信息安全工程师真题分类详解

2020-5 版

我能过软考出品

www.wngrk.com

淘宝二维码

微信公众号: 我能过软考

微信：wngrk666

QQ 66728193

PMP 免费交流 QQ 群：201994795

高项免费交流群 Q 群　　211890902

信息安全工程师免费交流群 523124613

第一部分 综合知识真题分类解析

第 1 章　信息安全基础

考点：信息安全概念

考点：信息安全法律法规

【2018 年上半年试题 1】

2016 年 11 月 7 日,十二届全国人大常委会第二十四次会议以 154 票赞成,1 票弃权,表决通过了《网络安全法》。该法律由全国人民代表大会常务员会于 2016 年 11 月 7 日发布,自（ ）起施行。

A.2017 年 1 月 1 日　　B.2017 年 6 月 1 日

C.2017 年 7 月 1 日　　D.2017 年 10 月 1 日

我能过软考分析：

本题取自于当年的网络安全重要事件，知道即可。《网络安全法》由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布，自 2017 年 6 月 1 日起实施。

参考答案

（1）B

2018 年上半年试题 5

《网络安全法》明确了国家落实网络安全工作的职能部门和职责，其中明确规定由（ ）负责统筹协调网络安全工作和相关监督管理工作。

A.中央网络安全与信息化小组　　B.国务院

C.国家网信部门　　D.国家公安部门

我能过软考分析：

本题在书中的第 19 页，也是当年的热点问题。《中华人民共和国网络安全法》第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

参考答案

（5）C

考点：信息安全管理基础

考点：信息安全标准化知识

2017 年上半年试题 2

《计算机信息系统安全保护等级划分准则》（GB17859——1999）中规定了计算机系统安全保护能力的五个等级，其中要求对所有主体和客体就行自助和强制访问控制的是（ ）。

A.用户自助保护级　　B.系统审计保护级

C.安全标记保护级　　D.结构化保护级

我能过软考分析：

本题在书中第 35-38 页，五个保护等级分别为用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级，随着级别的提高，计算机信息系统安全保护能力逐渐增强。结构化保护级要求对所有主体和客体进行自主和强制访问控制。本题同样知识点的题目在 18 年也进行了考查，需要引起重视。

参考答案

D

2018 年上半年试题 2

近些年,基于标识的密码技术受到越来越多的关注,标识密码算法的应用也得到了快速发展,我国国密标准中的标识密码算法是（ ）。

A. SM2　　B. SM3　　C. SM4　　D. SM9

我能过软考分析：

本题在教材中并未出现，只是在教材第 28 页，列明了无线局域网产品需要使用的系列密码算法。SM9 标识密码算法是一种基于双线性对的标识密码算法，它可以把用户的身份标识用以生成用户的公、私密钥对,主要用于数字签名、数据加密、密钥交换以及身份认证等；SM9 密码算法的密钥长度为 256 位，SM9 密码算法的应用与管理不需要数字证书、证书库或密钥库.该算法于 2015 年发布为国家密码行业标准(GM/T 0044-2016)。SM2 是国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法。SM3 是中华人民共和国

政府采用的一种密码散列函数标准。SMS4 算法是在国内广泛使用的 WAPI 无线网络标准中使用的对称加密算法。

参考答案

（2）D

2018 年上半年试题 3

《计算机信息系统安全保护等级划分准则》(GB17859-1999)中规定了计算机系统安全保护能力的五个等级，其中要求对所有主体和客体进行自主和强制访问控制的是（ ）。

A.用户自主保护级　　B.系统审计保护级

C.安全标记保护级　　D.结构化保护级

我能过软考分析：

本题在书中第 35-38 页，五个保护等级分别为用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级，随着级别的提高，计算机信息系统安全保护能力逐渐增强。安全标记保护级主要特征是计算机信息系统可信计算基对所有主体及其所控制的客体(例 如:进程、文件、段、设备)实施强制访问控制。而结构化保护级在第三级实施的自主和强制访问控制的基础上，进一步拓展到所有主体和客体。

参考答案

（3）D

考点：信息安全专业英语

1. 2018 年上半年试题 71-75

Trust is typically interpreted as a subjective belief in the reliability, honesty and security of an entity on which we depend （71） our welfare .In online environments we depend on a wide spectrun of things , ranging from computer hardware,software and data to people and organizations. A security solution always assumes certain entities function according to specific policies.To trust is precisely to make this sort of assumptions , hence , a trusted entity is the same as an entity that is assumed to function according to policy . A consequence of this is that a trust component of a system must work correctly in order for the security of that system to hold, meaning that when a trusted（72） fails , then the sytems and applications that depend on it can （73） be considered secure . An often cited articulation of this principle is: " a trusted system or component is one that can break your security policy" (which happens when the trust system fails). The same applies to a trusted party such as a service provider (SP for short)that is , it must operate according to the agreed or assumed policy in order to ensure the expected level of securty and quality of services . A paradoxical conclusion to be drawn from this analysis is that security

assurance may decrease when increasing the number of trusted components and parties that a service infrastructure depends on . This is because the security of an infrastructure consisting of many Trusted components typically follows the principle of the weakest link , that is ,in many situations the the overall security can only be as strong as the least reliable or least secure of all the trusted components. We cannot avoid using trusted security components,but the fewer the better. This is important to understand when designing the identity management architectures,that is, fewer the trusted parties in an identity management model , stronger the security that can be achieved by it .

The transfer of the social constructs of identity and trust into digital and computational concepts helps in designing and implementing large scale online markets and communities,and also plays an important role in the converging mobile and Internet environments . Identity management (denoted Idm hereafter) is about recognizing and verifying the correctness of identitied in online environment .Trust management becomes a component of （ ） whenever different parties rely on each other for identity provision and authentication . IdM and Trust management therefore depend on each other in complex ways because the correctness of the identity itself

must be trusted for the quality and reliability of the corresponding entity to be trusted. IdM is also an essential concept when defining authorisation policies in personalised services.

Establishing trust always has a cost , so that having complex trust requirement typically leads to high overhead in establishing the required trust . To reduce costs there will be incentives for stakeholders to "cut corners" regarding trust requirements ,which could lead to inadequate security . The challenge is to design IdM systems with relatively simple trust requirements.Cryptographic mechanisms are often a core component of IdM solutions,for example,for entity and data authentication.With cryptography,it is often possible to propagate trust from where it initially exists to where it is needed .The establishment of initial（ ）usually takes place in the physical world,and the subsequent propagation of trust happens online,often in an automated manner.

