本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html

# 信息安全导论课后习题答案

Ch01

1. 对于信息的功能特征，它的_____在于维持和强化世界的有序性动态性。

2. 对于信息的功能特征，它的_____表现为维系社会的生存、促进人类文明的进步和自身的发展。

3. 信息技术主要分为感测与识别技术、_____、信息处理与再生技术、信息的施用技术等四大类。

4. 信息系统是指基于计算机技术和网络通信技术的系统，是人、_____、数据库、硬件和软件等

各种设备、工具的有机集合。

5. 在信息安全领域，重点关注的是与_____相关的各个环节。

6. 信息化社会发展三要素是物质、能源和_____。

7. 信息安全的基本目标应该是保护信息的机密性、_____、可用性、可控性和不可抵赖性。

8. _____指保证信息不被非授权访问，即使非授权用户得到信息也无法知晓信息的内容，因而不

能使用。

9. _____指维护信息的一致性，即在信息生成、传输、存储和使用过程中不应发生人为或非人为

的非授权篡改。

10. _____指授权用户在需要时能不受其他因素的影响，方便地使用所需信息。这一目标是对信息

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
系统的总体可靠性要求。

11. _____指信息在整个生命周期内都可由合法拥有者加以安全的控制。

12.
_____指保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为。

13.
PDRR模型，即“信息保障”模型，作为信息安全的目标，是由信息的保护技术、信息使用中的检测

技术、信息受影响或攻击时的响应技术和受损后的_____组成的。 14.
当前信息安全的整体解决方案是PDRR模型和_____的整合应用。

15.
为了避免给信息的所有者造成损失，信息_____往往是有范围（区域上、时间上）和有条件的。 16.
信息技术IT简单地说就是3C，即Computer（计算机）、Communication（通信）和_____。 17. 数据链路层要负责建立、维持和释放_____的连接。
18.
传输层为两个用户进程之间建立、管理和拆除可靠而又有效的_____，常用协议有TCP和UDP。 19.
为了实现网络中各主机间的通信，每台主机都必须有一个唯一的_____。
20. IP基于_____，信息作为一个“数据包”序列--IP分组进行传递。

21.
TCP协议基于面向连接的技术，为数据包提供_____，在发送数据前需要通过三次握手建立

TCP连接。

22. TCP的报头中最为重要的部分是源端口号、_____和序列号。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
23.
每个以太网数据包都有包括源以太网地址、目的以太网地址和一个_____的报头。

24.
ARP协议可以通过发送网络广播信息的方式，将_____解释成相对应的物理层地址，即MAC

地址。

25.
ICMP即_____，用于处理错误消息，以及其他TCP/IP软件自己要处理的消息。 26.
僵尸网络是指由黑客通过控制服务器间接并_____的僵尸程序感染计算机群。 27.
网络仿冒就是通过_____来诱骗用户提供个人资料、财务账号和口令。 28.
DoS破坏了信息的（ ）。 A. 保密性 B. 完整性 C. 可用性 D. 可控性

29.
用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这是属于何种攻击手段？ A. 缓冲区溢出

B. 钓鱼攻击 C. 后门攻击 D. DDoS攻击

攻击

30.
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（ ）的

攻击。 A. 可用性 B. 保密性 C. 完整性 D. 真实性 31.
以下哪种形式不是信息的基本形态？ A. 数据 B. 文本 C. 声音和图像 D. 文稿 32.
OSI七层模型中，表示层的功能不包括（ ）。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
A. 加密解密 B. 压缩解压缩 C. 差错检验 33.
一般认为，信息化社会的发展要素不包括（ ）。 A. 电视 B. 物质 C. 能源 34.
PDRR模型不包括（ ）。 A. 保护 B. 备份 C. 检测 35.
网络环境下的安全机制不包括（ ）。 A. 数字签名 B. 访问控制 C. 灾难恢复

