、算法中需要大数

C、算法中需要素数　　D、被攻击过很多次

439、RSA 算法建立的理论基础是（C）。

A、DES　　B、替代想组合　　C、大数分解和素数检测　　D、哈希函数

440、SHA-1 产生的散列值是多少位？（D）。

A、56　　B、64　　C、128　　D、160

441、按密钥的使用个数，密码系统可以分为（C）。

A、置换密码系统和易位密码系统　　B、分组密码系统和序列密码系统

C、对称密码系统和非对称密码系统　　D、密码系统和密码分析系统

442、充分发挥了 DES 和 RSA 两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是：（C）。

A、数字签名　　B、数字指纹　　C、数字信封　　D、数字时间戳

443、从技术角度上看数据安全的技术特征主要包含哪几个方面？（B）。

A、数据完整性、数据的方便性、数据的可用性　　B、数据的完整性、数据的保密性、数据的可用性　　C、数据的稳定性、数据的保密性、数据的可用性　　D、数据的方便性、数据的稳定性、数据的完整性

444、单项散列函数的安全性来自于他的（A）。

A、单向性　　B、算法复杂性　　C、算法的保密性　　D、离散性

445、电路网关防火墙工作在 OSI 协议的哪一层？（A）。

A、传输层　　B、链路层　　C、应用层　　D、物理层

446、电子邮件的机密性与真实性是通过下列哪一项实现的？（A）

A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密

B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密

C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密

D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

447、端对端加密只需要保证消息都在哪里进行加密？（A）

A、源点和目的地节点　　B、经过的每一个节点

C、源点和中间经过的每一个节点　　D、所有节点

448、对明文字母重新排列，并不隐藏他们的加密方法属于（C）。

A、置换密码　　B、分组密码　　C、易位密码　　D、序列密码

449、对网络中两个相邻节点之间传输的数据进行加密保护的是（A）。

A、节点加密　　B、链路加密　　C、端到端加密　　D、DES 加密

450、发送消息和用发送方私钥加密哈希加密信息将确保消息的：（A）。

A、真实性和完整性　　B、真实性和隐私　　C、隐私和不可否认性　　D。隐私和不可否性

451、高级加密标准 AES 算法中，加密回合数不可能是（D）。

A、10　　B、12　　C、14　　D、16

452、公钥机制利用一对互相匹配的（B）进行加密，解密。

A、私钥　　B、密钥　　C、数字签名　　D、数字证书

453、公钥加密体制中，没有公开的是（A）。

A、明文　　B、密文　　C、公钥　　D、算法

454、公钥证书提供了一种系统的、可扩展的、统一的（A）。

A、公钥分发方案　　B、实现不可否认方案

C、对称密钥分发方案　　D、保证数据完整性方案

455、关于 CA 和数字证书的关系，以下说法不正确的是（B）。

A、数字证书是保证双方之间的通讯安全的垫子信任关系，它由 CA 签发

B、数字证书一般依靠 CA 中心的对称密钥机制来实现

C、在电子交易中，数字证书可以用于表明参与方的身份

D、数字证书能以一种不能被假冒的方式证明证书持有人身份

456、关于数字签名说法正确的是（A）。

A、数字签名的加密方法以目前的计算机的运算能力来破解是不现实的

B、采用数字签名，不能够保证信息自签发后到收到为止没有做过任何修改（能保证信息收到后没做个任何修改）

C、采用数字签名，能够保证信息是有签名者自己签名发送的，但由于不是真实的签名，签名者容易否认（签名不容易否认）

D、用户可以采用公钥对信息加以处理，形成数字签名（需使用私钥对信息加以处理）

457、基于私有密钥体制的信息认证方法采用的算法是（D）。

A、素数检测　　B、非对称算法　　C、RSA 算法　　D、对称加密算法

458、加密技术不能实现（D）。

A、数据信息的完整性　　B、基于密码技术的身份认证　　C、机密文件加密　　D 基于 IP 头信息的包过滤

459、加密技术不能提供以下哪种安全服务？（D）。

A、鉴别　　B、机密性　　C、完整性　　D 可用性

460、加密有对称密钥加密、非对称密钥加密两种，数字签名采用的是（B）。

A、对称密钥加密　　B、非对称密钥加密　　C、　　D

461、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 5，即 a 加密成 f。这种算法的密钥就是 5，那么它属于（A）。

A、对称加密技术　　B、分组加密技术　　C、公钥加密技术　　D、单项函数密码技术

462、就是通过使用公开密钥技术和数字证书等来提供网络信息安全服务的基础平台。（C）

A、公开密钥体制　　B、对称加密体制　　C、PKI（公开密钥基础设施）　　D、数字

签名

463、利用非对称密钥体制实现加密通信时，若 A 要向 B 发送加密信息，则该加密信息应该使用（B）。

A、A 的公钥加密　B、B 的公钥加密　C、A 的私钥加密　D、B 的私钥加密

464、利用物理设备将各类型的无法预测的输入集中起来生成随机数的设备是（A）。

A、随机数生成器　B、伪随机数生成器　C、中央处理　D、非易失存储

465、链路加密要求必须先对链路两端的加密设备进行（C）。

A、异步　B、重传　C、同步　D、备份

466、密码处理依靠使用密钥，密钥是密码系统里的最重要因素。以下哪一个密钥算法在加密数据与解密时使用相同的密钥？（C）

A、对称的公钥算法　B、非对称私钥算法　C、对称密钥算法　D、非对称密钥算法

467、密码分析的目的是什么？（A）

A、确定加密算法的强度　B、增加加密算法的代替功能

C、减少加密算法的换为功能　D、确定所使用的换位

468、请从下列各项中选出不是 HASH 函数算法的一项。（D）

A、MD5　B、SHA　C、HMAC　D、MMAC

469、如今，DES 加密算法面临的问题是（A）。

A、密钥太短，已经能被现代计算机暴力破解　B、加密算法有漏洞，在数学上已被破解　C、留有后门，可能泄露部分信息　D、算法过于陈旧，已经有更好的替代方案

470、若单项散列函数的输入串有很小的变化，则输出串（A）。

A、可能有很大的变化　B、一定有很大的变化　C、可能有很小的变化　D、一定有很小的变化

471、散列算法可以做哪些事？（C）。

A、碰撞约束　B、入侵检测　C、组合散列　D、随机数生成器

472、身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（B）。

A、可信性　B、访问控制　C、完整性　D、保密性

473、数字签名常用的算法有（B）。

A、DES 算法　B、RSA 算法　C、Hash 函数　D、AES 算法

474、数字签名和随机数挑战不能防范以下哪种攻击或恶意行为？（D）。

A、伪装欺骗　　B、重放攻击　　C、抵赖　　D、DOS 攻击

475、数字签名可以解决（D）。

A、数据被泄露　　B、数据被篡改　　C、未经授权擅自访问　　D、冒名发送数据或发送后抵赖

476、数字签名通常使用（B）方式。

A、公钥密码体系中的私钥　　B、公钥密码系统中的私钥对数字摘要进行加密

C、密钥密码体系　　D、公钥密码体系中公钥对数字摘要进行加密

477、数字信封是用来解决（C）。

A、公钥分发问题　　B、私钥分发问题　　C、对称密钥分发问题　　D、数据完整性问题

478、数字证书不包括（B）。

A、签名算法　　B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号　　D、颁发数字证书单位的数字签名

479、数字证书的应用阶段不包括（D）。

A、证书检索　B、证书验证　　C、密钥恢复　　D、证书撤销

480、下列说法中错误的是（D）。

A、非对称算法也叫公开密钥算法　　B、非对称算法的加密密钥和解密密钥是分离的
C、非对称算法不需要对密钥通信进行保密　　D、非对称算法典型的有 RSA 算法、AES 算法等

481、下列算法中，哪种不是对称加密算法？（C）

A、AES　　B、DES　　C、RSA　　D、RC5

482、下列算法中属于 Hash 算法的是（C）。

A、DES　　B、IDEA　　C、SHA　　D、RSA

483、以下对于链路加密哪项是正确的？（B）

A、消息只在源点加密，目的节点解密　　B、消息在源点加密，在每一个经过的节点解密并加密　　C、消息在所有经过的节点中都是加密的，但只在目的节点解密　　D、消息以明文形式在节点之间传输

484、以下各种加密算法中属于单钥制加密算法的是（A）。

A、DES 加密算法　　B、Caesar 替代法　　C、Vigenere 算法　　D、Diffie-Hellman

加密算法

485、以下各种加密算法中属于双钥制加密算法的是（D）。

A、DES 加密算法　　B、Caesar 替代法　　C、Vigenere 算法　　D、Diffie-Hellman 加密 486、以下各种算法中属于古典加密算法的是（B）。

A、DES 加密算法　　B、Caesar 替代法　　C、Vigenere 算法　　D、Diffie-Hellman 加密 487、以下关于 CA 认证中心说法正确的是（C）。

A、CA 认证时使用对称密钥机制的认证方法　　B、CA 认证中心支负责签名，不负责证书的产生　　C、CA 认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份 D、CA 认证中心不用保持中立，可以随便找一个用户来作为 CA 认证中心

488、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，和公共网络物理上完全隔离的、安全的线路

B、VPN 指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接

C、VPN 不能做到信息认证和身份认证　　D、VPN 只能提供身份认证、不能提供加密数据的功能

489、以下关于数字签名说法正确的是（D）。

A、数字签名是在所传输的数据后附上一段和传输数据毫无关系的数字信息

B、数字签名能够解决数据的加密传输，即安全传输问题

C、数字签名一般采用对称加密机制　　D、数字签名能够解决篡改、伪造等安全性问题

490、以下密码使用方法中正确的是（D）。

A、将密码记录在日记本上以避免忘记　　B、任何情况下均不得使用临时性密码

C、密码中的字母不得重复　　D、不要使用全部由字母组成的密码

491、以下哪个不包含在证书中？（C）

A、密钥采取的算法　　B、公钥及其参数　　C、私钥及其参数　　D、签发证书的 CA 名称

492、以下哪个选项不会破坏数据库的完整性？（A）

A、对数据库中的数据执行删除操作　　B、用户操作过程中出错

C、操作系统的应用程序错误　　D、DBMS 或操作系统程序出错

493、以下哪项不属于数据库系统实体安全？（B）

A、环境安全　　B、线路安全　　C、设备安全　　D、媒体安全

494、以下哪一种算法产生最长的密钥？（D）

A、Diffe-Hellman　　B、DES　　C、IDEA　　D、RSA

495、以下认证方式中，最为安全的是（D）。

A、用户名+密码　　B、卡+密码　　C、用户名+密码+验证码　　D、卡+指纹

496、远程访问控制机制是基于一次性口令（one-time password），这种认证方式采用下面哪种认证技术？（B）

A、知道什么　　B、拥有什么　　C、是谁　　D、双因素认证

497、在 3DES 算法中，密钥最高可达到多少位？（C）

A、96　　B、128　　C、168　　D、200

498、在 IPSec 中，（C）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的 IPSec 协议、密码算法、密钥等信息。