71.A.with	B. on	C. of	D. For
72.A.entity	B.person	C.component	D.thing
73.A. No longer	B. never	C. always	D.often
74.A. SP	B. IdM	C.Internet	D.entity

75.A.trust　　B.cost　　C.IdM　　D. solution

原文翻译

信任通常被理解为对我们赖以生存的实体的可靠性,诚实性和安全性的主观信念在网络环境中，我们依赖于各种各样的东西，从计算机硬件、软件和数据到人员和组织。安全解决方案总是根据特定的信任来假定某些实体的功能。因此，要实现这种假设，受信任的实体与假定根据策略工作的实体是相同的。其结果是为了保证系统的安全性，系统的信任组件必须正确工作，这意味着当可信实体不再可信时，依赖它的和应用程序就永远不能被认为是安全的。常被引用的此原则的另一项原则是：“受信任的系统或组件可以破坏您的安全策略”(当信任系统不再适用时会发生这种情况)。这同样适用于受信任的方，例如服务提供者(简称 SP)，即它必须按照商定或假定的政策运作，以确保预期的服务水平和服务质量。从这一分析中可以得出的另一结论是，当增加服务基础结构所依赖的受信任组件和各方的数量时，安全保证可能会下降。这是因为由多个受信任的组件组成的基础设施的安全性通常遵循最弱环节的原则，也就是说，在许多情况下，总体安全可能 仅与所有受信任组件中最不可靠或最不安全的组件一样。我们不能避免使用可信的安全组件，但越少越好。在设计身份管理体系结构时，这一点很重要，也就是说，使用统一的一个身份管理模型，可以增强了实现的安全性。

将身份和信任的社会结构转化为数字和数值概念，有助于设计和实施大规模的在线市场和社区，同时也起到了重要的作用。在移动和互联网环境中扮演重要角色。身份管理（以下简称 IDM）是指在网络环境下识别和验证身份识别

的正确性。信任管理成为身份管理的一个组件，每当不同的各方在身份提供和身份验证方面相互依赖时。因此，信任管理与信任管理在信任管理中相互依赖。 因为身份本身的正确性必须是可信的，因此对应实体的质量和可靠性也是定义身份管理的一个基本概念。

建立信任总是有代价的，因此复杂的信任需求通常会导致建立所需信任的高开销。为了降低成本，会有激励措施。 对信任要求“走捷径”，这可能导致安全性不足。我们面临的挑战是如何设计具有相对简单信任度的辅助系统。机制通常是解决方案的核心组件，例如，对于实体和数据来说，从最初存在的地方到新的地方，信任是可能的。 初始信任的建立通常发生在物理世界，随后信任的传播发生在网上，通常是自动化的。

我能过软考分析：

71 题考查 depend on 的介词固定搭配。

72 题考查上下文的匹配，前文讲述的都是关于实体。

73 题考查对内容的理解，当假设不再成立，那么就不可能是安全的。

74 题本段主要讲述身份管理的内容，根据上下文应当选择 IDM。

75 题根据上下文能够知道，这里讲的是信任。

参考答案

（71）B（72）A（73）B（74）B（75）A

第 2 章 密码学基础

考点：密码学与信息安全基础

1. 2018 年上半年试题 6

一个密码系统如果用 E 表示加密运算，D 表小解密运算，M 表示明文,C 表示密文,则下面描述必然成立的是（ ）。

A. E(E(M))=C　　B. D(E(M))=M

C. D(E(M))=C　　D. D(D(M))=M

我能过软考分析：

本题对书中 77 页的密码体制进行考察，加解密运算是一对逆运算，先对 M 进行 E 加密变换为密文，再进行 D 解密还原为明文 M。

参考答案

（6）B

2. 2018 年上半年试题 14

如果未经授权的实体得到了数据的访问权，这属于破坏了信息的（ ）。

A.可用性　　B.完整性　　C.机密性　　D.可控性

我能过软考分析：

本题考查教材 75 页，信息安全的基本属性，信息安全的基本属性贯穿整个课程始终，具有很重要的意义，一定要认真掌握。保密性是指网络信息不被泄露给非授权的用户、实体或过程，即信息只为授权用户使用。

参考答案

（14）C

3. 2018 年上半年试题 50

网络系统中针对海量数据的加密,通常不采用（ ）方式。

A.会话加密　　B.公钥加密　　C.链路加密　　D.端对端加密

我能过软考分析：

本题考查在网络中各个层加密的特点。公钥加密加密算法复杂且加解密效率低，一般只适用于少量数据的加密。会话加密是在应用层按照会话到会话的方式进行加密。端到端加密是传输层之间加密的方式。链路加密是在链路到链路之间也就是两个交换机之间就需要加解密的方式。

参考答案

（50）B

4. 2017 年上半年试题 3

1949 年，（ ）发表了题为《保密系统的同学理论》的文字，为密码技术的研究奠定了理论基础，由此密码学成了一门科学。

A.Shannon　　B.Diffie　　C.Hellman　　D.Shamir

我能过软考分析：

1949 年 Shannon 发表了《保密系统的通信理论》一文，为私钥密码系统建立了理论基础，从此密码学成为一门科学。香浓的信息论是密码学的基础。

参考答案

（3）A

5. 2017 年上半年试题 5

凯撒密码体制是一种代表性的古典密码算法，在凯撒密码体制中，设置钥参数 k = 3，一次对密文“zhongguo”进行加密，则相应的密文为（ ）。

A.ckrqjjxr B.cdrqijxr C.akrajjxr D.ckrqiixr

我能过软考分析：

本题考查教材 79 页关于古典密码的内容。将明文“zhongguo”中的字母依次往后移 3 位，得到密文“ckrqjjxr ”

参考答案

（5）A

6. 2017 年上半年试题 39

在非安全的通信环境中，为了保证消息来源的可靠性，通常采用的安全防护技术是（ ）。

A.信息隐蔽技术 B.数据加密技术C.消息认证技术D.数据水印技术

我能过软考分析：

消息认证就是验证消息的完整性，当接收方收到发送方的报文时，接收方能够验证收到的报文是真实的和未被篡改的。它包含两层含义：一是验证信息的发送者是真正的而不是冒充的，即数据起源认证；二是验证信息在传送过程中未被篡改、重放或延迟等。信息隐藏技术和数据加密技术都是用来保证保密性。数据水印技术常用于数据版权保护。