D. 数据格式转换 D. 信息 D. 恢复 D. 数据加密

Ch02

36.
漏洞是指硬件、软件或策略上存在的_____，从而使得攻击者能够在未授权的情况下访问、控

制系统。

37. 典型的拒绝服务攻击有_____和资源过载两种形式。

38.
扫描是采取_____的形式对目标可能存在的已知安全漏洞逐项进行检查，利用各种工具在攻击

目标的IP地址或地址段的主机上寻找漏洞。

39.
_____就是指漏洞信息公布后、还没有对应的安全补丁就出现相应的攻击手段。 40. 任何以干扰、破坏网络系统为目的的_____都称之为网络攻击。
41. 一个开放的_____就是一条与计算机进行通信的信道。

42. 互联网的“_____”三大基本特征决定了网络与信息的不安全。

43.
系统风险是由组成系统的各部件的脆弱性构成的，以下哪个不是系统风险的构成组件？ A. 访问规则 B. 硬件组件 C. 软件组件 D. 网络协议 44.
威胁和攻击的主要来源不包括（ ）。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
B. 内部管理不严造成系统安全C. 来自外部的威胁

A. 内部操作不当 D. 设备故障

管理失控 和犯罪

45. 以下（ ）不是安全威胁的表现形式。 A. 伪装 B. 解密 C. 非法连接 D. 非授权访问 46. 以下（ ）不是安全威胁的表现形式。 A. 拒绝服务 B. 非法连接 C. 业务流分析 D. 网络扫描

Ch03

47.
系统安全与功能实现的方便性是矛盾的对立。必须牺牲方便性求得安全，我们必须在这两者之间找出

_____。

48.
现实系统的安全一般要求是根据安全需求，建立安全模型，使信息安全风险被控制在可接受的

_____。

49.
信息安全的最终任务是保护信息资源被_____安全使用，并禁止非法用户、入侵者、攻击者和

黑客非法偷盗、使用信息资源。 50. ISC2的中文名称是_____。 51. CNNIC的中文名称是_____。 52. CNCERT的中文名称是_____。 53. ISO 7498-2是_____。

54. _____是指用来保护系统免受侦听、阻止安全攻击及恢复系统的机制。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html

55.
_____就是加强数据处理系统和信息传输的安全性的一类服务，其目的在于利用一种或多种安

全机制阻止安全攻击。

56. 访问控制策略的目的是保证_____。

57.
完整的信息系统安全体系框架由技术体系、_____和管理体系共同构建。

58.
组织机构体系是信息系统安全的_____，由机构、岗位和人事三个模块构成一个体系。 59.
信息系统安全的管理体系由法律管理、_____和培训管理三个部分组成。