A、ESP　　B、SPI　　C、SA　　D、SP

499、在 IPSec 中，IKE 提供（B）方法供两台计算机建立。

A、解释域　　B、安全关联　　C、安全关系　　D、选择关系

500、在 RIP 的 MD5 认证报文中，经过加密的密钥是放在哪里的？（B）

A、保温的第一个表项里　　B、报文的最后一个表项里

C、报文的第二个表项里　　D、报文头里

501、在非对称加密算法中，涉及到的密钥个数是？（B）

A、一个　　B、两个　　C、三个　　D、三个以上

502、在高级加密标准 AES 算法中，区块大小为（A）。

A、128 位　　B、192 位　　C、256 位　　D、512 位

503、在给定的密钥体制中，密钥与密码算法可以看成是（A）。

A、前者是可变的，后者是固定的　　B、前者是固定的，后者是可变的

C、两者都是可变的　　D、两者都是固定的

504、在公钥体制中，不公开的是（B）。

A、公钥　　B、私钥　　C、公钥和私钥　　D、私钥和加密算法

505、在密码学中，需要被交换的原消息被称为什么？（D）

A、密文　　B、算法　　C、密码　　D、明文

506、一般证书采用哪个标准？（D）

A、ISO/IEC 15408　　B、ISO/IEC 17799　　C、BS　7799　　D、X. 509V3

507、一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（D）

A、信息的数据和时间戳　　B、识别发信的计算机

C、对信息内容进行加密　　D、对发送者的身份进行识别

508、在数据库中，下列哪些数据不能加密？（A）

A、索引字段　　B、存放日期字段

C、存放密码的　　D、存放名称字段

509、在一个网络节点中，链路加密仅在以下哪项中提供安全性？（D）

A、数据链路层　　B、物理层

C、通信层　　D、通信链路

510、在以下隧道协议中，属于三层隧道协议的是（D）。

A、L2F　　B、PPTP　　C、L2TP　　D、IPSec

511、以下哪一项是基于一个大的整数很难分解成两个素数因数？（B）

A、ECC　　B、RSA　　C、DES　　D、D-H

512、以下哪种数据加密技术可以在基础架构层面进行？（A）

A、IPSec　　B、Secure Sockets Layer

C、Transport Layer Securit　　D、RSA

513、目前最安全的身份认证机制是（A）。

A、一次口令机制　　B、双因素法

C、基于智能卡的用户身价认证　　D、身价认证的单因素法

514、当数据库由于各种原因而使其完整性遭到破坏时，必须采取以下哪项措施来恢复数据库？（C）

A、重新安装数据库　　B、换一种数据库

C、使用数据库备份　　D、将数据库中的数据利用工具导出，并保存

515、PGP 加密算法是混合使用（B）算法和 IDEA 算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES　　B、RSA　　C、IDEA　　D、AES

516、以下哪些软件是用于加密的软件？（A）

A、PGP　　B、SHA　　C、EFS　　D、DES

517、如果消息接受方要确定发送方身价，则要使用（B）原则。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

518、对于现代密码破解，（D）是最常的方法。

A、攻破算法　　B、监听截获　　C、信息猜测　　D、暴力破解

519、非对称密码技术的缺点有哪些？（B）

A、密钥持有量减少　　B、加/解密速度慢　　C、耗用资源较少　　D、以上都是

520、CA 不能提供下列哪种证书？（D）

A、个人数字证书　　B、SSL 服务器证书

C、安全电子邮件证书　　D、SET 服务器证书

521、以下关于混合加密方式说法正确的是（B）。

A、采用公开密钥体制进行通信过程中的加解密处理

B、采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C、采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D、采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密

处理速度快的双重优点

522.、果要保证（C）原则，则不能在中途修改消息内容。

A、保密性　　B、鉴别　　C、完整性　　D、访问控制

523、口令是验证用户身份的最常用手段，以下哪一种口令的潜在风险影响范围最大？（D）

A、长期没有修改的口令　　B、过短的口令

C、两个人共用的口令　　D、设备供应商提供的默认的口令

524.非对称密钥的密码技术具有很多优点，其中不包括：（B）。

A、可提供数字签名、零知识证明等额外服务

B、加密/解密速度快，不需占用较多资源

C、通信双方事先不需要通过保密信道交换密钥

D、密钥持有量大大减少

525．DES 是一种 block（块）密文的加密算法，是把数据加密成多大的块？（B）

A、32 位　　B、64 位　　C、128 位　　D、256 位

526．CA 数字证书中不包含的信息有（C）。

A、CA 的数字签名　　B、证书申请者的个人信息

C、证书申请者的私钥　　D、证书申请者的公钥信息

527．以下关于对称密钥加密说法正确的是（C）。

A、加密方和解密可以使用不同的算法　　B、加密密钥和解密密钥可以是不同的

C、加密密钥和解密密钥必须是相同的　　D、密钥的管理非常简单

528、在为计算机设置使用密码时，下面（D）密码是最安全的。

A、12345678　　B、66666666

C、20061001　　D、72aB@#41

529、（C）的攻击者发生在 Web 应用层？

A、25%　　B、50%

C、75%　　D、90%

530、“U 盘破坏者”病毒（Worm.vhy）采用（B）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。

A、网上邻居　　B、我的电脑

C、我的文档　　D、收藏夹

531、“冲击波”病毒运行时会将自身复制到 Windows 目录下，并命名为（C）

A、Gsrss.exe　　B、msbast.exe

C、msblast.exe　　D、lsass.exe

532、Code Red 爆发于 2001 年 7 月，利用微软的 IIS 漏洞在 Web 服务器之间传播。针对这一漏洞，微软早在 2001 年三月就发布了相关的补丁。如果今天服务器仍然感染 Code Red，那么属于哪个阶段的问题？（A）

A、系统管理员维护阶段的失误　　B、微软公司软件的设计阶段的失误

C、最终用户使用阶段的失误　　D、微软公司软件的实现阶段的失误

533、病毒的传播机制主要有哪些？（D）

A、移动存储　　B、电子邮件　　C、网络共享　　D、以上均是

534、病毒的反静态反汇编技术都有（D）。

A、数据压缩　　B、数据加密　　C、感染代码　　D、以上均是

535、病毒在感染计算机系统时，一般（B）感染系统的。

A、病毒程序都会在屏幕上提示，待操作者确认（允许）后

B、实在操作者不觉察的情况下

C、病毒程序会要求操作者制定存储的磁盘和文件夹后

D、在操作者为病毒制定存储的文件名以后

536、杀毒软件时提示“重新启动计算机后删除文件”其主要原因是（A）

A、文件插入了系统关键进程，杀毒时无法处理

B、文件是病毒文件，无法处理

C、由于病毒的加壳形式不同，杀毒时无法正确处理

D、文件正在运行且无法安全的结束，需要其他处理方法

537、蠕虫的目标选择算法有（D）。

A、随机性扫描　　B、基于目标列表的扫描

C、顺序扫描　　D、以上均是

538、网络钓鱼是指（A）

A、通过大量发送声来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息。

B、网上进行钓鱼活动

C、通过网络组织钓鱼活动，从而获得利益　　D、以上都不是

539、不属于常见把入侵主机的信息发送给攻击者的方法是（D）。

A、E-MAIL　　B、UDP　　C、ICMP　　D、连接入侵主机

540、不属于黑客被动攻击的是（A）

A、缓冲区溢出　　B、运行恶意软件　　C、浏览恶意代码网页　　D、打开病毒附件

541、不属于黑客前期收集信息的工具是（D）

A、Nmap　　B、Xscan　　C、Nslookup　　D、LC

542、常见 Web 攻击方法，不包括？（D）

A、利用服务器配置漏洞　　B、恶意代码上传下载

C、构造恶意输入（SQL 注入攻击、命令注入攻击、跨站脚本攻击）

D、业务测试

543、常用的抓包软件有（A）。

A、ethereal　　B、MS office　　C、fluxay　　D、netscan

544.网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（A）

A、密码加密后，不会被窃听　　B、Cookie 字段可以被窃听

C、报文和帧可以窃听　　D、高级窃听者还可以进行 ARPSpoof，中间人攻击

545、除了在代码设计开发阶段预防 SQL 注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（C）

A、禁止将任何高权限账号（例如 sa,dba 等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户

B、拒绝用户访问敏感的系统存储过程

C、禁止用户访问的数据库表　　D、限制用户所能够访问的数据库表

546、防止用户被冒名所欺骗的方法是（A）。

A、对信息源发放进行身份验证　　B、进行数据加密

C、对访问网络的流量进行过滤和保护　　D、采用防火墙

547、给电脑设置多道口令，其中进入电脑的第一道口令是（B）。

A、系统口令　　B、CMOS 口令

C、文件夹口令　　D、文档密码

548、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（D）。

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

549、故意制作、传播计算机病毒，造成计算机信息系统不能正常运行，但如果后果不严重就无罪，可以原谅，这种说法（C）。

A、不对，对这种蓄意破坏行为不能原谅　　B、即使不是故意的，后果也不很严重

C、对。我国实行成文法，根据《中华人民共和国刑法》第 286 条的规定，只有造成严重后果者才有罪

D、无法断定

550、关于 80 年代 Mirros 蠕虫危害的描述，哪句话是错误的？（B）

A、占用了大量的计算机处理器的时间，导致拒绝股务

B、窃取用户的机密信息，破坏计算机数据文件

C、该蠕虫利用 Unix 系统上的漏洞传播

D、大量的流量堵塞了网络，导致网络瘫痪

551、关于黑客注入攻击说法错误的是： (D)

A、它的主要原因是程序对用户的输入缺乏过滤

B、一般情况下防火墙对它无法防范

C、对它进行防范时要关注操作系统的版本和安全补丁

D、注入成功后可以获取部分权限

552、基于主机评估报告对主机进行加固时，第一步是（B）。

A、账号、口令策略修改　　B、补丁安装

C、文件系统加固　　D、日志审核增强

553、计算机病毒会对下列计算机服务造成威胁，除了（C）。

A、完整性　　B、有效性

C、保密性　　D、可用性

554、计算机病毒是一段可运行的程序，它一般（C）保存在磁盘中。

A、作为一个文件　　B、作为一段数据

C、不作为单独文件　　D、作为一段资料

555、什么方式能够从远程绕过防火墙去入侵一个网络？(D)

A、IP services_　　B、Active　ports

C、Identified network topology　　D、Modem banks

556、输入法漏洞通过（D）端口实现的。

A、21　　B、23　　C、445　　D、3389

557、特洛伊木马攻击的威胁类型属于（B）。

A、授权侵犯威胁　　B、植入威胁

C、渗入威胁　　D、旁路控制威胁

558、通常黑客扫描目标机的 445 端口是为了(B)。

A、利用 NETBIOS SMB 服务发起 DOS 攻击

B、发现并获得目标机上的文件及打印机共享

C、利用 SMB 服务确认 Windows 系统版本

D、利用 NETBIOS 服务确认 Windows 系统版本

559、网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？(A)

A、残余风险评估阶段　　B、检查阶段

C、入侵检测系统监控阶段　　D、网络异常流量临控阶段

560、网络病毒预防范阶段的主要措施是什么？(A)

A、强制补丁、网络异常流量的发现　　B、强制补丁、入侵检测系统监控

C、网络异常流量的发现、入侵检测系统的监控阶段　　D、缺少 D 选项

561、下列除了(B)以外，都是防范计算机病毒侵害的有效方法。

A、使用防病毒软件　　B、机房保持卫生，经常进行消毒

C、避免外来的磁盘接触系统　　D、网络使用防病毒网关设备

562、下列除了(A)以外，都是计算机病毒传

A、通过操作员接触传播　　B、通过 U 盘接触传播

C、通过网络传播　　D、通过电子播的途径邮件传播

563、下列措施中，(C)不是减少病毒的传染

和造成的损失的好办法。

A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B、外来的文件要经过病毒检测才能使用，不要使用盗版软件

C、不与外界进行任何交流，所有软件都自行开发

D、定期用抗病毒软件对系统进行查毒、杀毒

564、下列哪项是跨站脚本 Cross Site Scripting 攻击具体事例？（B）

A、搜索用户　　B、发帖子，发消息　　C、上传附件　　D、下载文件

565、下列哪项为信息泄露与错误处理不当 Information Leakage and Improper

Error Handlina 攻击具体实例？(D)

A、不明邮件中隐藏的 html 链接　　B、发帖子，发消息

C、上传附件　　D、错误信息揭示路径

566、下面哪一项是黑客用来实施 DDoS 攻击的工具？(D)

A、LC5　　B、Rootkit　　C、Icesword　　D、Trinoo

567、以下哪个工具可以抹去所有 NT/2K 配置，并将其还原到初始状态？(A)

A、Rollback. exe　　B、Recover. exe　　C、Zap. exe　　D、Reset. exe

568、以下哪个工具通常是系统自带任务管理器的替代？(D)

A、Regmon　　B、Filemon　　C、Autoruns　　D、Process explorer

569、以下哪个针对访问控制的安全措施是最容易使用和管理的？(C)

A、密码　　B、加密标志　　C、硬件加密　　D、加密数据文件

570、以下哪项不是分布式拒绝服务攻击常用的工具？(D)

A、Trinoo　　B、Trinoo　　C、TFN　　D、synkill

571、以下哪项不属于针对数据库的攻击？(D)

A、特权提升　　B、强力破解弱口令或默认的用户名及口令

C、SQL 注入　　D、利用 xss 漏洞攻击

572、以下哪项工具不适合用来做网络监听？(B)