参考答案

（39）C

7. 2016 年下半年试题 29

以下关于加密技术的叙述中，错误的是（ ）。

A.对称密码体制的加密密钥和解密密钥是相同的

B.密码分析的目的就是千方百计地寻找密钥或明文

C.对称密码体制中加密算法和解密算法是保密的

D.所有的密钥都有生存周期

我能过软考分析：

本题考查的是对密码学基本原理的理解。对于一个好的密码体制，其安全强度应该不依赖密码体制本身的保密，而只依赖于密钥。

参考答案

（29）C

8. 2016 年下半年试题 39

信息通过网络进行传输的过程中，存在着被篡改的风险，为了解决这一安全隐患，通常采用的安全防护技术是（ ）。

A.加密技术　　B.匿名技术

C.消息认证技术　　D.数据备份技术

我能过软考分析：

消息认证就是验证消息的完整性，当接收方收到发送方的报文时，接收方能够验证收到的报文是真实的和未被篡改的。这道题和 2017.39 题实质上是一样的。

参考答案

（39）C

考点：密码攻击

1. 2018 年上半年试题 4

密码分析者针对加解密算法的数学基础和某些密码学特性,根据数学方法破译密码的攻击方式称为（ ）。

A.数学分析攻击　　B.差分分析攻击

C.基于物理的攻击　　D.穷举攻击

我能过软考分析：

本题考查教材 78 页，对于密码的分析，数学分析攻击是指密码分析者针对加解密算法的数学基础 和某些密码学特性，通过数学求解的方法来破译密码。其他三种攻击也需要大概了解，差分分析是在 DES 时代提出的，DES 算法可以抵御差分分析攻击，基于物理的攻击是从密码实现过程物理器件的变化来进行分析。穷举攻击是依次试遍所有可能的密钥进行解密。

参考答案

（4）A

2. 2018 年上半年试题 68

如果破译加密算法所需要的计算能力和计算时间是现实条件所不具备的,那么就认为相应的密码体制是（ ）。

A.实际安全　　B.可证明安全　　C.无条件安全　　D.绝对安全

我能过软考分析：

这道题实际上在考查香浓的信息论。衡量密码体制安全性的基本准则有以下几种：

（1） 计算安全的：如果破译加密算法所需要的计算能力和计算时间是现实条件所不具备的，那么就认为相应的密码体制是满足计算安全性的。这意味着强力破解证明是安全的，即实际安全。

（2） 可证明安全的：如果对一个密码体制的破译依赖于对某一个经过深入研究的数学难题的解决，就认为相应的密码体制是满足可证明安全性的。这意味着理论保证是安全的。

（3） 无条件安全的：如果假设攻击者在用于无限计算能力和计算时间的前提下，也无法破译加密算法，就认为相应的密码体制是无条件安全性的。这意味着在极限状态上是安全的。

参考答案

（68）A

3. 2017 年上半年试题 1

根据密码分析者可利用的数据资源来分类，可将密码攻击的类型分为四类，其中密码分析者能够选择密文并获得相应明文的攻击密码的类型属于（ ）。

A.仅知密文攻击　　B.选择密文攻击

C.已知密文攻击　　D.选择明文攻击

我能过软考分析：

本题考查教材 79 页针对密码的攻击。选择密文攻击是指密码分析者能够选择密文并获得相应的明文。ABCD 四个选项攻击难度逐渐减小。

参考答案

（1）B

4. 2017 年上半年试题 7

下列技术中，不能预防重放攻击的是（ ）。

A.时间戳　　B.Nonce　　C.明文填充　　D.序号

我能过软考分析：

Nonce 是 Number used once 的缩写，Nonce 是一个只被使用一次的任意或非重复的随机数值，它跟时间戳、序号都是能够预防重放攻击的。明文填充方式不能阻止重放攻击。

参考答案

（7）C

5. 2017 年上半年试题 53

密码分析的目的是（ ）。

A.发现加密算法　　B.发现密钥或者密文对应的明文

C.发现解密算法　　D.发现攻击者

我能过软考分析：

本题考查教材 78 页，关于密码分析的目的。密码分析的目的是发现密钥或者密文对应的明文。

参考答案

（53）B

6. 2016 年下半年试题 32

密码分析学是研究密码破译的科学，在密码分析过程中，破译密文的关键是（ ）。

A.截获密文

B.截获密文并获得秘钥

C.截获密文，了解加密算法和解密算法

D.截获密文，获得秘钥并了解解密算法

我能过软考分析：

本题考查教材 78 页，关于密码分析的目的。破译密文的关键是截获密文，获得密钥并了解其解密算法。只有这三项都有的前提下才能够恢复出明文。本题与 2017 年 32 题基本相同。

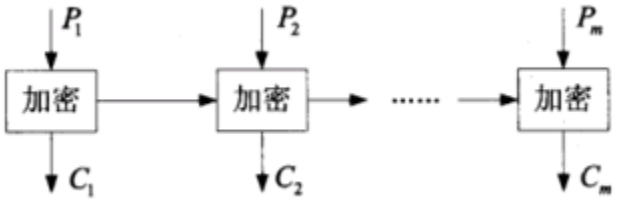
参考答案

（32）D

考点：对称密码体制与公钥密码体制

1. 2018 年上半年试题 53

分组密码常用的工作模式包括:电码本模式（ECB 模式）、密码反馈模式（CFB 模式）,密码分组链接模式（CBC 模式）,输出反馈模式（OFB 模式）。下图描述的是（ ）模式（图中 P_i 表示明文分组,C_i 表示密文分组）