60.
安全防范技术体系划分为物理层安全、系统层安全、_____、应用层安全和管理层安全等五个

层次。

61.
信息安全等级保护与分级认证主要包含产品认证、人员认证和_____三大类。 Ch6

62. 访问控制是在保障授权用户能获取所需资源的同时_____的安全机制。
63. 访问控制的资源可以是信息资源、处理资源、通信资源或者_____。

64.
访问控制的访问方式可以是获取信息、修改信息或者完成某种功能，一般情况可以理解为读、写或者

_____。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html

65.
访问控制的目的是为了限制访问主体对访问客体的访问权限，从而使计算机系统在合法范围内使用。

这里所指的主体一般为_____，客体一般为文件（夹）资源。

66.
访问控制一般包括自主访问控制、_____和基于角色的访问控制等三种类型。

67.
自主访问控制基于对主体或主体所属的主体组的识别来限制对客体的访问，这种控制是自主的，即完

全由客体的拥有者_____。

68. 系统中的访问控制一般由_____来表示。

69. 访问控制矩阵中的一行表示一个主体的所有权限，也称_____。

70.
访问控制矩阵中的一列则是关于一个客体的所有权限，也称_____访问控制表。

71.
访问控制矩阵中的元素是该元素所在行对应的主体对该元素所在列对应的客体的_____。 72. 可以改变文件（夹）访问控制列表的命令是_____。

73.
审计系统是追踪、恢复的直接依据，甚至是司法依据。Windows中的审计事件可以通过_____

查看。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html

74.
Windows的审计日志由一系列的事件记录组成。每一个事件记录又可分为头、_____和可选的

附加数据项三个功能部分。

75. 以下哪个不是Windows资源的共享访问权限？

D. 完全控

A. 读取及运行 B. 读取 C. 更改

制

76. 以下哪个不是Windows资源的本地访问权限？ A. 读取及运行 B. 完全控制 C. 修改 D. 复制 77. 审计跟踪可以实现多种安全相关目标，但不包括（ ）。 A. 个人职能 B. 入侵检测 C. 鉴别认证 D. 故障分析 78.
安全审计分析的主要内容有不包括（ ）。

A. 访问控制 B. 基于异常检测的轮廓 C. 简单攻击探测 D. 复杂攻击探测 79.
Windows的日志文件很多，通过事件查看器不能查阅（ ）。 A. 补丁安装日志 B. 系统日志 C. 应用程序日志 D. 安全日志

Ch08

80. CVE的中文名称为_____。

81.
主机扫描器又称本地扫描器，它与待检查系统运行于_____，执行对自身的检查。

82.
主机扫描器的主要功能为分析各种系统文件内容，查找可能存在的对系统安全造成威胁的漏洞或

_____。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html

83.
网络扫描器，一般和待检查系统运行于不同的节点上，通过网络_____，检查安全漏洞。

84.
扫描器由以下几个模块组成：用户界面、_____、扫描方法集、漏洞数据库、扫描输出报告等。 85.
风险综合分析系统在基础数据基础上，_____系统的风险。 86.
风险评估的要素包括（ ）。 A. 资产及其价值 B. 威胁 C. 脆弱性 D. 以上全部 87.
风险评估的内容不包括资产（ ）。

A. 类型及其价值 B. 面临的威胁 C. 存在的弱点 D. 造成的影响

88. 以下哪个不是互联网常用的互连协议？ A. IP B. ICMP C. DNS D. IGMP 89.
网络扫描不可以通过（ ）方式实现。 A. ICMP B. SNMP C. 端口 D. TCP/UDP

90. 很多程序接收到一些异常数据后会导致缓冲区溢出。这种漏洞属于（ ）。 A. 管理漏洞 B. 软件漏洞 C. 结构漏洞 D. 信任漏洞

91. Ping命令通过ICMP协议完成对网络中目标主机的探测，所用的端口为（ ）。

A. 7 B. 21 C. 23 D. 没有端口

Ch09

92.
数据安全采用现代密码技术对数据进行保护，是_____的安全技术，如数据保密、数据完整性、

身份认证等技术。

93.
密码学是研究数据的_____的学科，涵盖数学、计算机科学、电子与通信学科。 94.
加密技术的基本思想就是_____，使非法接入者无法理解信息的真正含义。

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html

95.
在有5个用户的单位中，若采用对称密钥密码体制，为保证加密的可靠性，必须采用互不相同的密码

用作信息的加解密，这样的系统至少需要_____个密钥。

96.
如果一个登录处理系统允许一个特定的用户识别码，通过该识别码可以绕过通常的口令检查，这种安

全威胁称为_____。

97. 在电子政务建设中，网络是基础，_____是关键，应用是目的。 98.
特洛伊木马攻击的威胁类型属于： A. 授权侵犯威胁 B. 植入威胁 C. 渗入威胁 D. 旁路控制威胁

99.
如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，

这样的系统称为：

A. 常规加密系统 B. 单密钥加密系统 C. 公钥加密系统 D. 对称加密系统

100.
用户A通过计算机网络向用户B发消息，表示自己同意签订某个合同，随后用户A反悔，不承认自

己发过该条消息。为了防止这种情况，应采用： A. 数字签名技术 B. 消息认证技术 C. 数据加密技术 D. 身份认证技术 101.
关于防火墙的功能，以下哪一种描述是错误的？