A、sniffer　　B、Webscan　　C、 Windump　　D、 D-Iris

573、以下哪项是 SYN 变种攻击经常用到的工具？(B)

A、sessionIE　　B、synkill　　C、TFN　　D、Webscan

574、以下哪一项不是流氓软件的特征？(D)

A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装

B、通常添加驱动保护使用户难以卸载

C、通常会启动无用的程序浪费计算机的资源

D、通常会显示下流的言论

575、一个数据仓库中发生了安全性破坏。以下哪一项有助于安全调查的进行？(B)

A、访问路径　　B、时戳　　C、数据定义　　D、数据分类

576、以下哪一项不属于恶意代码？(C)

A、病毒　　B、蠕虫　　C、宏　　D、特洛伊木马

577、以下哪一项不属于计算机病毒的防治策略？(D)

A、防毒能力　　B、查毒能力　　C、杀毒能力　　D、禁毒能力

578、以下哪一项是常见 Web 站点脆弱性扫描工具？(A)

A、Appscan　　B、Nmap　　C、Sniffer　　D、LC

579、以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？(A)

A、用所有者的公钥对硬盘进行加密处理　　B、激活引导口令（硬件设置口令）

C、利用生物识别设备　　D、利用双因子识别技术将臀陆信息写入记事本

580、以下哪种符号在 SQL 注入攻击中经常用到？(D)

A、$_　　B、1　　C、@　　D、;

581、以下哪种工具能从网络上检测出网络监听软件(A)

A、sniffdet, ,　　B、purify, ,　　C、Dsniff　　D、WireShark

582、以下哪种攻击可能导致某些系统在重组 IP 分片的过程中宕机或者重新启动？(B)

A、分布式拒绝服务攻击　　B、Ping of Death

C、NFS 攻击　　D、DNS 缓存毒化攻击

583、下面哪部分不属于入侵的过程？(B)

A、数据采集　　B、数据存储　　C、数据检测　　D、数据分析

584、以下对木马阐述不正确的是(A)。

A、木马可以自我复制和传播

B、有些木马可以查看目标主机的屏幕

C、有些木马可以对目标主机上的文件进行任意揉作

D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。

585、由于攻击者可以借助某种手段，避开 DBMS 以及应用程序而直接进入系统访问数据，我们通常采取以下哪种方式来防范？(A)

A、数据库加密

B、修改数据库用户的密码，将之改得更为复杂

C、使用修改查询法，使用户在查询数据库时需要满足更多的条件

D、使用集合法

586、在大多数情况下，病毒侵入计算机系统以后，(D)。

A、病毒程序将立即破坏整个计算机软件系统

B、计算机系统将立即不能执行我们的各项任务

C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

587、在确定威胁的可能性时，可以不考虑以下哪项？(D)

A、威胁源　　B、潜在弱点

C、现有控制措施　　D、攻击所产生的负面影响

588、在以下人为的恶意攻击行为中，属于主动攻击的是(A)。

A、身份假冒　　B、数据 GG　　C、数据流分析　　D、非法访问

589、下面哪一种攻击方式最常用于破解口 令？(B)

A、哄骗(spoofing)　　B、字典攻击(dictionary attack)

C、拒绝服务(DoS)　　D、WinNuk

590、针对 DNS 服务器发起的查询 DoS 攻击，属于下列哪种攻击类型？(C)

A、syn flood　　B、ack flood　　C、 udpflood　　D、Connection flood

591、下列哪项不是安全编码中输入验证的控制项？(D)

A、数字型的输入必须是合法的数字

B、字符型的输入中对’进行特殊处理

C、验证所有的输入点，包括 Get，Post，Cookie 以及其他 HTTP 头

D、正确使用静态查询语句，如 PreDaredStatement

592、以下关于垃圾邮件泛滥原因的描述中，哪些是错误的？(C)

A、早期的 SMTP 协议没有发件人认证的功能

B、网络上存在大量开放式的邮件中转服务器，导致垃圾邮件的来源难于追查

C、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

D、Internet 分布式管理的性质，导致很难控制和管理

593、以下哪种方法是防止便携式计算机机密信息泄露的最有效方法？（A）

A、用所有者的公钥对硬盘进行加密处理　　B、激活引导口令（硬件设置口令）

C、利用生物识别设备　　D、利用双因子识别技术将登录信息写入记事本

594、以下哪种攻击属于 DDoS 类攻击？（A）

A、SYN 变种攻击　　B、smurf 攻击　　C、arp 攻击　　D、Fraggle 攻击

595、URL 访问控制不当不包括（D）

A、Web 应用对页面权限控制不严　　B、缺乏统一规范的权限控制框架

C、部分页面可以直接从 URL 中访问　　D、使用分散登录认证

596、Web 应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（A）

A、静态密码　　B、短信挑战　　C、指纹认证　　D、图片认证

597、Web 应用漏洞按类别进行排名，由多到少正确的顺序为？（A）

A、跨站脚本、注入、恶意代码、引用不当

B、注入、跨站脚本、恶意代码、引用不当

C、恶意代码、跨站脚本、注入、引用不当

D、引用不当、跨站脚本、注入、恶意代码

598、从技术角度，以下不是漏洞来源的是（D）

A、软件或协议设计时候的瑕疵　　B、软件或协议实现中的弱点

C、软件本身的瑕疵　　D、显示卡内存容量过低

599、（C）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A、身份假冒　　B、数据篡改　　C、信息窃取　　D、越权访问

600、有关密码学分支的定义，下列说法中错误的是（D）

A、密码学是研究信息系统安全保密的科学，由两个相互对立、相互斗争、而且又相辅

相成、相互渗透的分支科学所组成的、分别称为密码编码学和密码分析学

B、密码编码学是对密码体制、密码体制的输入输出关系进行分析、以便推出机密变量、包括明文在内的敏感数据

C、密码分析学主要研究加密信息的破译或信息的伪造

D、密码编码学主要研究对信息进行编码，实现信息的隐藏

601、与 RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（C）

A、数字签名　　B、鉴别机制　　C、加密机制　　D、数据完整性

602、以下哪项是数据库加密方法中的库外加密的缺点？（A）

A、即使访问一条数据也要对整个数据库解密　　B、密钥管理比较复杂

C、加密之后不能完整的查询数据　　D、密钥过于简单，容易被破解

603、以下哪项数据中涉及安全保密的最主要问题？（A）

A、访问控制问题　　B、数据完整性　　C、数据正确性　　D、数据安全性

604、以下哪一个最好的描述了数字证书？（A）

A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，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