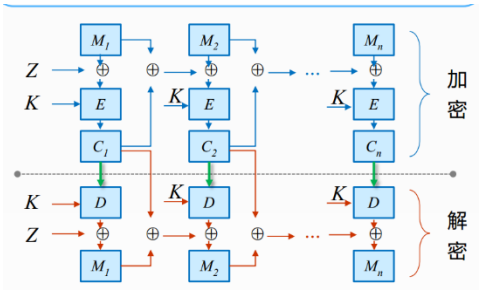
A.ECB 模式　　B.CFB 模式　　C.CBC 模式　　D.OFB 模式

我能过软考分析：

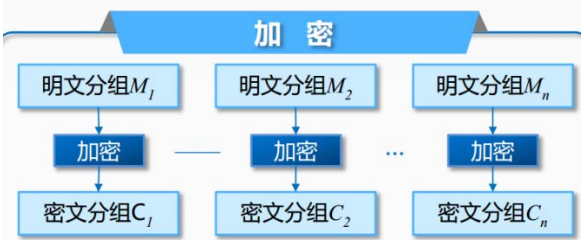
1) 本题考查了 108 页分组密码的工作模式，CBC 和 CFB 都有密文参与下一次加密。但题目中的图，把明文进行了分组,如 p1、p2，符合 CBC 的分组特点。CFB 是把分组密码转化为流密码，不强调分组。

2) OFB 是输出反馈模式，指从移位寄存器出来的信息要反馈到下一次的输入端。

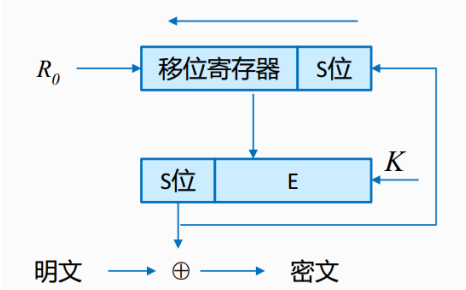
3) 四种工作模式的连接图、加解密框图、错误传播都需要掌握。



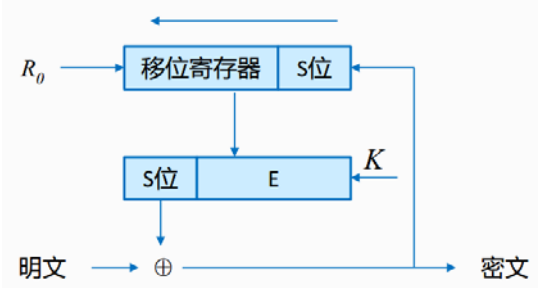
CBC



ECB



OFB



CFB

参考答案

（53）C

2. 2018 年上半年试题 54

关于祖冲之算法的安全性分析不正确的是（ ）。

A.祖冲之算法输出序列的随机性好,周期足够大

B.祖冲之算法的输出具有良好的线性、混淆特性和扩散特性

C.祖冲之算法可以抵抗已知的序列密码分析方法

D.祖冲之算法可以抵抗弱密分析

我能过软考分析：

本题考查 117 页祖冲之密码算法，祖冲之算法是我国自主研发的一种重要的序列密码算法，ZUC 算法在逻辑上采用三层结构设计，具有非常高的安全强度，能够抵抗目前常见的各种流密码攻击方法。zuc 算法本质上是一种非线性序列产生器。由此，在种子密钥的作用下，可以产生足够长的安全密钥序列。

把与密钥序列明文数据模 2 相加，便完成了数据加密。同样，把密钥序列与密文数据模 2 相加，便完成了数据解密。

参考答案

（54）B

3. 2018 年上半年试题 15

按照密码系统对明文的处理方法,密码系统可以分为（ ）。

A.对称密码系统和公钥密码系统

B.对称密码系统和非对称密码系统

C.数据加密系统和数字签名系统

D.分组密码系统和序列密码系统

我能过软考分析：

本题考查教材 77 页，密码体制的内容，按照密码系统对明文的处理方法，密码系统可以分为分组密码系统和序列密码系统。对称密码体制和非对称密码系统的区别在于能否通过加密密钥推导出解密密钥。数据加密和数字签名的区别是两种密码学技术的应用，数据加密保证了保密性，数字签名保证了不可否认性。

参考答案

（15）D

4. 2018 年上半年试题 66

下列关于公钥密码体制说法不正确的是（ ）。

A.在一个公钥密码体制中,一般存在公钥和私钥两个密钥

B.公钥密码体制中仅根据密码算法和加密密钥来确定解密密钥在计算上是可行的

C.公钥密码体制中仅根据密码算法和加密秘钥来确定解密秘钥在计算上是不可行的

D.公钥密码体制中的私钥可以用来进行数字签名

我能过软考分析：

本题考查教材 130 页，公钥密码体制。公钥体制中，一般存在公钥和私钥钥两种密钥；公钥体制中仅根据密码算法和加密密钥去确定解密密钥在计算上是不可行的；公钥体制中的公钥可以以明文方式发送；公钥密钥中的私钥可以用来进行数字签名。

参考答案

（66）B

5. 2018 年上半年试题 70

利用公开密钥算法进行数据加密时,采用的方式是（ ）。

A.发送方用公开密钥加密,接收方用公开密钥解密

B.发送方用私有密钥加密,接收方用私有密钥解密

C.发送方用公开密钥加密,接收方用私有密钥解密

D.发送方用私有密钥加密,接收方用公开密钥解密

我能过软考分析：

本题考查教材 130 页，公钥密码体制。在进行加密时，发送方用对方的公钥加密，接收方用自己的私钥解密。

参考答案

（70）C

6. 2017 年上半年试题 4

（ ）属于对称加密算法。

A. ELGamal　　B. DES　　C. MD5　　D. RSA

我能过软考分析：

本题考查的是常见密码算法的分类。DES 是一种典型的分组密码，属于对称加密算法。其余三种分别是公钥密码算法、杂凑函数、公钥密码算法。

参考答案

（4）B

7. 2017 年上半年试题 56

下列关于公钥体制中说法不正确的是（ ）。

A.在一个公钥体制中，一般存在公钥和密钥两种密钥

B.公钥体制中仅根据加密密钥去确定解密密钥在计算机上是可行的

C.公钥体制中的公钥可以以明文方式发送

D.公钥密钥中的私钥可以用来进行数字签名

我能过软考分析：

本题考查教材 130 页，公钥密码体制的理解。公钥体制中，一般存在公钥和私钥钥两种密钥；公钥体制中仅根据加密密钥去确定解密密钥在计算上是不可行的；公钥体制中的公钥可以以明文方式发送；公钥密钥中的私钥可以用来进行数字签名。