A. 防火墙可以检查B. 防火墙可以使用应用网C. 防火墙可以使用过D. 防火墙可以阻止来

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
进出内部网的通关技术在应用层上建立滤技术在网络层对自内部的威胁和攻信量协议过滤和转发功能 数据包进行选择 击

102.
有一种原则是对信息进行均衡、全面的防护，提高整个系统的“安全最低点”的安全性能，该原则

称为

A. 木桶原则 B. 整体原则 C. 等级性原则 D. 动态化原则

Ch10

103. 防火墙是位于两个(或多个)网络间，实施_____的一组组件的集合。

104.
防火墙可以实现对基于地址、用户、时间、方向、_____、内容等方面的访问控制。 105.
防火墙的体系结构有双重宿主主机体系结构、_____和屏蔽子网体系结构等三种。 106. 以下哪个不是防火墙的工作模式？ A. 路由模式 B. 桥模式 C.
混合模式 D. 网关模式 107. 网络防火墙工作在OSI七层协议中的哪一层？ A.
物理层 B. 数据链路层 C. 网络层 D. 表示层 108.
根据网络防火墙的功能，要求设备最少必须具备几个网络接口？

A. 1 B. 2 C. 3 D. 4

109. 以下说法哪个是正确的？

A. 防火墙可以防范B. 只要在网络中安C. 防火墙能自动侦测内部D.
只有符合安全策略的

来自于网络内部装了防火墙，就网络与外部网络的所有数据流才能通过防火的攻击能防范所有攻击 连接，并能自动禁用 墙 110.
能根据数据包的IP地址来判断是否放行，这样的防火墙称为：

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
A. 状态检测防火墙 B. 包过滤防火墙 C. 电路层防火墙 D. 应用网关防火墙

Ch14

111.
信息内容安全的核心技术包括信息获取技术、信息内容识别技术、_____、信息内容分级、

图像过滤、信息内容审计。

112. 信息获取技术分为主动获取技术和_____技术。

113.
主动获取技术通过向网络_____后的反馈来获取信息，接入方式简单，但会对网络造成额外

的负担。

114.
被动获取技术则在网络出入口上通过镜像或_____方式获取网络信息，不会对网络造成额外

流量。

115.
信息内容识别是指对_____进行识别、判断、分类，确定其是否为所需要的目标内容。 116.
控制/阻断技术指对于识别出的_____，阻止或中断用户对其访问。

117.
信息内容审计就是真实全面地将发生在网络上的_____记录下来，为事后的追查提供完整准

确的资料。 118. 信息内容审计采用的主要技术是以旁

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
路方式捕获受控网段内的数据流，通过协议分析、模式匹配等技术手段对网络数据流进行审计，并对_____进行监控和取证。 Ch11

1. 入侵检测系统一般由 和控制中心两部分构成。

2.在入侵检测系统中，控制中心主要用于显示和分析事以及策略定制等工作。

3.信等。

4.

5.有的知识的检测。

6.不受实质性的攻击。

7.

8.

Ch12

1.隧道协议利用附加的报头封装帧，附加的报头提供了路由信息，封装后的包所途经的公网的逻辑路径称为隧道。

2.IPSEC的传输模式只对IP数据包的数据负载进行加密或认证。 3.IPSEC 4.SA

5.一个VPN系统由VPN服务器、传输介质和VPN客户端三部分组成。

填空与选择参考答案： 1.基本功能 2.社会功能 3.信息传递技术 4.规程

5.信息处理生命周期 6.信息 7.完整性 8.机密性 9.完整性 10.可用性 11.可控性 12.不可抵赖性 13.恢复技术 14.信息安全管理 15.共享

16.Control（控制） 17.数据链路 18.端到端的连接 19.网络地址 20.无连接技术 21.可靠的连接服务 22.目标端口号 23.类型码 24.IP地址