605、TCP SYN Flood 网络攻击时利用了 TCP 建立连接过程需要（C）次握手的特点而完成对目标进行攻击的。

A、1　　B、2　　C、3　　D、6

二、多项选择题（606-789）

606、COBIT 度量过程的三个纬度分别是（ABC）。

A、能力　　B、绩效　　C、控制度　　D、能力成熟度

607、IT 系统内网与互联网连接检查手段有哪些？（BCD）

A、工具扫描　　B、人员访谈　　C、人工检查　　D、文档检查

608、公司应该采取以下措施，对第三方访问进行控制。（ABCD）

A、公司应于第三发公司法人签署保密协议，并要求其第三方个人签署保密承诺，此项工作应在第三方获得网络与信息资产的访问权限之前完成

B、实行访问授权管理，未经授权，第三方不得进行任何形式的访问

C、公司应加强第三方访问的过程控制，监督其活动及操作，对其进行适当的安全宣传与培训

D、第三方人员应佩戴易于识别的标志，并在访问公司重要场所时有专人陪同

609、计算机信息系统安全的三个相辅相成，互补互通的有机组成部分是（ABD）

A、安全策略　　B、安全法规　　C、安全技术　　D、安全管理

610、劳动合同中应包含网络与信息安全条款，这些条款规定（ACD）。

A、员工的安全责任和违约罚则

B、安全责任不可延伸至公司场所以外和正常工作时间以外

C、安全责任可延伸至公司场所以外和正常工作时间以外

D、如必要，一些安全责任应在雇佣结束后延续一段特定的时间

611、审核是网络安全工作的核心，下列应用属于主动审核的是：（CD）

A、Windows 事件日志记录　　B、数据库的事务日志记录

C、防火墙对访问站点的过滤　　D、系统对非法链接的拒绝

612、通用准则 CC 实现的目标有（ABC）

A、成为统一的国际通用安全产品、系统的安全标准

B、在不同国家达成协议，相互承认产品安全等级评估

C、概述 IT 产品的国际通用性　　D、都不是

613、系统用户账号登记表应包括（ABCD）。

A、使用者姓名、部门、职务、联系电话　　B、账号权限

C、批准人、开通人　　D、开通时间、到期日

614、下列情况哪些是对公司经营管理的影响为“一般”级别的互联网网络安全事件？（ABD）

A、发生未到达“预警”的一般性安全事件

B、出现新的漏洞，尚未发现利用方法或利用迹象

C、有来自境外的网络性能明显下降的报警，并且其技术原因普遍适用于我国互联网

D、出现新的蠕虫/病毒或其它恶意代码，尚未证明可能造成严重危害

615、信息安全的主要原则有（BCD）

A、认证性　　B、保密性　　C、可用性　　D、完整性

616、针对支撑系统，除业务关联性、对业务网络的影响，资产价值主要体现在（ACD）几个方面。　　缺少 D 选项

A、业务收益的影响　　B、设备购买成本　　C、面向客户的重要程度　　D、

617、IT 系统病毒泛滥的主要原因有哪些？（ABCD）

A、主机和终端防病毒软件缺乏统一管理

B、主机和终端防病毒软件没有设置为自动更新或更新周期较长

C、防病毒服务器没有及时更新放病毒库

D、缺乏防病毒应急处理流程和方案

618、IT 系统病毒防护评估检查对象包括哪些内容？（ABCD）

A、防病毒服务器　　B、重要应用 Windows 主机

C、Windows 终端　　D、主机管理员

619、互联网连接防火墙设备的安全策略配置要求包括哪几点（ABCD）。

A、远程登录是否禁止 telnet 方式　　B、最后一条策略是否是拒绝一切流量

C、是否存在允许 any to any 的策略

D、是否设置了管理 IP，设备只能从管理 IP 登录维护

620、《安全基线标准》在安全管理层面主要围绕哪几部分考评安全基线？（ABC）

A、组织架构管理　　B、人员安全管理　　C、运维安全管理　　D、制度安全管理

621、IT 系统维护人员权限原则包括（ACD）。

A、工作相关　　B、最大授权　　C、最小授权　　D、权限制约

622、安全系统加固手册中关于造成系统异常中断的各方面因素，主要包括哪三方面（ABD）

A、人为原因　　B、环境原因　　C、生产原因　　D、设备原因

623、IT 系统维护人员权限原则包括（ACD）

A、工作相关　　B、最大授权　　C、最小授权　　D、权限制约

624、计算当前 Linux 系统中所有用户的数量，可以使用（ABC）命令

A、wc -l /etc/passwd　　B、wc -l</etc/passwd

C、cat/etc/passwd|wc -l　　D、cat/etc/passwd>wc -l

625、Solarid 系统中，攻击者在系统中增加账户会改变哪些文件？（AB）

A、shadow　　B、passwd　　C、inetd,conf　　D、hosts

626、Syn Flood 攻击的现象有以下哪些？（ABC）

A、大量连接处于 SYN_RCVD 状态　　B、正常网络访问受阻

C、系统资源使用率高

627、UNIX 安全审计的主要技术手段有哪些？（ABCDEF）

A、文件完整性审计　　B、用户、弱口令审计　　C、安全补丁审计

D、端口审计　　E、进程审计　　F、系统日志审计

628、Unix 系统提供备份工具有（ABCD）

A、cp：可以完成把某一目录内容拷贝到另一目录

B、tar：可以创建、把文件添加到或从一个 tar 档案中解开文件

C、cpio：把文件拷贝进或拷贝出一个 cpio 档案或 tar 档案

D、dump：用来恢复整个文件系统或提取单个文件

629、操作系统应利用安全工具提供以下哪些访问控制功能？（ABC）

A、验证用户身份，必要的话，还应进行终端或物理地点识别

B、记录所有系统访问日志

C、必要时，应能限制用户连接时间　　D、都不对

630、从哪些地方可以看到遗留痕迹？（ABCD）

A、回收站　B、最近使用过的文件　C、注册表　D、文件最后更改的时间戳 631、

632、关于 Windows 活动目录说法正确的是（ABD）。

A、活动目录是采用分层结构来存储网络对象信息的一种网络管理体系

B、活动目录可以提供存储目录数据和网络用户级管理员使用这些数据的方法

C、利用活动目录来实现域内计算机的分布式管理

D、活动目录与域紧密结合构成与目录林和域目录树，使大型网络中庞大、复杂的网络管理、控制、访问变得简单，使网络管理效率更高

633、建立堡垒主机的一般原则是（AC）。

A、最简化原则　B、复杂化原则　C、预防原则　D、网络隔离原则

634、逻辑空间主要包括哪些部分？（ABDE）

A、TABLESPACES　　B、SEGMENTS　　C、DATAFILE

D、EXTENTS　　E、BLOCK

635、哪些属于 Windows 日志？（ABCD）

A、AppEvent.Evt　B、SecEvent.Evt　C、SysEvent.Evt　D、W3C 扩展日志

636、如何设置 listener 口令？（ACDE）

A、以 Oracle 用户运行 lsnrctl 命令　　B、set log_file

C、change_password　　D、set password　　E、save_config

637、审计启动其日志有哪两种存放方式？（BD）

A、NONE　　B、OS　　C、TRUE　　D、SYS.AUD$

638、生产服务器通常都是 UNIX 平台，资产价值最高，不直接连接外部网络，主要的安全需求是（ABD）

A、访问控制　　B、账号口令　　C、数据过滤　　D、权限管理和补丁管理

639、使用 md5sum 工具对文件签名，以下说法正确的是？（ADE）

A、md5sum 对任何签名结果是定长的 16 字节

B、md5sum 对文件签名具有不可抵赖性

C、md5sum 是对文件进行加密运算得出签名，不同文件结果几乎不相同

D、md5sum 是对文件进行哈希运算得出签名，不同文件结果几乎不相同

E、md5sum 对文件签名时，与文件的日期和时间无关

640、为了正确获得口令并对其进行妥善保护，应认真考虑的原则和方法有（ABCD）

A、口令/账号加密　　B、定期更换口令

C、限制对口令文件的访问　　D、设置复杂的、具有一定位数的口令

641、文件系统是构成 Linux 基础，Linux 中常用文件系统有（ABD）？

A、ext3　　B、ext2　　C、hfs　　D、reiserfs

642、下列关于 UNIX 下日志说法正确的是（AC）

A、wtmp 记录每一次用户登录和注销的历史信息

B、acct 记录每个用户使用过的命令

C、sulog 记录 su 命令的使用情况

D、acct 记录当前登录的每个用户

643、下列哪些操作可以看到自启动项目？（ABD）

A、注册表　　B、开始菜单　　C、任务管理器　　D、msconfig

644、下列哪些命令行可用于查看当前进程？（ABC）

A、Ps -ef　　B、Strings -f/proc/[0-9]*/cmdline

C、Ls -al /proc/[0-9]*/exe　　D、Cat/etc/inetd.conf

645、下面操作系统中，哪些是 UNIX 操作系统？（CD）

A、Red-hat Linux　　B、Novell Netware　　C、Free BSD　　D、SCO Unix

646、严格的口令策略应当包含哪些要素（ABC）

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

647、在 Solaris 8 下，使用 ps -ef 命令列出进程中有一行如下“root 1331 0 00:01:00?　　0:00

/usr/sbin/inetd -s -t”，以下说法正确的是（ABE）

A、参数-t 是 trace，记录包括 IP 和 PORT 等信息

B、参数-t 对于 UDP 服务无效　　C、进程启动的时间不能确定

D、进程已经运行了 1 分钟　　E、进程的父进程号是 1

648、在 Solaris 8 下，以下说法正确的是：（AB）

A、/etc/rc2.d 里 S 开头的文件在系统缺省安装的缺省级别会自动运行

B、/etc/rc3.d 里 S 开头的文件在系统缺省安装的缺省级别会自动运行

C、/etc/init.d 里的文件在系统启动任何级别时会自动运行

D、init 0 是进入单用户级别　　E、init 6 命令会运行所有级别的 rc 目录下以 S 开头的文件

649、在 Solaris 8 下，以下说法正确的是：（BC）

A、PATH 环境变量最后带有“.”，会使当前目录的命令比其他目录的命令有限执行

B、可以修改/etc/inittab 里 ttymon 的参数，使得登录的 SHELL 在无输入时自动退出

C、在使用/bin/ksh 时，可以设置 TMOUT 值，使得登录的 SHELL 在无输入时自动退出

D、在/etc/login 中，可以设置 TIMEOUT 值，使得登录的 SHELL 在无输入时自动退出

E、tar xvf 命令的意思是以 tar 格式解开输入，并且保持文件属性等参数不变

650、在配置 Apache 访问控制时，Allow 和 Deny 指令可以允许或拒绝来自特定主机名或主机名地址的访问。那么下列哪些配置是不正确的？（AD）

A、Order allow,deny Allow from 192.101.205

B、B、Order deny,allow Deny from all Allow from example

C、C、Order deny,allow Deny from 192.101.205

D、D、Order allow,deny Deny from 192.101.205 Allow from all

651、造成操作系统安全漏洞的原因是（ABC）。

A、不安全的编程语言　　B、不安全的编程习惯

C、考虑不周的架构设计　　D、人为的恶意破坏

652、针对 Linux 主机，一般的加固手段包括（ABC）。

A、打补丁　　B、关闭不必要的服务　　C、限制访问主机　　D、切断网络

653、做系统快照，查看端口信息的方式有（AD）。

A、netstat -an　　B、net share　　C、net use　　D、用 taskinfo 来查看连接情况

654、网厅安全解决方案主要从哪几个方面对网厅安全进行建议和指导？（ABCD）

A、安全管理　　B、安全防护　　C、安全运维　　D、灾备/恢复

655、IT 系统软件设计中应当考虑并执行安全审计功能，详细记录访问信息的活动，包括（ABCD）。

A、记录的活动以是否有数据的修改、应用程序的异常关闭、异常删除触发

B、应用系统应当配置单独的审计数据库，审计记录应单独存放，并设置严格的边界访问控制，只有安全管理人员才能够看到审计记录

C、信息系统的审计功能包括：事件日期、时间、发起者信息、类型、描述和结果

D、应用系统的审计进程为后台处理，与应用系统运行同步进行，并且对于审计进程应当涉及相应的守护进程，一旦出现异常停止系统可重新启动审计进程，从而保障审计的“完整性”

656、IPSec 的配置步骤包括：（ABCD）

A、防火墙基本配置　　B、定义保护数据流和域间规则

C、配置 IPSec 安全提议　　D、配置 IKEPeer

657、Juniper 路由器在配置 SSH 访问时应注意如下（ABCD）细节。

A、建立允许访问的 SSH-ADDRESSES 过滤器

B、确保只允许来自内部接口的授权用户访问

C、针对 SSH 进行限速以保护路由引擎

D、过滤器应用在 loopback 接口

658、对于使用 RPF 反向地址验证，以下说法错误的是：（BCD）。

A、对称路由可以使用　　B、非对称路由可以使用

C、有些情况不可以使用，但与对称或非对称路由无关

D、在任何情况下都可以使用

659、防病毒服务升级检查包括如下几项内容？（ABC）

A、检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决

B、在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本

C、对重要的服务器，定期抽查防病毒客户端的病毒库升级情况

660、防范 DOS 攻击的方法主要有（ABCD）。

A、安装 Dos 检测系统　　B、对黑洞路由表里的地址进行过滤

C、及时打好补丁　　D、正确配置 TCP/IP 参数

661、防火墙 trust 域中的客户机通过 nat 访问 untrust 中的服务器的 ftp 服务，已经允许客户

机访问服务器的 tcp21 端口，但只能登陆到服务器，却无法下载文件，以下解决办法中可能的是：（ABC）

A、修改 trust untrust 域间双向的默认访问策略为允许

B、FTP 工作方式为 port 模式时，修改 untrust trust 域间 in 方向的默认访问策略为允许

C、在 trust untrust 域间配置中启用 detect ftp

D、FTP 工作方式为 passive 模式时，修改 untrust trust 域间 in 方向的默认访问策略为允许

662、防火墙不能防止以下哪些攻击？（ABD）

A、内部网络用户的攻击　　B、传送已感染病毒的软件和文件

C、外部网络用户的 IP 地址欺骗　　D、数据驱动型的攻击

663、防火墙常见的集中工作模式有（ABC）。

A、路由　　B、NAT　　C、透明　　D、旁路

664、防火墙的缺陷主要有（ABCD）。

A、限制有用的网络服务　　B、无法防护内部网络用户的攻击

C、不能防备新的网络安全问题　　D、不能完全防止传送已感染病毒的软件或文件

665、防火墙的日志管理应遵循如下原则：（BC）

A、本地保存日志　　B、本地保存日志并把日志保存到日志服务器上

C、保持时钟的同步　　D、在日志服务器保存日志

666、防火墙的特征是（ABCD）。

A、保护脆弱和有缺陷的网络服务　　B、加强对网络系统的访问控制

C、加强隐私，隐藏内部网络结构　　D、对网络存取和访问进行监控审计

667、防火墙的主要功能有哪些？（ABCD）

A、过滤进、出网络的数据　　B、管理进、出网络的访问行为

C、封堵某些禁止的业务，对网络攻击进行检测和报警

D、记录通过防火墙的信息内容和活动

668、防火墙的作用主要有（ABCD）。

A、实现一个公司的安全策略　　B、创建一个阻塞点

C、记录 Internet 活动　　D、限制网络暴露

669、防火墙技术，涉及到（ABCD）。

A、计算机网络技术　　B、密码技术　　C、软件技术　　D、安全操作系统

670、防火墙可以部署在下列位置：（ABCD）。

A、安全域边界　　B、服务器区域边界

C、可信网络区域和不可信网络区域之间　　D、根据网络特点设计方案

671、防火墙配置时应确保（ABCD）服务不开放。

A、Rlogin　　B、NNTP　　C、Finger　　D、NFS

672、启用 Cisco 设备的访问控制列表，可以起到如下作用（ABC）。

A、过滤恶意和垃圾路由信息　　B、控制网络的垃圾信息流

C、控制未授权的远程访问　　D、防止 DDoS 攻击

673、如果 Cisco 设备的 VTY 需要远程访问，则需要配置（ABCD）。

A、至少 8 位含数字、大小写、特写字符的密码　　B、远程连接的并发数目

C、访问控制列表　　D、超市退出

674、如果需要配置 Cisco 路由器禁止从网络启动和自动从网络下载初始配置文件，配置命令包括（AB）。

A、no boot network　　B、no service config　　C、no boot config　　D、no service network

675、入侵检测的内容主要包括：（BC）。

A、独占资源、恶意使用　　B、试图闯入或成功闯入、冒充其他用户

C、安全审计　　D、违反安全策略、合法用户的泄露

676、入侵检测系统包括以下哪些类型？（AC）

A、主机入侵检测系统　　B、链路状态入侵检测系统

C、网络入侵检测系统　　D、数据包过滤入侵检测系统

677、随着交换机的大量使用，基于网络的入侵检测系统面临着无法接收数据的问题。由于交换机不支持共享媒质的模式，传统的采用一个嗅探器（sniffer）来监听整个子网的办法不再可行。可选择解决的办法有（ABCD）。

A、使用交换机的核心芯片上的一个调试的端口

B、把入侵检测系统放在交换机内部或防火墙等数据流的关键入口

C、采用分解器（tap）

D、使用以透明网桥模式接入的入侵检测系统

678、通常要求把路由器的日志存储在专用日志服务器上，假设把 Cisco 路由器日志存储在 192.168.0.100 的 syslog 服务器上，需要在路由器侧配置的操作时：（ABCD）。

A、使用 Router(config)# logging on 启用日志：使用 Router(config)# logging trap information 将记录日志级别设定为“information”

B、使用 Routee(config)# logging192.168.0.100 将记录日志类型设定为“local6”