参考答案

（56）B

8. 2017 年上半年试题 65

SM4 是一种分组密码算法，其分组长度和密钥长度分别为（ ）。

A.64 位和 128 位　　B.128 位和 128 位

C.128 位和 256 位　　D.256 位和 256 位

我能过软考分析：

本题实际上是考察 SM4 算法，SM4 是一种分组密码算法，也是我国公关部的第一批商用密码算法，因此才会在教材中提及和考查。其分组长度和密钥长度分别为 128 位和 128 位。

参考答案

（65）B

9. 2016 年下半年试题 4

（ ）不属于对称加密算法。

A.IDEA　　B.DES　　C.RC5　　D.RSA

我能过软考分析：

本题考查对常见密码算法的分类。IDEA、DES、RC5 都属于对称加密算法，RSA 属于非对称加密算法。

参考答案

（4）D

10. 2016 年下半年试题 6

如果发送方使用的加密密钥和接收方使用的解密秘钥不相同，从其中一个秘钥难以推出别一个秘钥，这样的系统称为（ ）。

A.公钥加密系统　　B.单秘钥加密系统

C.对称加密系统　　D.常规加密系统

我能过软考分析：

本题考查教材 130 页对公钥密码算法的理解。公钥加密系统又称之为非对称加密系统，其使用的加密密钥和解密密钥不同，从其中的一个密钥难以推出另一个密钥。

参考答案

（6）A

11. 2016 年下半年试题 15

按照密码系统对明文的处理方法，密码系统可以分为（ ）。

A.置换密码系统和易位密码系统

B.密码学系统和密码分析学系统

C.对称密码系统和非对称密码系统

D.分组密码系统和序列密码系统

我能过软考分析：

本题考查 85 页，对分组密码系统和序列密码的区分。按照密码系统对明文的处理方法，密码系统可以分为分组密码系统和序列密码系统。

参考答案

（15）D

12. 2016 年下半年试题 33

利用公开密钥算法进行数据加密时，采用的方式是（ ）。A.发送方用公开密钥加密，接收方用公开密钥解密

B.发送方用私有密钥加密，接收方用私有密钥解密

C.发送方用公开密钥加密，接收方用私有密钥解密

D.发送方用私有密钥加密，接收方用公开密钥解密

我能过软考分析：

本题考查 130 页，对公钥密码系统的理解。在进行加密时，发送方用对方的公钥加密，接收方用自己的私钥解密。

参考答案

（33）C

13. 2016 年下半年试题 50

网络系统中针对海量数据的加密，通常不采用（ ）方式。

A.链路加密　　B.会话加密　　C.公钥加密　　D.端对端加密

我能过软考分析：

本题实际上在考查对第二章知识的理解，公钥加密加密算法复杂且加解密效率低，一般只适用于少量数据的加密。链路加密、会话加密和端到端加密是指在数据链路层、应用层和传输层的加密方式。

参考答案：

（50）C

考点：DES 算法教材 86-94 页

DES 算法是一种极其重要的分组密码算法，在密码学发展中有极其重要的地位。关于 DES 算法的各个部分设计的方法、存在的问题都是需要掌握的部分，对于基础比较好的同学，可以自己实现一下 DES 算法，加深对这个部分的理解。

1. 2018 年上半年试题 26

已知 DES 算法 S 盒如下:

°	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

如果该 S 盒的输入为 100010,则其二进制输出为（ ）。

A.0110　　B.1001　　C.0100　　D.0101

我能过软考分析：

本题考查的是一个 S 盒查表的方法，如果增加难度，可以给一个每行空一格的 S 盒，先自己补全 S 盒，而后进行查表。已知 S 盒的输入为 100010，取其输入第一位和第六位数字为 S 盒的行 10，即第 2 行，中间四位为 S 盒的列 0001，即第 1 列，在 S 盒中查到第 2 行和第 1 列交叉的数字为 6，其二进制输出为 0110。

参考答案

（26）A

2. 2018 年上半年试题 35

在 DES 加密算法中,子密钥的长度和加密分组的长度分别是（ ）。

A.56 位和 64 位　　B.48 位和 64 位

C.48 位和 56 位　　D.64 位和 64 位

我能过软考分析：

DES 算法的密钥分组长度为 64 位，经过置换选择 1、循环左移、置换选择 2 等变换，产生 16 个 48bit 的子密钥，被加密的分组长度为 64 位。在 DES 算法设计的过程中，充分考虑的奇偶校验的问题，就带来了很多 64 位、56 位和 48 位的问题，可以做一个归纳。

参考答案

（35）B

3. 2016 年下半年试题 26

已知 DES 算法 S 盒如下：

°	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

如果该 S 盒的输入 110011，则其二进制输出为（ ）。

A. 0110　　B. 1001　　C. 0100　　D. 0101

我能过软考分析：

已知 S 盒的输入为 110011，取其输入第一位和第六位数字为 S 盒的行 11，即第 3 行，中间四位为 S 盒的列 1001，即第 9 列，在 S 盒中查到第 3 行和第 9 列交叉的数字为 4，其二进制输出为 0100。这道题和 2018 年 26 题是一致的。

参考答案

（26）C

4. 2016 年下半年试题 35

在 DES 加密算法中，密钥长度和被加密的分组长度分别是（ ）。

A.56 位和 64 位　　B.56 位和 56 位

C.64 位和 64 位　　D.64 位和 56 位

我能过软考分析：

DES 算法的密钥分组长度为 64 位，除去 8 位校验位，实际密钥长度为 56 位，被加密的分组长度为 64 位。本题和 2018 年 35 题要做一个区分 2018 年考察的是子密钥。

参考答案

（35）A

5. 2016 年下半年试题 65

两个密钥三重 DES 加密：$c=E_{K1}[D_{K2}[E_{K1}[p]]$，K1≠K2 其有效的密钥长度为（ ）。

A. 56　　B.128　　C.168　　D.112

我能过软考分析：

两个密钥三重 DES 的有效密钥长度为 112 位。涉及两个密钥 K1，K2，实现三次加密，分别用 K1 加密，K2 解密，K1 再加密。有效密钥为 2*56=112 位。