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
25.Internet控制消息协议 26.集中控制 27.仿冒正宗网页 28.C 29.B 30.A 31.D
32.C 33.A 34.B 35.C 36.缺陷 37.资源耗尽 38.模拟攻击 39.零日攻击
40.非授权行为 41.端口

42.无序、无界和匿名 43.A 44.D 45.B

46.D 47.平衡点 48.最小限度内 49.合法用户

50.国际信息系统安全认证组织 51.中国互联网络信息中心
52.中国计算机事件应用响应中心 53.开放系统互连安全体系结构 54.安全机制
55.安全服务 56.信息的可用性 57.组织机构体系 58.组织保障系统 59.制度管理
60.网络层安全 61.系统认证 62.A 63.D 64.B 65.D

66.拒绝非授权用户 67.物理资源 68.执行 69.用户或进程 70.强制访问控制
71.授予或取消 72.访问控制矩阵 73.访问能力表 74.访问控制表 75.访问能力
76.CACLS 77.事件查看器 78.事件描述 79.A 80.D 81.C 82.A 83.A

84.公共漏洞和暴露 85.同一节点 86.配置错误 87.远程探测目标节点 88.扫描引擎
89.定量、综合分析 90.D

91.A 92.C 93.B 94.B 95.D 96.主动

97.加密、解密及其变换 98.伪装信息 99.10

100.陷门或非授权访问 101.安全 102.B 103.C 104.A 105.D 106.A

107.网络间访问控制 108.流量

109.屏蔽主机体系结构 110.D 111.C 112.C 113.D 114.B

115.控制/阻断技术 116.被动获取 117.注入数据包 118.旁路侦听

119.获取的网络信息内容 120.非法信息内容 121.所有事件 122.非法流量

信息系统是指基于计算机技术和网络通信技术的系统，是人、规程、数据库、硬件和软件等各种设备、工具的有机集合

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

拒绝服务攻击通过各种手段来消耗网络宽带和系统资源，或者攻击系统缺陷，使系统的正常服务陷于瘫痪状态，不能对正常用户进行服务，从而实现拒绝正常用户的服务访问

风险评估就是对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来风险的可能性的评估

物理安全是指为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施、环境人员，系统等采取适当的安全措施

灾难备份是指利用技术、管理手段以及相关资源，确保已有的关键数据和关键业务在灾难发生后在确定的时间内可以恢复和继续运营的过程

灾难恢复是指将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态的活动流程

访问控制是在保障授权用户能获取所需资源的同时拒绝非授权用户的安全机制，是信息安全理论基础重要组成部分

计算机病毒是一个能够通过修改程序，把自身复制进去，进而去传染其他程序的程序

漏洞是指硬件、软件或策略上存在的安全缺陷，从而使攻击者能够在未来授权的情况下访问、控制系统

公开密钥密码体制是为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全的媒体上的通信双方交换信息，安全达成一致的密钥，也叫非对称加密算法

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
PKI是一个用公钥密码算法原理和技术来提供安全服务的通用性基础平台，用户可以利用PKI平台提供的安全服务进行安全通信

数字证书是标志通信各方身份的数据，是一种安全发公钥的方式

防火墙指的是隔离在本地网络与外界网络之间执行访问控制策略的一道防御系统

DMZ（中文名隔离区，也称非军事区）是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区

入侵检测是通过计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象，并对此做出适当反应的过程

VPN（虚拟专用网）指的是依靠ISP和其他NSP在公用网络中建立虚拟的专用数据通信网路的技术

信息系统
：是指基于计算机技术和网络通信技术的系统，是人、规程、数据库、硬件和软件等各种设备、工具的有机集合。

信息安全：是指信息网络的硬件、软件及其系统中的数据得到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露、系统连续、可靠、正常地运行，信息服务不中断。