C、使用(config)# logging facility local6 将日志发送到 192.168.0.100

D、使用(config)# logging sourceinterface loopback0 设定日志发送源 loopback0

679、通过 SSL VPN 接入企业内部的应用，其优势体现在哪些方面：（ABCD）。

A、应用代理　　B、穿越 NAT 和防火墙设备

C、完善的资源访问控制　　D、抵御外部攻击

680、网络地址端口转换（NAPT）与普通地址转换有什么区别？（AD）

A、经过 NAPT 转换后，对于外网用户，所有报文都来自于同一个 IP 地址

B、NAT 只支持应用层的协议地址转换

C、NAPT 只支持网络层的协议地址转换

D、NAT 支持网络层的协议地址转换

681、网络攻击的类型包括以下哪几种？（ABCD）

A、窃取口令　　B、系统漏洞和后门　　C、协议缺陷　　D、拒绝服务

682、网络面临的典型威胁包括（ABCD）。

A、未经授权的访问　　B、信息在传送过程中被截获、篡改

C、黑客攻击　　D、滥用和误用

683、网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，该类病毒程序大规模爆发后，会对相关网络造成拒绝服务攻击，为了防止受到网络蠕虫的侵害，应当注意对（ACD）及时进行升级更新。

A、计算机操作系统　　B、计算机硬件　　C、文字处理软件　　D、应用软件

684、下列关于 NAT 地址转换的说法中哪些事正确的：（ABCD）。

A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

B、地址转换可以按照用户的需要，在局域网内向外提供 FTP、WWW、Telnet 等服务

C、有些应用层协议在数据中携带 IP 地址信息，对它们作 NAT 时还要修改上层数据中的 IP 地址信息

D、对于某些非 TCP、UDP 的协议（如 ICMP、PPTP），作上层 NAT 时，会对它们的特征参数（如 ICMP 的 id 参数）进行转换。

685、下列哪两项正确描述了由 WPA 定义的无线安全标准？（BC）

A、使用公开密钥的认证方法　　B、当客户端连接的时候都要进行动态密钥交换

C、包含 PSK 认证　　D、定制了一个经常更换的静态的加密密钥来增强安全性

686、下列配置中，可以增强无线 AP（access point）安全性的有（ABCD）。

A、禁止 SSID 广播　　B、禁用 DHCP 服务

C、采用 WPA2-PSK 加密认证　　D、启用 MAC 地址接入过滤

687、下面可以攻击状态检测的防火墙方法有：（ABD）

A、协议隧道攻击　　B、利用 FTP-pasv 绕过防火墙认证的攻击

C、ip 欺骗攻击　　D、反弹木马攻击

688、下面什么路由协议不可以为 HSRP 的扩充：（ABC）

A、SNMP　　B、CDP　　C、HTTP　　D、VRRP

689、下面什么协议有 MD5 认证：（ABC）

A、BGP　　B、OSPF　　C、EIGER　　D、RIPversion 1

690、下面是网络安全技术的有：（ABC）

A、防火墙　　B、防病毒　　C、PKI　　D、UPS

691、选购一个防火墙时应该考虑的因素有：（ABCD）

A、网络受威胁的程度　　B、可能受到的潜在损失

C、站点是否有经验丰富的管理员　　D、未来扩展的需要

692、一台路由器的安全快照需要保存如下哪些信息？（AB）

A、当前的配置--running-config　　B、当前的开放端口列表

C、当前的路由表　　D、当前的 CPU 状态

693、以下对于包过滤防火墙的描述正确的有（ACD）。

A、难以防范黑客攻击　　B、处理速度非常慢

C、不支持应用层协议　　D、不能处理新的安全威胁

694、以下对于代理防火墙的描述正确的有（ABCD）。

A、能够理解应用层上的协议　　B、时延较高，吞吐量低

C、能做复杂一些的访问控制，并做精细的认证和审核　　D、可伸缩性较差

695、以下关于 L2TP VPN 配置注意事项的说法中正确的有：（ABC）

A、L2TP 的 LNS 端必须配置虚拟接口模板（Virtual-Template）的 IP 地址，该虚拟接口模板需要加入域

B、防火墙缺省需要进行隧道的认证。如果不配置认证，需要 undo tunnel authentication 命令

C、为了使 L2TP 拨号上来的用户分配的地址不能喝内网用户的地址在同一个网段

D、LNS 端不允许配置多个 L2TP-Group

696、以下哪几项关于安全审计和安全审计系统的描述是正确的？（CD）

A、对入侵和攻击行为只能起到威慑作用

B、安全审计不能有助于提高系统的抗抵赖性

C、安全审计是对系统记录和活动的独立审查和检验

D、安全审计系统可提供侦破辅助和取证功能

697、以下哪些属于网络欺骗方式？（ABCD）

A、IP 欺骗　　B、ARP 欺骗　　C、DNS 欺骗　　D、Web 欺骗

698、以下哪些是防火墙规范管理需要的？（ABCD）

A、需要配置两个防火墙管理员　　B、物理访问防火墙必须严密地控制

C、系统软件、配置数据文件在更改后必须进行备份

D、通过厂商指导发布的硬件和软件的 bug 和防火墙软件升级版

699、以下硬件安装维护重要安全提示正确的有：（ABCD）

A、不要在雷雨天气进行故障处理　　B、保持故障处理区域的干净、干燥

C、上防静电手套或防静电腕带再执行安装和更换操作

D、在使用和操作设备时，需要按照正确的操作流程来操作

700、以下属于 DTE(Data Terminal Equipment)数据终端设备的有（AB）

A、路由器　　B、PC　　C、交换机　　D、HUB

701、在防火墙的“访问控制”应用中，内网、外网、DMZ 三者的访问关系为：（ABD）

A、内网可以访问外网　　B、内网可以访问 DMZ 区

C、DMZ 区可以访问内网　　D、外网可以访问 DMZ 区

702、关于 GRE 校验和验证技术，当本端配置了校验和而对端没有配置校验和时，以下叙述正确的有（BC）。

A、本端对接收报文检查校验和　　B、对端对接收报文检查校验和

C、本端对发送报文计算校验和　　D、对端对发送报文计算校验和

703、配置 PPP 链路层协议时，链路层协议状态始终不能转为 Up 状态的处理建议：（ABCD）

A、PPP 链路两端的接口上配置的参数和验证方式都必须一致，LCP 检查才能成功

B、如果 LCP 协商失败，请检查 LCP 配置协商参数

C、请检查验证方式配置是否正确。因为 LCP 协商中，包含验证方式的协商。因为 LCP 协商中，包含验证方式的协商。验证方式协商失败也会导致 LCP 协商失败

D、接口试图下先执行 shutdown 命令将接口关闭，再执行 undo shutdown 命令重启接口

704、对 DNSSEC 的描述正确的有（AC）。

A、为 DNS 数据提供来源验证，即保证数据来自正确的名称服务器

B、DNSSEC 可防御 DNS Query Flood 攻击

C、为域名数据提供完整性验证，即保证数据在传输的过程中没有被篡改

D、实施 DNSSEC 后，只需升级软件系统，对网络、服务器等硬件设备不需考虑

705、MySQL 安装程序会给出三种选择，用户可以根据自身的需要选择一种适合的安装方式，以下哪些是正确的？（ABD）

A、Typical（典型安装）　　B、Compact(最小安装)

C、Full(全部安装)　　D、Custom(选择安装)

706、MySQL 中用 DROP 语句可删除数据库和数据表，以下哪句是正确的语法？（ABCD）

A、DROP TABLE table_name1　　B、DROP TABLE table_name1,table_name2

C、DROP TABLE IF EXISTS table_name1　　D、DROP DATABASE DB name1

707、Oracle 7.2 之前的数据库连接用户名和密码在网络传输时是不进行加密的，为了要和旧版本兼容 Oracle 数据库 9.02 存在 DBLINK_ENCRYPT_LOGIN 参数用来调节数据库连接时用户名和密码的加密特性，以下说法正确的是：（ACD）。

A、DBLINK_ENCRYPT_LOGIN 为 TRUE 时，数据库连接加密用户名和密码

B、DBLINK_ENCRYPT_LOGIN 时，数据库连接不加密用户名和密码

C、DBLINK_ENCRYPT_LOGIN 为 FALSE 时，如果加密的数据库连接失败，会尝试不加密的连接

D、DBLINK_ENCRYPT_LOGIN 为 TRUE 时，加密的数据库连接失败，也不会尝试不加密的连接

708、Oracle 实例主要由哪两部分组成：（AC）

A、内存　　B、Share pool buffer　　C、后台进程　　D、pmon 和 smon

709、Oracle 中如何设置 audit trail 审计，正确的说法是：（ABD）

A、在 init.ora 文件中设置“audit_trail = true”或者“audit_trail = db”

B、以 SYSDBA 身份使用 AUDIT ALL ON SYS.AUD$ BY ACCESS，语句对 audit trail

审计

C、Oracle 不支持对 audit trail 的审计

D、在设置 audit trail 审计前，要保证已经打开 Oracle 的审计机制

710、SQL Server 的登录认证种类有以下哪些？（ACD）

A、Windows 认证模式　　B、双因子认证模式

C、混合认证模式　　D、SQL Server 认证

711、SQL Server 的取消权限的操作有以下哪些？（ABC）

A、在“详细信息”窗格中右击要授予/拒绝/取消其权限的用户定义的角色

B、单击“属性”命令在“名称”下单击“权限”单击列出全部对象

C、选择在每个对象上授予拒绝或废除的权限，选中标志表示授予权限，X 表示拒绝权限，空框表示废除权限，只列出适用于该对象的权限

D、回到“数据库用户属性”对话框中，再点击“确定”按钮，所有的设置就完成了

712、SQL Server 中 ALTER DATABASE 可以提供以下哪些功能选项？（ABCD）

A、更改数据库名称　B、文件组名称　C、数据文件　D、日志文件的逻辑名称

713、SQL Server 中关于实例的描述，请选择正确的答案。（ABD）

A、如果安装选择“默认”的实例名称。这时本 SQL Server 的名称将和 Windows 2000 服务器的名称相同

B、SQL Server 可以在同一台服务器上安装多个实例

C、SQL Server 只能在一台服务器上安装一个实例

D、实例各有一套不为其他实例共享的系统及用户数据库，所以各实例的运行是独立的。

714、SQL Server 中使用企业管理器从数据库中删除数据或日志文件的步骤如下，正确的步骤是？（ABCD）

A、展开服务器组，然后展开服务器

B、展开“数据库”文件夹，右击要从中删除数据或日志文件的数据库，然后单击“属性”命令

C、若要删除数据文件，单击“常规”选项卡。若要删除日志文件，单击“事务日志”选项卡

D、在“文件名”列户，单击要删除的文件名旁边的箭头，再点 DELETE 键，文件名旁出现十字光标，表明将删除此文件

715、参数 REMOTE_LOGIN_PASSWORDFILE 在 Oracle 数据库实例的初始化参数文件中，

此参数控制着密码文件的使用及其状态，以下说法正确的是：（ABCD）

A、NONE：只是 Oracle 系统不使用密码文件，不允许远程管理数据库

B、EXCLUSIVE：指示只有一个数据库实例可以使用密码文件

C、SHARED：指示可有多个数据库实例可以使用密码文件

D、以上说法都正确

716、关于 SQL Server 2000 中的 SQL 账号、角色，下面说法正确的是：（ABC）

A、PUBLIC,guest 为缺省的账号　　B、guest 不能从 master 数据库清除

C、可以通过删除 guest 账号的角色，从而消弱 guest 可能带来的安全隐患

D、SQL Server 角色的权限是不可以修改的

717、连接 MySQL 后选择需要的数据库 DB_NAME？以下哪些方法是对的（AC）

A、连接后用 USE DB_NAME 选择数据库

B、连接后用 SET DB_NAME 选择数据库

C、用 mysql -h host -u user -p DB_NAME 连接数据库

D、用 mysql -h host -u user -p -T DB_NAME 连接数据库

718、如果数据库不需要远程访问，可以禁止远程 tcp/ip 连接，以增强安全性。可选择的有效方法：（AC）

A、用防火墙封堵数据库侦听端口避免远程连接　　B、禁止 tcp/ip 协议的使用

C、在 mysqld 服务器中参数中添加 --skip-networking 启动参数来使 mysql

D、在/etc/my.cnf 下添加 remoteConnnect=disable

719、以下哪些 MySQL 中 GRANT 语句的权限指定符？（ABCDEF）

A、ALTER　　B、CREATE　　C、DELETE

D、UPLOAD　　E、DROP　　F、INSERT

720、用 THC 组织的 Oracle 的工具，通过 sniffer 方式抓取数据库的认证信息可有效破解 Oracle 密码，以下哪些数据是必须获取的？（ABC）