参考答案

（65）D

6. 2016 年下半年试题 70

在 DES 算法中，需要进行 1 6 轮加密，每一轮的子密钥长度为（ ）位。

A.16　　B.32　　C.48　　D.64

我能过软考分析：

DES 算法中，64 位密钥经过置换选择 1、循环左移、置换选择 2 等变换，产生 16 个 48 位长的子密钥。

参考答案

（70）C

考点：AES 算法（教材 95-102 页）

AES 算法也是一个很重要的分组密码算法，在 DES 发展一段时间以后，其 56 位密钥的安全性受到了威胁，也无法证明其没有后门，因此就出现了一种新的商用密码标准 AES 算法，他用求逆的方式来设计 S 盒，在具体实现中也是通过查表的方式实现的，但是多项式求逆的方法是需要掌握的内容。

1. 2016 年下半年试题 68

AES 结构由以下 4 个不同的模块组成，其中（ ）是非线性模块。

A.字节代换　　B.行移位　　C.列混淆　D.轮密钥加

我能过软考分析：

AES 算法中的 S 盒变换是按字节进行的代替变换，又称之为字节代换。线性模块与非线性模块在密码学中也是比价重要的概念，但从考题看，没有考查线性与非线性模块的概念，只是考察了算法中线性非线性的模块。

参考答案

（68）A

考点：RSA 算法（教材 134-136 页）

RSA 算法是公钥密码算法中的重要算法，整个过程都需要掌握，考试中考查的基本上以计算题目为主。可以自己按照算法进行一遍计算增加自己的印象。

1. 2016 年下半年试题 69

67 mod 119 的逆元是（ ）。

A.52　　B.67　　C.16　　D.19

我能过软考分析：

本题考查了逆元的概念，关于逆元在书中求解 67*X≡1 mod 119，得出 X=16。在这种考试中我们可以通过带入答案的方法，希望同学们也按照辗转相除法进行一下练习。**或者参见 RSA 讲解视频。**

参考答案

（69）C

2. 2018 年上半年试题 65

设在 RSA 的公钥密码体制中,公钥为(e,n)=(7，55),则私钥 d=（ ）。

A.11　　B.15　　C.17　　D.23

我能过软考分析：

已知 n=55，则可推断ρ（n）=（5-1）*（11-1）=40，则 d*e≡1 mod 40，算出 d=23。

参考答案

（65）D

3. 2018 年上半年试题 69

a=17,b=2,则满足 a 与 b 取模同余的是（ ）。

A.4　　B.5　　C.6　　D.7

我能过软考分析：

两个整数 a、b，若它们除以整数 m 所得的余数相等，则称 a 与 b 对于模 m 同余或 a 同余于 b 模 m，记作 a≡b (mod m)，即求解 17≡2（mod m），m=5。同余运算是 RSA 密码算法中很重要的运算，需要掌握，难度不大。

参考答案

（69）B

4. 2017 年上半年试题 66

设在 RSA 的公钥密码体制中，用于为（e，n）=（7,55），则私钥 d=（ ）。

A.8　　B.13　　C.23　　D.37

我能过软考分析：

由 n=55 得出，ρ（n）=（p-1）*（q-1）=（5-1）*（11-1）=40，求解（7*d-1）mod 40 使其等于 0，将下列选项代入可得，d=23。本题和 2018 年 66 题相同。

参考答案

（66）C

5. 2016 年下半年试题 66

设在 RSA 的公钥密码体制中，公钥为(e，n)=(13，35)，则私钥 d=（ ）。

A.11　　B.13　　C.15　　D.17

我能过软考分析：

已知 n=35，则可推断ρ（n）=（5-1）*（7-1）=24，则 d*e≡1 mod 24，算出 d=13。

参考答案

（66）B

考点：其他公钥密码算法

1. 2018 年上半年试题 62

对于定义在 GF(p)上的椭圆曲线,取素数 P=11,椭圆曲线 $y^2=x^3+x+6 \bmod 11$,则以下是椭圆曲线 11 平方剩余的是（ ）。

A. x=1 B. x=3 C. x=6 D. x=9

我能过软考分析：

本题考查 138 页椭圆曲线算法，首先应了解平方剩余；假设 p 是素数，a 是整数。 如果存在一个整数 y 使得 y^2≡a(mod p) （即 y^2-a 可以被 p 整除）， 那么就称 a 在 p 的剩余类中是平方剩余的。

根据这个定义，将选项值进行代入运算可知，当 x=3，y^2≡36（mod 11），此时 y 的值可为 5 或 6；其余选项都是不满足平方剩余条件的。椭圆曲线的计算对基础知识的要求比较高，对于这样的题目，采用代入法即可。

参考答案

（62）B

考点：杂凑函数

这个部分实际计算是比较麻烦的，实际考试中，基本集中在考查具体的数值上，如分组长度与输出长度，在下午的考试中，常出现在认证的考点中。

1. 2018 年上半年试题 67

SM3 密码杂凑算法的消息分组长度为（ ）比特。

A.64 B.128 C.512 D.1024

我能过软考分析：

本题考查教材 126 页，SM3 密码算法。SM3 算法是国家密码管理局于 2010 年的安全密码杂凑算法。其基本迭代结构采用 了增强型的 Merk1e-Damgård 结构;压缩函数包含消息扩展和压缩主函数两个部分，压缩主函数采

用了非对称 Feistel 结构。其消息分组长度为 512 位，输出为 256 位。

参考答案

（67）C

2. 2017 年上半年试题 35

SHA1 算法的消息摘要长度是（ ）位。

A.128 B.160 C.256 D.512

我能过软考分析：

本题考查教材 121 页。SHA1 算法将任意长度的明文加密成固定长度为 160 位的消息摘要。

参考答案

（35）B

3. 2016 年下半年试题 67

杂凑函数 SHA-1 的输入分组长度为（ ）比特。

A.128 B.256 C.512 D.1024

我能过软考分析：

本题考查教材 121 页。SHA-1 算法对输入按 512 位进行分组，并以分组为单位进行处理。

参考答案

（67）C

考点：密码学应用

密码学的应用包括数字签名、认证、数字信封（PGP 协议）、数字证书应用等多种形式。在此没有将每个部分详细分解开。希望大家能从一个整体的角度掌握，可以考虑自己分析一下 PGP 协议，了解实际使用的方法和过程。

这个部分需要重点说明的是关于数字证书与 PKI 的部分，这些内容在各个部分中都有所散落。这个部分希望大家还是根据张老师的课程进行学习，学有余力可以参照信息安全概论教材的内容，进行系统学习。