简答：

1、 什么是PDRR模型？请说明它在信息安全整体解决方案中的作用。

答：PDRR模型即“信息保障”模型，作为信息安全的目标中，是由信息的保护、信息使用中的检测、信息受影响或攻击时的响应和受损后的恢复组成的。

在PDRR技术保障模型的前提下，综合信息安全管理措施，实施立体化的信息安全防护，即整体解决方案=PDRR模型+安全管理。 2、
网络安全与信息安全的关系？

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
答：信息安全是指信息在整个生命周期中需要保持机密性、完整性和可用性，即“CIA”特性；也包括了保证信息在网络环境中的安全性。网络安全指的是通过各种技术或设备，保证网络环境的持续、可靠、安全的运行，为信息安全提供平台的保证。因此，网络安全只是信息安全范畴中的一部分。 3、
网络攻击的途径有哪些？

答：网络攻击的途径可分为以下几种“

针对端口攻击；针对服务攻击；针对第三方软件攻击；DoS攻击；针对系统攻击；口令攻击；欺骗。

4、 什么是业务流分析？它有什么危害？

答：业务流分析是通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。威胁信息安全。 5、
什么是安全机制？什么是安全服务？请简述两者间的关系。

答：安全机制：一种安全策略可以使用不同的机制来实施，或单独使用，或联合使用取决于该策略的目的以及使用的机制。安全机制是具体化了的策略要求。
安全服务：由参与通信的开放系统的层所提供的服务，它确保该系统或数据传送具有足够的安全性。安全服务是功能性的，具有可操作性。
一种安全服务可以通过某种安全机制单独提供，也可以通过多种安全机制联合提供；同一种安全机制也可用于提供一种或多种安全服务。每层的安全服务依赖于该层所配置的安全机制。安全机制是服务得到实现的保证。 6、
请简要说明灾难备份三要素的含义。

答：灾难备份必须满足的三个要素：一是系统中的部件、数据都具有冗余性，即一个系统发生故障，另一个系统能够保持数据传送的顺畅；
二是具有长距离性，因为灾难总是在一定范围内发生，因而保持足够长的距离才能保证数据不会被同一个灾害全部破坏；

三是灾难备份系统追求全方位的数据复制。 7、
请简述访问控制的概念及工作原理

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html
答：访问控制是在保障授权用户能获取所需资源的同时拒绝非授权用户的安全机制，是信息安全理论基础的重要组成部分。
工作原理：在用户身份认证和授权之后，访问控制机制将根据预先设定的规则对用户访问某项资源进行控制，只有规则允许时才能访问，违反预定的安全规则的访问行为将被拒绝。 8、 请简要介绍网络扫描的一般过程。
答：第一阶段：发现目标主机或网络

第二阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务以及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

第三阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。 9、 请简述对称密钥密码体制的概念与优缺点。

答：对应对称密钥的密钥管理体制称为对称密钥密码体制，也称单钥密码体制。优点是安全性高，加、解密速度快。缺点是进行保密通信之前，双方必须通过安全信道传送所用的密钥，这对于相距较远的用户可能要付出较大的代价，甚至难以实现。 10、 请简单比较NIDS和HIDS的两种技术。

11、请简述VPN的概念、协议和工作原理 答：概念如名词解释。 协议：隧道协议
工作原理：

用心打造免费、绿色、专业、海量的教育文库网站 www.wenku1.com

本文档来源于第一文库网：https://www.wenku1.com/news/143E265E4FD0160A.html

**相关文档：**


- 信息安全概论课后答案
- 信息安全导论答案
- 信息安全技术课后答案
- 信息安全导论论文
- 信息安全意识培训答案
- 信息安全管理考试答案
- 信息安全管理答案
- 信息安全技术答案
- 信息安全导论试题
- 信息技术与信息安全公需科目考试答案


**更多相关文档请访问：https://www.wenku1.com/**