A、AUTH_SESSKEY　　B、AUTH_PASSWORD　　C、用户名　　D、实例名

721、在 Oracle 9 数据库可以通过配置$Oracle_HOME\network\admin\sqlnet.ora 文件实现数据库层次的基于 TCP 协议和地址的访问控制。下面说法正确的是：（ABCD）

A、首先需要配置 TCP,VALIDNODE_CHECKING=yes 启用节点检查功能

B、其次配置 TCP.INVITED_NODES=192.168.0.12，192.168.0.33 将会允许地址是 192.168.0 网段的 12 和 33 的主机访问

C、然后配置 TCP.EXCLUDED_NONES=192.168.0.123 将会禁止地址是 192.168.0 网段的 123 的主机访问

D、要以上配置生效必须重启 lsnrctl 监听器

722、在 SQL Server 2000 中，如果想查询当前数据库服务器软件的版本，可以使用下面哪些方式（ABCD）

A、在查询分析器中通过如下语句查询 SELECT ServerPROPERTY(‘productversion’),ServerPROPERTY(‘productlevel’),ServerPROPERTY(‘edition’)

B、在命令行下，用 SQL Server 自带的管理工具 osql 连接进入数据库，输入 select@@version

C、企业管理器查看服务器属性　　D、在 SQL Server 服务管理器里面查看“关于”

723、在 SQL Server 2000 中一些无用的存储过程，这些存储过程极容易被攻击者利用，攻击数据库系统。下面的存储过程哪些可以用来执行执行系统命令或修改注册表？（ABC）

A、xp_cmdshell　　B、xp_regwrite　　C、xp_regdeletekey　　D、select * from master

724、在 SQL Server 中创建数据库，如下哪些描述是正确的？（ABCD）

A、创建数据库的权限默认授权 sysadmin 和 dbcreator 固定服务器角色的成员，但是它仍可以授予其他用户

B、创建数据库的用户将成为该数据库的所有者

C、在一个服务器上，最多可以创建 32,767 个数据库

D、数据库名称必须遵循标示符规则

725、在对 SQL Server 2000 的相关文件、目录进行安全配置时，下面可以采用的措施是：（ABCD）

A、删除缺省安装时的例子样本库

B、将存放数据的库文件，配置权限为 administrators 组、system 和启动 SQL Server 服务的用户账号及 DBA 组具有完全控制权限

C、对 SQL Server 安装目录，去除 everyone 的所有控制权限

D、将数据库数据相关的文件，保存在非系统盘的 NTFS 独立分区

726、sybase 数据库文件系统需要哪些裸设备？（ABCD）

A、master　　B、proce　　C、data　　D、log

727、Oracle 支持哪些加密方式？（ABCD）

A、DES　　B、RC4_256　　C、RC4_40　　D、DES40

728、SQL Server 用事件探测器可以帮助排除故障和解决问题，创建跟踪的步骤如下哪些是正确的？（ABCD）

A、从“模板名称”下拉菜单为你创建跟踪选择一个模板

B、“事件探查器”主界面打开后，从“文件”菜单选择“新跟踪”

C、在“跟踪名称”文本框中输入你想要为这个跟踪创建的跟踪名称

D、修改这些默认的选项设置。通过点击“显示全部事件”和“显示全部列”复选框来查看其他的选项。

729、最重要的电磁场干扰源是：（BCD）

A、电源周波干扰　　B、雷电电磁脉冲 LEMP

C、电网操作过电压 SEMP　　D、静电放电 ESD

730、雷电侵入计算机信息系统的途径主要有：（ABD）

A、信息传输通道线侵入　　B、电源馈线侵入　　C、建筑物　　D、地电位反击

731、电信生产其机房作业，是由专门的值机员、机务员来完成，作业内容是：固定电话、无线电话、电报、载波、短波、微波、卫星和电力等电信通信设备，使设备出去良好状态，保证其正常运行。（ABCD）

A、安装　　B、值守　　C、维护　　D、检修

732、对计算机系统有影响的腐蚀性气体大体有如下几种：（ABCD）

A、二氧化硫　　B、氢化硫　　C、臭氧　　D、一氧化碳

733、防火工作的基本措施有：（ABCD）

A、加强对人员的教育管理　　B、加强对可燃物的管理

C、加强对物的管理　　D、加强对火源、电源的管理

734、会导致电磁泄漏的有（ABCDE）

A、显示器　　B、开关电路及接地系统

C、计算机系统的电源线　　D、机房内的电话

E、信号处理电

735、火灾自动报警、自动灭火系统部署应注意（ABCD）。

A、避开可能招致电磁干扰的区域或设备　　B、具有不间断的专用消防电源

C、留备用电源　　D、具有自动和手动两种触发装置

736、计算机场地安全测试包括（ABCD）。

A、温度，湿度，尘埃　　B、照度，噪声，电磁场干扰环境场强

C、接地电阻，电压、频率　　D、波形失真率，腐蚀性气体的分析方法

737、计算机信息系统设备处于不同雷电活动地区，其雷电电磁场强度有很大差异，根据这一差异，将被防护空间分为下列哪些防护区？（ABCD）

A、直击雷非防护区（LPZOA）　　B、直击雷防护区（LPZOB）

C、第一防护区（LPZI）　　D、后续防护区（LPZ2,3...等）

738、静电的危害有（ABCD）。

A、导致磁盘读写错误，损坏磁头，引起计算机误动作　　B、造成电路击穿或者毁坏

C、电击，影响工作人员身心健康　　D、吸附灰尘

739、灭火的基本方法有（ABCD）。

A、冷却法　　B、隔离法　　C、窒息法　　D、抑制

740、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

741、使用配有计算机的仪器设备时，不应该做的有：（ABCD）

A、更改登机密码和系统设置

B、自行安装软件

C、玩各种电脑游戏

D、将获得的图像、数据等资料存储在未予指定的硬盘分区上

742、硬件设备的使用管理包括（ABCD）。

A、严格按硬件设备的操作使用规程进行操作

B、建立设备使用情况日志，并登记使用过程

C、建立硬件设备故障情况登记表

D、坚持对设备进行例行维护和保养

743、预防静电的措施有（ABCD）。

A、接地　　B、不使用或安装产生静电的设备

C、不在产生静电场所穿脱工作服　　D、作业人员穿防静电鞋

744、在实验室中引起火灾的通常原因包括：（ABCD）

A、明火　　B、电器保养不良

C、仪器设备在不使用时未关闭电源　　D、使用易燃物品时粗心大意

745、直击雷：直接击在（ABCD）并产生电效应、热效应和机械力的雷电放电。

A、建筑物　　B、构建物　　C、地面突进物　　D、大地或设备

746、员工区域安全守则包括：（ABCD）

A、非工作时间，员工进入或离开办公区域，应在值班人员处登记

B、外来人员进入办公区域或机房，相关员工必须全程陪同

C、将物品带入/带出公司，要遵守公司相关的规定及流程

D、参加会议时遵守会前、会中、会后的保密流程

747、机房出入控制措施包括：（ABCD）

A、机房接待前台须核查弄清业务系统安全区域的来访者的身份，并记录其进入和离开安全区域的日期与时间

B、机房须告知进入安全区的来访者，该区域的安全要求和紧急情况下的行动步骤

C、可采用强制性控制措施，对来访者的访问行为进行授权和验证

D、要求所有进出机房人员佩带易于辨识的标识

748、为了减小雷电损失，可以采取的措施有（ACD）

A、机房内应设等电位连接网络　　B、部署 UPS

C、设置安全防护地与屏蔽地

D、根据雷击在不同区域的电磁脉冲强度划分，不同的区域界面进行等电位连接

749、安全要求可以分解为（ABCDE）。

A、可控性　　B、保密性　　C、可用性　　D、完整性　　E、不可否认性

750、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（ABC）

A、MD2　　B、MD4　　C、MD5　　D、Cost256

751、利用密码技术，可以实现网络安全所要求的。（ABCD）

A、数据保密性　　B、数据完整性　　C、数据可用性　　D、身份验证

752、一个密码体系一般分为以下哪几个部分？（ABCD）

A、明文　　B、加密密钥和解密密钥

C、密文　　D、加密算法和解密算法

753、公钥密码体质的应用主要在于。（AC）

A、数字签名　　B、加密　　C、密钥管理　　D、哈希函数

754、目前基于对称密钥体制的算法主要有。（BC）

A、RSA　　B、DES　　C、AES　　D、DSA

755、使用 esp 协议时，可以使用的加密运算是。（ABC）

A、DES　　B、3DES　　C、AES　　D、RSA

756、数字签名的作用是。（ACD）

A、确定一个人的身份　　B、保密性

C、肯定是该人自己的签字　　D、使该人与文件内容发生关系

757、以下属于对称加密算法的是：（ABD）

A、DES　　B、3DES　　C、SHA-1　　D、RC4　　E、MD5

758、在加密过程中，必须用到的三个主要元素是（ABC）

A、所传输的信息（明文）　　B、加密 钥匙(Encryption Key)

C、加密函数　　D、传输信道

759、账号口令管理办法适用于所有和 DSMP 系统、智能网系统、彩铃平台相关的（ACD）

A、系统管理员　　B、操作系统

C、操作维护人员　　D、所有上述系统中存在的账号和口令

760、为保证密码安全，我们应采取的正确措施有（ABC）

A、不使用生日做密码　　B、不使用少于 5 为的密码

C、不适应纯数字密码　　D、将密码设的非常复杂并保证 20 位以上

761、公司在使用数据签名技术时，除充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名外，还应注意（ABCD）

A、采取保护公钥完整性的安全措施，例如使用公约证书

B、确定签名算法的类型、属性以及所用密钥长度

C、用于数字签名的密钥应不同于用来加密内容的密钥

D、符合有关数字签名的法律法规，必要时，应在合同或协议中规定使用数字签名的相关事宜

762、相对于对称加密算法，非对称密钥加密算法（ACD）

A、加密数据的速率较低

B、更适合于现有网络中对所传输数据（明文）的加解密处理

C、安全性更好　　D、加密和解密的密钥不同

763、一个典型的 PKI 应用系统包括（ABCD）实体

A、认证机构 CA　　B、册机构 RA　　C、证书及 CRL 目录库　　D、用户端软件

764、加密的强度主要取决于（ABD）

A、算法的强度　　B、密钥的保密性　　C、明文的长度　　D、密钥的强度

765、一下对于对称密钥加密说法正确的是（BCD）

A、对称加密算法的密钥易于管理　　B、加解密双方使用同样的密钥

C、DES 算法属于对称加密算法　　D、相对于非对称加密算法，加解密处理速度比较快

766、在通信过程中，只采用数字签名可以解决（ABC）等问题

A、数据完整性　　B、数据的抵抗赖性　　C、数据的篡改　D、数据的保密性

767、对称密钥算法体系包括：（ABCDE）

A、明文(plaintext)：原始消息或数据，作为算法的输入

B、加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换

C、秘密密钥(secret key)：秘密密钥也是算法输入，算法进行的具体替换和转换取决于这个密钥

D、密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对于一个给定的消息，两个不同的密钥会产生两个不同的密文