数字信封技术实际上就是以 PGP 技术为代表的利用公钥密码算法不需要事先共享信息及对称密码算法加密速度快的特点，使用公钥密码对对称密码算法的密钥进行加密，而后使用对称密码算法对数据进行加密。把握这一点就很容易理解数字信封技术了。

1. 2018 年上半年试题 11

以下关于认证技术的描述中，错误的是（ ）。

A.身份认证是用来对信息系统中实体的合法性进行验证的方法

B.消息认证能够验证消息的完整性

C.数字签名是十六进制的字符串

D.指纹识别技术包括验证和识别两个部分

我能过软考分析：

本题考查教材 146 页，数字签名的概念。数字签名与手写签名类似，只不过手写签名是模拟的，因人而异。数字签名是 0 和 1 的数字串，因消息而异。

参考答案

（11）C

2. 2018 年上半年试题 16

数字签名是对以数字形式存储的消息进行某种处理,产生一种类似于传统手书签名功效的信息处理过程,实现数字签名最常见的方法是（ ）。

A.数字证书和 PKI 系统相结合

B.对称密码体制和 MD5 算法相结合

C.公钥密码体制和单向安全 Hash 函数算法相结合

D.公钥密码体制和对称密码体制相结合

我能过软考分析：

本题考查教材 146 页，数字签名的概念。数字签名可以利用公钥密码体制、对称密码体制或者公证系统来实现。最常见的的实现方法是建立在公钥密码体制和单向安全散列函数算法的组合基础之上。

参考答案

（16）C

3. 2018 年上半年试题 17

以下选项中,不属于生物识别方法的是（ ）。

A.掌纹识别　　B.个人标记号识别　　C.人脸识别　　D.指纹识别

我能过软考分析：

本题考查教材 156 页生物特征识别的问题，生物特征识别的唯一性和稳定性的要求以及验证和辨识两类技术都需要了解。对一个人进行识别时，主要个人特征认证技术有：指纹识别、声音识别、笔记识别、虹膜识别和手形等。

参考答案

（17）B

4. 2018 年上半年试题 31

以下关于数字证书的叙述中,错误的是（ ）。

A.证书通常携带 CA 的公开密钥

B.证书携带持有者的签名算法标识

C.证书的有效性可以通过验证持有者的签名验证

D.证书通常由 CA 安全认证中心发放

我能过软考分析：

数字证书通常包含用户身份信息、持有者的签名算法标识、公开密钥以及 CA 的数字签名信息等。

参考答案

（31）A

5. 2018 年上半年试题 32

2017 年 11 月,在德国柏林召开的第 55 次 ISO/IEC 信息安全分技术委员会(SC27)会议上,我国专家组提出的（ ）算法一致通过成为国际标准。

A.SM2 与 SM3　　B.SM3 与 SM4

C.SM4 与 SM9　　D.SM9 与 SM2

我能过软考分析：

2017 年 10 月 30 日至 11 月 3 日，第 55 次 ISO/IEC 信息安全分技术委员会（SC27）会议在德国柏林召开。我国 SM2 与 SM9 数字签名算法一致通过为国际标准，正式进入标准发布阶段，这也是本次 SC27 会议上密码与安全机制工作组通过的唯一进入发布阶段的标准项目。SM2 椭圆曲线数字签名算法和 SM9 标识数字签名算法是我国国家密码管理局发布的数字签名标准。数字签名，又称电子签名，用于保证身份的真实性、数据的完整性和行为的不可否认性等，是世界各国保障网络空间安全、构建可信可控信息技术体系的密码重器。

参考答案

（32）D

6. 2018 年上半年试题 34

数字信封技术能够（ ）。

A.隐藏发送者的真实身份

B.保证数据在传输过程中的安全性

C.对发送者和接收者的身份进行认证

D.防止交易中的抵赖发生

我能过软考分析：

数字信封使用私有密钥加密算法并利用接收人的公钥对要传输的数据进行加密，以保证数据信息在传输过程中的安全性。

参考答案

（34）B

7. 2018 年上半年试题 36

甲不但怀疑乙发给他的信遭人幕改,而且怀疑乙的公钥也是被人冒充的,为了消除甲的疑虑,甲和乙需要找一个双方都信任的第三方来签发数字证书,这个第三方是（ ）。

A.注册中心 RA　　B.国家信息安全测评认证中心

C.认证中心 CA　　D.国际电信联盟 ITU

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。通信双方进行保密通信时，通常会通过双方信任的第三方认证中心 CA 来签发数字证书。

参考答案

（36）C

8. 2018 年上半年试题 39

信息通过网络进行传输的过程中,存在着被慕改的风险,为了解决这一安全隐患通常采用的安全防护技术是（ ）。

A.信息隐藏技术 B.数据加密技术 C.消息认证技术 D.数据备份技术

我能过软考分析：

消息认证就是验证消息的完整性，当接收方收到发送方的报文时，接收方能够验证收到的报文是真实的和未被篡改的。

参考答案

（39）C

9. 2018 年上半年试题 7

S/key 口令是一种一次性口令生成方案，它可以对抗（ ）。

A.恶意代码攻击 B.暴力分析攻击 C.重放攻击 D.协议分析攻击

我能过软考分析：

一次一密指在流密码当中使用与消息长度等长的随机密钥,密钥本身只使用一次。重放攻击又称重播攻击或回放攻击，是指攻击者发送一个目的主机已接收过的包，特别是在认证的过程中，用于认证用户身份所接收的包，来达到欺骗系统的目的。一次一密这样的密钥形式可以对抗重放攻击。

参考答案

（7）C

10. 2018 年上半年试题 60

在 PKI 中,关于 RA 的功能,描述正确的是（ ）。

A.RA 是整个 PKI 体系中各方都承认的一个值得信赖的、公正的第三方机构

B.RA 负责产生,分配并管理 PKI 结构下的所有用户的数字证书,把用户的公钥和用户的其他信息绑在一起,在网上验证用户的身份

C.RA 负责证书废止列表 CRL 的登记和发布

D.RA 负责证书申请者的信息录入,审核以及证书的发放等任务,同时,对发放的证书完成相应的管理功能

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。

RA(Registration Authority)，数字证书注册审批机构。RA 系统是 CA 的证书

发放、管理的延伸。它负责证书申请者的信息录入、审核以及证书发放等工作(安全审计)。同时，对发放的证书完成相应的管理功能(安全管理)。

参考答案

（60）D

11. 2017 年上半年试题 16

数字签名是对以数字形式存储的消息进行某种处理，产生一种类似于传统手书签名功效的信息处理过程，一个数字签名体制通常包括两个部分（ ）。

A.施加签名和验证签名　　B.数字证书和身份认证

C.身份消息加密和解密　　D.数字证书和消息摘要

我能过软考分析：

本题考查教材 146 页，数字签名的概念。数字签名体制通常包括两个部分，即：施加签名和验证签名。

参考答案

（16）A

12. 2017 年上半年试题 17

身份识别在信息安全领域有着广泛的应用，通过识别用户的生理特征来认证用户的身份是安全性很高的身份认证方法。如果把人体特征用于身份识别，则它应该具有不可复制的特点，必须具有（ ）。