、.解密算法(decryption algorithm)：本质上是加密算法的执行。它使用密文和统一密钥产生原始明文

768、一下对于混合加密方式说法正确的是。（BCD）

A、 使用公开密钥密码体制对要传输的信息（明文）进行加解密处理

B、使用对称加密算法对要传输的信息（明文）进行加解密处理

C、使用公开密钥密码体制对称加密密码体制的密钥进行加密后的通信

D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的

769、电信的网页防篡改技术有（ABC）

A、外挂轮询技术　　B、核心内嵌技术

C、时间触发技术　　D、安装防病毒软件

770、病毒发展的趋势是？（ABC）

A、 范围更广　　B、度更快　　C、方式更多

771、病毒自启动方式一般有（ABC）

A、 修改注册表　　B、将自身添加为服务

C、将自身添加到启动文件夹　　D、修改系统配置文件

772、常见 Web 攻击方法有一下哪种？（ABCD）

A、SQL Injection　　B、Cookie 欺骗　　C、跨站脚本攻击

D、信息泄露漏洞　　E、文件腹泻脚本存在的安全隐患

F、 GOOGLE HACKING

773、宏病毒感染一下哪些类型的文件？（ABCDEF）

A.、DOC　　B、EXE　　C、XLS　　D、DOT

774、木马传播包括一下哪些途径：（ACD）

A.、通过电子邮件的附件传播　　B、通过下载文件传播

C、通过网页传播　　D、通过聊天工具传播

775、目前最好的防病毒软件能做到的是（ABCD）

A.、检查计算机是否感染病毒，消除已感染的任何病毒

B、杜绝病毒对计算的侵害

C、查出计算机已感染的已知病毒，消除其中的一部分

D、检查计算机是否染有已知病毒，并作相应处理

776、通用的 DoS 攻击手段有哪些？（CD）

A、 SYN Attack　　B、ICMP Flood　　C、UDP Flood

D、Ping of Death　　E、Tear Drop　　F、Ip Spoofing

777、以下关于蠕虫的描述正确的有：（ABCDEF）

A、 蠕虫具有自动利用网络传播的特点，在传播的同时，造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪

B、 隐藏式蠕虫的基本特征，通过在主机上隐藏，使得用户不容易发现它的存在

C、蠕虫需要传播受感染的宿主文件来进行复制

D、蠕虫的传染能力主要是针对计算机内的文件系统。

778、以下哪几种扫描检测技术属于被动式的检测技术？（AB）

A、 基于应用的检测技术　　B、基于主动的检测技术

C、基于目标的漏洞检测技术　　D、基于网络的检测技术

779、以下是检查磁盘与文件是否被病毒感染的有效方法：（BC）

A、 检查磁盘目录中是否有病毒文件　　B、用抗病毒软件检查磁盘的各个文件

C、用放大镜检查磁盘编码是否有霉变现象　　D、检查文件的长度是否无故变化

780、造成计算机不安全的因素有（BD）等多种。

A、 技术原因　　B、自然原因　　C、认为原因　　D、管理原因

781、嗅探技术有哪些特点？（ABCD）

A、间接性　　B、.直接性　　C、隐蔽性　　D、开放性

782、一个恶意的攻击者必须具备哪几点？（ABC）

A、 方法　　B、机会　　C、动机　　D、运气

783、对于 DOS 网络攻击，可以采用以下哪些措施来缓解主机系统被攻击进程。（ACD）

A.、缩短 SYN Timeout 时间和设置 SYN Cookie　　B、增加网络带宽

C、在系统之前增加负载均衡设备　　D、在防火墙上设置 ACL 或黑客路由

784、利用 Bind/DNS 漏洞攻击的分类主要有（ACD）

A、 拒绝服务　　B、匿名登录　　C、.缓冲区溢出

D、DNS 缓存中毒　　E、病毒或后门攻击

785、常见 Web 攻击方法有一下哪种？（ABCD）

A、 SQL Injection　　B、 Cookie 欺骗　　C、 跨站脚本攻击　　D、信息泄露漏洞

786、黑客所使用的入侵技术主要包括（ABCDE）

A.、协议漏洞渗透　　B、密码分析还原　　C、应用漏洞分析与渗透

D、拒绝服务攻击　　E、病毒或后门攻击

787、主动响应，是指基于一个检测到的入侵所采取的措施。对于主动响应来说，其选择的措施可以归入的类别有（ABC）

A、针对入侵者采取措施　　B、修正系统

C、收集更详细的信息　　D、入侵追踪

788、下面哪些漏洞属于网络服务类安全漏洞：（BC）

A.、Windows 2000 中文版输入法漏洞　　B、IS Web 服务存在的 IDQ 远程溢出漏洞

C、RPC DCOM 服务漏洞　　D、Web 服务 asp 脚本漏洞

789、系统感染病毒后的现象有哪些？（ABCD）

A、系统错误或系统崩溃　　B、系统反应慢，网络拥塞

C、陌生的进程或服务　　D、陌生的自启动

三、判断题：（790-1000）

790、TCSEC 将信息安全风机防护等级一共分为 7 个安全等级：D、C1、C2、B1、B2、B3、A。(A)

A、正确　　B、错误

791、通用标准 v2 版（CC）的安全等级是以 EAL 来表示的。（A）

A、正确　　B、错误

792、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。（A）

A、正确　　B、错误

793、在信息安全领域，CIA 通常是指：保密性、完整性和可用性。（A）

A、正确　　B、错误

794、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。（A）

A、正确　　B、错误

795、在信息安全领域，CIA 通常是指：保密性、完整性和非抵赖性。（B）

A、正确　　B、错误

796、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确　　B、错误

797、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。（B）

A、正确　　B、错误误

798、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。（B）

A、正确　　B、错误

799、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。（A）

A、正确　　B、错误

800、网络与信息都是资产，具有不可或缺的重要价值。（A）

A、正确　　B、错误

801、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。（B）

A、正确　　B、错误

802、主机加固完成后，一般可以有效保证主机的安全性增强。（A）

A、正确　　B、错误

803、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。（A）

A、正确　　B、错误

804、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。（A）

A、正确　　B、错误

805、HP-UX 系统加固中在设置 ROOT 环境变量不能有相对路径设置。（A）

A、正确　　B、错误

806、屏幕保护的木马是需要分大小写。（B）

A、正确　　B、错误

807、安全审计就是日志的记录。（B）

A、正确　　B、错误误

808、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。（A）

A、正确　　B、错误

809、AIX 系统加固时，对系统配置一般需要自编脚本完成。（A）

A、正确　　B、错误

810、Windows NT 中用户登录域的口令是以明文方式传输的。（B）

A、正确　　B、错误

811、操作系统普通用户账号审批记录应编号、留档。（A）

A、正确　　B、错误

812、计算机病毒是计算机系统中自动产生的。（B）

A、正确　　B、错误

813、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。（A）

A、正确　　B、错误

814、4A 系统的建设能够减轻账户管理员的维护工作。（A）

A、正确　　B、错误

815、4A 系统的接入管理可以管理到用户无力访问的接入。（B）

A、正确　　B、错误

816、Cisco 路由器可以使用 enable password 命令为特权模式的进入设置强壮的密码。（B）

A、正确　　B、错误

817、Cisco 设备的 AUX 端口默认是启用的。（A）

A、正确　　B、错误

818、DHCP 可以向终端提供 IP 地址、网关、DNS 服务器地址等参数。（A）

A、正确　　B、错误误

819、Inbound 方向的 NAT 使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际 IP 地址。（B）

A、正确　　B、错误

820、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。（A）

A、正确　　B、错误

821、IPS 的过滤器规则不能自由定义。（B）

A、正确　　B、错误

822、IPS 的某些功能和防火墙类似。（A）

A、正确　　B、错误

823、IPS 和 IDS 都是主动防御系统。（B）

A、正确　　B、错误

824、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。（A）

A、正确　　B、错误

825、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。(A)

A、正确　　B、错误

826、Netscreen 防火墙的外网口应禁止 PING 测试，内网口可以不限制。（B）

A、正确　　B、错误

827、OSI 是开放的信息安全的缩写。（B）

A、正确　　B、错误

828、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。（A）

A、正确　　B、错误

829、OSI 中会话层不提供机密性服务。（A）

A、正确　　B、错误

830、SSH 使用 TCP 79 端口的服务。（B）

A、正确　　B、错误

831、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。（B）

A、正确　　B、错误

832、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。　（A）

A、正确　　B、错误

833、TCP/IP 协议体系结构中，IP 层对应 OSI/RM 模型的网络层。（A）

A、正确　　B、错误

834、默认情况下需要关闭 Cisco 设备的 Small TCP/UDP 服务。（A）

A、正确　　B、错误

835、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。（B）

A、正确　　B、错误

836、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。（A）

A、正确　　B、错误

837、入侵检测可以处理数据包级的攻击。（B）

A、正确　　B、错误

838、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。（A）

A、正确　　B、错误

839、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。（B）

A、正确　　B、错误

840、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。（A）

A、正确　　B、错误

841、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。（B）

A、正确　　B、错误

842、统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。（A）

A、正确　　B、错误

843、透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决 IP 地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的 IP 的地址。（A）

A、正确　　B、错误

844、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。（A）

A、正确　　B、错误

845、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。（B）

A、正确　　B、错误

846、网络边界的 Cisco 路由器应关闭 CDP 服务。（A）

A、正确　　B、错误

847、网络边界 Cisco 设备的 CDP 协议可以开放。（B）

A、正确　　B、错误

848、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。（B）

A、正确　　B、错误

849、针对不同的攻击行为，IPS 只需要一个过滤器就足够了。（B）

A、正确　　B、错误

850、主机型 IDS 其数据采集部分当然位于其所检测的网络上。（B）

A、正确　　B、错误

851、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。（B）

A、正确　　B、错误

852、IPS 虽然能主动防御，但是不能坚挺网络流量。（B）

A、正确　　B、错误

853、防火墙安全策略定制越多的拒绝规则，越有利于网络安全。（B）

A、正确　　B、错误

854、审计系统进行关联分析时不需要关注日志时间。（B）

A、正确　　B、错误

855、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。（A）

A、正确　　B、错误

856、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。（A）

A、正确　　B、错误

857、侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。（A）

A、正确　　B、错误

858、模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。（A）

A、正确　　B、错误

859、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。（A）

A、正确　　B、错误

860、VPN 的主要特点是通过加密是信息安全的通过 Internet 传递。（A）

A、正确　　B、错误

861、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。（B）

A、正确　　B、错误

862、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。（A）

A、正确　　B、错误

863、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。（A）

A、正确　　B、错误

864、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。（A）

A、正确　　B、错误

865、HTTP 协议是文本协议，可利用回车换行做边界干扰。（A）

A、正确　　B、错误

866、Init<sid>.ora 文件是 Oracle 启动文件，任何参数的配置错误都会造成 Oracle 不能启动，任何参数的不合理配置都可能造成系统故障。（A）

A、正确　　B、错误

867、Mysqldump 是采用 SQL 级别的备份机制，它将数据表导成 SQL 脚本文件，在不同的 MySQL 版本之间升级时相对比较合适，这也是最常见的备份方法。（A）

A、正确　　B、错误

868、Orabrute 是进行远程破解 Oracle 密码的工具，要猜解的密码可以在 password.txt 中设置。（A）

A、正确　　B、错误

869、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。（A）

A、正确　　B、错误

870、Oracle 的若算法加密机制：两个相同的用户名和密码在两个不同的 Oracle 数据库机器中，将具有相同的哈希值。（A）

A、正确　　B、错误

871、Oracle 密码允许包含像“SELECT”，“DELETE”，“CREATE”这类的 Oracle/SQL 关键字。（B）

A、正确　　B、错误

872、Oracle 的 HTTP 的基本验证可选择 SYS 破解，因为它始终存在和有效。（A）

A、正确　　B、错误

873、Oracle 默认情况下，口令的传输方式是加密。（B）

A、正确　　B、错误

874、Oracle 数据库的归档日志不是在线日志的备份。（B）

A、正确　　B、错误

875、OSI 网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。（A）

A、正确　　B、错误

876、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）

A、正确　　B、错误

877、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。（A）

A、正确　　B、错误

878、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。（A）

A、正确　　B、错误

879、SQL Server 数据库应禁止使用除 tcp/ip 以外的协议，保护数据库通信安全。（A）

A、正确　　B、错误

880、SQL Server 应该社会自日志审核无法追踪回溯安全事件。（A）

A、正确　　B、错误

881、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。(A)

882、Web 攻击面不仅仅是浏览器中可见的内容。（A）

A、正确　　B、错误

883、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。（B）

A、正确　　B、错误

884、暴力猜解不能对 Web 应用进行攻击。（B）

A、正确　　B、错误

885、在 Oracle 自身的配置上做限定方法是：修改$Oracle_HOME\network\admin 目录下面的 SQLNET..ORA 文件，类似设置如下：

Tcp_validnode_checking=YES

Tcp_invited_nodes=

(192.168.0.1,ip2,ip3•...)。

(　A　)

A、正确　　B、错误

886、不设置必要的日志审核，就无法追踪回溯安全事件，Oracle 中若果要审计记录成功的登陆语句”SQL>audit session whenever successful;”.　(　A　)

A、正确　　B、错误

887、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。（B）

A、正确　　B、错误

888、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。（B）

A、正确　　B、错误

889、访问控制、强制登陆、自动安全更新都属于 Window2000 的安全组件（B）

A、正确　　B、错误

890、复杂的系统存在大量的相互引用访问，如果开发者不能有效的进行权限控制，就可能被恶意引用。（A）

A、正确　　B、错误

891、攻击者可以通过 SQL 注入手段获取其他用户的密码。（A）

A、正确　　B、错误

892、几乎所有的关系数据库系统和相应的 SQL 语言都面临 SQL 注入的潜在威胁。（A)

A、正确　　B、错误

893、简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架（B）

A、正确　　B、错误

894、默认可通过 Web 程序来远程管理 Oracle10g 数据库，端口是 8080.（A）

A、正确　　B、错误

895、如果 sa 是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。（A）

A、正确　　B、错误

896、如果在 SQL Server 等领域成功并不意味这该用户已经可以访问 SQL Server 上的数据库。（A）

A、正确　　B、错误

897、如果知道 Oracle 密码长度，用 Rainbow 表生成器来破解其密码哈希值是绝对成功的。（A）

A、正确　　B、错误

898、所有操作系统、数据库、网络设备，包括一部分业务系统，均需要支持基于账号的访问控制功能。（B）

A、正确　　B、错误

899、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。（A）

A、正确　　B、错误

900、为 Oracle 数据库安全考虑，在对人共同对数据库进行维护时应依赖数据库预定义的传统角色。（B）

A、正确　　B、错误

901、为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。(A)

A、正确　　B、错误

902、系统类型鉴别为检查主机系统与开放服务是否存在安全漏点。（B）

A、正确　　B、错误

903、系统漏洞扫描为检查目标的操作系统与应用系统信息。（B）

A、正确　　B、错误

904、选择远程破解 Oracle 的最好账户是 SYS，因为此账户永远有效。（A）

A、正确　　B、错误

905、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。（A）

A、正确　　B、错误

906、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。（A）

A、正确　　B、错误

907、用 Sqlplus 登陆到 Oracle 数据库，使用 slesct username, password form dba_users 命令可查看数据库中的用户名和密码明文。（B）

A、正确　　B、错误

908、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。（A）

A、正确　　B、错误

909、在 Oracle 所有版本在安装的时候都没有提示修改 SYS 的默认密码。（B）

A、正确　　B、错误

910、在 ORacle 数据库安装补丁时，不需要关闭所有与数据库有关的服务。（B）

A、正确　　B、错误

911、在 SQL Server 安装 SP3 补丁时不需要系统中已经安装了 SP1 或 SP2。（B）

A、正确　　B、错误

912、在 SQL Server 中具有 sysadmin 权限的用户可以通过 xp_cmdshell 存储扩展以 system 的权限执行任意系统命令。（A）

A、正确　　B、错误

913、Oracle 默认配置下，每个账户如果有 30 次的失败登陆，此账户将被锁定。（B）

A、正确　　B、错误

914、定制开发 Web 系统的安全度不如标准的产品。（A）

A、正确　　B、错误

915、对 MySQL 注入攻击时，经常用到注释符号#来屏蔽剩下的内置 SQL 语句。（A）

A、正确　　B、错误

916、一个登录名只能进入服务器，但是不能让用户访问服务器中的数据库资源。每个登录名的定义存放在 msater 数据库的 syslogins 表中。（A）

A、正确　　B、错误

917、Web 错误信息可能泄露服务器型号版本、数据库型号、路径、代码。（A）

A、正确　　B、错误

918、Oracle 的密码哈希值存储在 SYS.USER$表中。可以通过像 DBA USERS 这类的视图来访问。（A）

A、正确　　B、错误

919、产品的定制开发是应用安全中最薄弱的一环。（A）

A、正确　　B、错误

920、Oracle 限制了密码由英文字母，数字，#，下划线（_），美元字符（$）构成，密码的最大长度为 30 字符；并不能以”$”,”#”,”_”或任何数字开头。（A）

A、正确　　B、错误

921、网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。（B）

A、正确　　B、错误

922、计算机场地可以选择在公共区域人流量比较大的地方。（B）

A、正确　　B、错误

923、EMC 测试盒约束用户关心的信息信号的电磁发射、TEMPEST 只测试盒约束系统和设备的所有电磁发射。（B）

A、正确　　B、错误

924、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。（B）

A、正确　　B、错误

925、出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。（B）

A、正确　　B、错误

926、红区：红新号的传输通道或单元电路称为红区，反之为黑区。（A）

A、正确　　B、错误

927、机房应设置相应的活在报警和灭火系统。（A）

A、正确　　B、错误

928、计算机机房的建设应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。（A）

A、正确　　B、错误

929、计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。（B）

A、正确　　B、错误

930、接地线在穿越墙壁、楼板和地坪时应套钢管或其他非金属的保护套管，钢管应与接地线做电气连通。（A）

A、正确　　B、错误

931、提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。（A）

A、正确　　B、错误

932、在计算机机房附近施工，不负有维护计算机信息系统安全的责任和义务。（B）

A、正确　　B、错误

933、只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。（B）

A、正确　　B、错误

934、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。（B）

A、正确　　B、错误

935、防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。（A）

A、正确　　B、错误

936、对于公司机密信息必须根据公司的相关规定予以适当的标识。（A）

A、正确　　B、错误

937、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。（A）

A、正确　　B、错误

938、如果在电话、电视会议中涉及讨论工伤机密信息，会议主持人或组织人在会议全过程中一定要确认每一个与会者是经授权参与的。（A）

A、正确　　B、错误

939、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。（B）

A、正确　　B、错误

940、将公司的机密信息通过互联网络传送时，必须予以加密。（A）

A、正确　　B、错误

941、机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。（A）

A、正确　　B、错误

942、有很高使用价值或很高机密程度的重要数据应采用加密等方式进行保密。（A）

A、正确　　B、错误

943、“一次一密”属于序列密码的一种。（A）

A、正确　　B、错误

944、3DES 算法的加密过程就是用一个秘钥对待加密的数据执行三次 DES 算法的加密操作。（B）

A、正确　　B、错误

945、AES 加密算法的秘钥长度为 128、192 或 256 位。（A）

A、正确　　B、错误

946、AES 是一种非对称算法。（B）

A、正确　　B、错误

947、DES3 和 RSA 是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。（A）

A、正确　　B、错误

948、Diffie-Hellman 算法的安全性取决于离散对数计算的困难性，可以实现秘钥交换。（A）

A、正确　　B、错误

949、DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。（A）

A、正确　　B、错误

950、MD5 是一种加密算法。（B）

A、正确　　B、错误

951、PGP 协议缺省的压缩算法是 ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。（A）

A、正确　　B、错误

952、PKI 是一个用对称密码算法和技术来实现并提供安全服务的具有通用性的安全基础设施。（B）

A、正确　　B、错误

953、RC4 是典型的的序列密码算法。（A）

A、正确　　B、错误

954、RSA 算法作为主要的非对称算法，使用公钥加密的秘闻一定要采用公钥来街。（B）

A、正确　　B、错误

955、安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。（A）

A、正确　　B、错误

956、常见的公钥密码算法有 RSA 算法、Diffie-Hellman 算法和 EIGamal 算法。（A）

A、正确　　B、错误

957、当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。（A）

A、正确　　B、错误

958、发送方使用 AH 协议处理数据包，需要对整个 IP 的数据包计算 MAC，包括 IP 头的所有字段和数据。（B）

A、正确　　B、错误

959、分组密码的优点是错误扩展小、速度快、安全程度高。（B）

A、正确　　B、错误

960、公共迷药密码体制在秘钥管理上比对称秘钥密码体制更安全。（A）

A、正确　　B、错误

961、古典加密主要采用的主要方法是置换，代换。（A）

A、正确　　B、错误

962、古典加密主要是对加密算法的保密，现代加密算法是公开的，主要是针对秘钥进行保密。（A）

A、正确　　B、错误

963、基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。（A）

A、正确　　B、错误

964、口令应在 120 天至少更换一次。（B）

A、正确　　B、错误

965、链路加密方式适用于在广域网系统中应用。（B）

A、正确　　B、错误

966、密码保管不善属于操作失误的安全隐患。（B）

A、正确　　B、错误

967、日常所见的校园饭卡是利用身份认证的单因素法。（A）

A、正确　　B、错误

968、身份认证要求对数据和信息来源进行验证，以确保发信人的身份。（B）

A、正确　　B、错误

969、身份认证与权限控制是网络社会的管理基础。（A）

A、正确　　B、错误

970、数据在传输过程中用哈希算法保证其完整性后，非法用户无法无法对数据进行任何修改。（B）

A、正确　　B、错误

971、数字签名比较的是摘要结果长度是否都是 128 位。（B）

A、正确　　B、错误

972、通信数据与文件加密是同一个概念。（B）

A、正确　　B、错误

973、为 AES 开发的 Rijndae1 算法的秘钥长度是 128 位，分组长度也为 128 位。（B）

A、正确　　B、错误

974、为了保证安全性，密码算法应该进行保密。（B）

A、正确　　B、错误

975、文件压缩变换是一个单向加密过程。（B）

A、正确　　B、错误

976、我的公钥证书不能在网络上公开，否则其他人可能冒充我的身份或伪造我的数字签名。（B）

A、正确　　B、错误

977、现代加密算法可以分为对称加密算法和非对称加密。（A）

A、正确　　B、错误

978、虚拟专用网 VPN 的关键技术主要是隧道技术、加解密技术、秘钥管理技术以及使用者与设备身份认证技术。（A）

A、正确　　B、错误

979、以当前的技术来说，RSA 体制是无条件安全的。（B）

A、正确　　B、错误

980、在 4A 系统的远期建设中，应用系统自身不需要保留系统从账户信息。（B）

A、正确　　B、错误

981、在 MD5 算法中，要先将以初始化的 A、B、C、D 这四个变量分别复制到 a、b、c、d 中。（A）

A、正确　　B、错误

982、在 MD5 算法中要用到 4 个变量，分别表示 A、B、C、D，均为 32 位长。（A）

A、正确　　B、错误

983、在 PKI 中，注册机构 RA 是必要的组件。（B）

A、正确　　B、错误

984、在 SSL 握手协议过程中，需要服务器发送自己的证书。（A）

A、正确　　B、错误

985、在非对称加密过程中，加密和解密使用的是不同的秘钥。（A）

A、正确　　B、错误

986、在公钥加密系统中，用公钥加密的密文可以由私钥解密，但用公钥加密的密文，不能用公钥解密。　（B）

A、正确　　B、错误

987、在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一种“破解”。 （A）

A、正确 B、错误

988、账户管理的 Agent 不适用于在网络设备中部署。 （A）

A、正确 B、错误

989、整个 PKI 系统有证书服务器 AS、票据许可服务器 TGS、客户机和应用服务器四部分组成。 （B）

A、正确 B、错误

990、最基本的认证方式选择证书是数字证书。（B）

A、正确 B、错误

991、最小特权、纵深防御是网络安全原则之一。（A）

A、正确 B、错误

992、数字证书是由权威机构 CA 发行的一种权威的电子文档，是网络环境中的一种身份证。（A）

A、正确 B、错误

993、数字证书是由权威机构 PKI 发行的一种权威性的电子文档，是网络环境中的一种身份证。 （B）

A、正确 B、错误

994、信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段。（A）

A、正确 B、错误

995、病毒能隐藏在电脑的 CMOS 存储器里。（B）

A、正确 B、错误

996、对感染病毒的软盘进行浏览会导致硬盘被感染。（B）

A、正确 B、错误

997、已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。（B）

A、正确 B、错误

998、重新格式化硬盘可以清楚所有病毒。（B）

A、正确 B、错误

999、专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，

并根据评估结果提供评估报告。 （A）

A、正确 B、错误

1000、冒充信件回复、假装纯文字 ICON、冒充微软雅虎发信、下载电子贺卡同意书、是使用的叫做字典攻击法的方法。（B）

A、正确 B、错误