A.唯一性和保密性　　B.唯一性和稳定性

C.保密性和可识别性　　D.稳定性和可识别性

我能过软考分析：

本题考查教材 156 页生物特征识别的问题，把人体特征要用于身份识别，则它应具有不可复制的特点，必须具有唯一性和稳定性。

参考答案

（17）B

13. 2017 年上半年试题 26

下列各种协议中，不属于身份认证协议的是（ ）。

A.S/Key 口令协议　　B.Kerberos　　C.X.509 协议　D.IPSec 协议

我能过软考分析：

Internet 协议安全性 (IPSec)是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯，不属于身份认证协议。

参考答案

（26）D

14. 2017 年上半年试题 31

下面不属于 PKI 组成部分的是（ ）。

A.证书主体　　B.使用证书的应用和系统　C.证书特威机构　　D.AS

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。PKI 的组成部分包括：证书主体、CA、RA、使用证书的应用和系统、证书权威机构等；自治系统 AS 在互联网中是一个有权自主地决定在本系统中应采用何种路由协议的小型单位，其不属于 PKI 的组成部分。

参考答案

（31）D

15. 2017 年上半年试题 36

A 方有一对密钥（KApub，KApri），B 方有一对密匙（KBpub，KBpri），A 方给 B 方发送信息 M，对信息 M 加密为：M ‘= KBpub（KApri（M））。B 方收到密文，正确的解决方案是（ ）。

A. KBpub（KApri（M ‘））　　B.KBpub（KApub（M ‘））

C.KApub（KBpri（M ‘））　　D.KBpRI（KApri（M ‘））

我能过软考分析：

接收方 B 接收到密文 M’后，首先用自己的私钥对 m’进行解密，即 KBpri（M ‘），然后再用发送方 A 的公钥 KApub 对 KBpri（M ‘）进行解密，得到 KApub（KBpri（M ‘））。

参考答案

（36）C

16. 2017 年上半年试题 49

以下关于认证技术的描述中，错误的是（ ）。

A.基于剩余特征认证一般分为验证和识别两个过程

B.身份认证是用来对信息系统中实体的合法性进行验证的方法

C.数字签名的结果是十六进制的字符串

D.消息认证能够确定接收方收到的消息是否被篡改过

我能过软考分析：

数字签名与手写签名类似，只不过手写签名是模拟的，因人而异。数字签名是 0 和 1 的数字串，因消息而异。

参考答案

（49）C

17. 2017 年上半年试题 54

下列关于数字签名的说法正确的是（ ）。

A.数字签名是不可信的　　B.数字签名容易被伪造

C.数字签名容易抵赖　　D.数字签名不可改变

我能过软考分析：

本题考查教材 146 页，数字签名的概念。数字签名是可信的、不容易被伪造的、不容抵赖的，而且是不可改变的。

参考答案

（54）D

18. 2017 年上半年试题 55

以下关于公钥基础设施（PKI）的说法中，正确的是（ ）。

A.PKI 可以解决公钥可信性问题

B.PKI 不能解决公钥可信性问题

C.PKI 只能由政府来建立

D.PKI 不提供数字证书查询服务

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。PKI 公钥基础设施是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范，它支持公开密钥管理并能支持认证、加密、完整性和可追究性服务的基础设施。

参考答案

（55）A

19. 2017 年上半年试题 60

证书授权中心（CA）的主要职责不包含（ ）。

A.证书管理　　B.证书签发　　C.证书加密　　D.证书撤销

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。CA 的功能主要有证书管理、证书签发、证书验证、证书撤销等，不包括证书加密。

参考答案

（60）C

20. 2017 年上半年试题 61

X.509 数字证书的内容不包括（ ）。

A.版本号　　B.签名算法标识

C.加密算法标识　　D.主体的公开密钥信息

我能过软考分析：

本题考查教材 329 页关于 X.509 标准。X.509 是现在比较流行的一种证书标准。X.509 数字证书内容包括：版本号、序列号、签名算法标识、发行者名称、有效期、主体名称、主体公钥信息、发行者唯一标识符、主体唯一识别符、扩充域、CA 的签名等。不包括加密算法标识。

参考答案

（61）C

21. 2017 年上半年试题 67

DSS 数字签名标准的核心是数字签名算法 DSA，该签名算法中杂凑函数采用的是（ ）。

A.SHA1　　B. MDS　　C. MD4　　D. SHA2

我能过软考分析：

DSS 数字签名标准的核心是数字签名算法 DSA，该签名算法中杂凑函数采用的是 SHA1 算法。

参考答案

（67）A

22. 2016 年下半年试题 5

面向身份信息的认证应用中，最常用的认证方式是（ ）。

A.基于数据库认证　　B.基于摘要算法认证

C.基于 PKI 认证　　D.基于帐户名，口令认证

我能过软考分析：

在面向身份信息认证应用中最常用的方式是基于账户名和口令认证，比如日常常用的操作系统登录，邮件系统登录等都需要输入对应的用户名和密码才能进入系统。

参考答案

（5）D

23. 2016 年下半年试题 7

S/Key 口令是一种一次性口令生成方案，它可以对抗（ ）。

A.恶意代码木马攻击　　B.拒绝服务攻击

C.协议分析攻击　　D.重放攻击

我能过软考分析：

一次一密指在流密码当中使用与消息长度等长的随机密钥,密钥本身只使用一次。重放攻击又称重播攻击或回放攻击，是指攻击者发送一个目的主机已接收过的包，特别是在认证的过程中，用于认证用户身份所接收的包，来达到欺骗系统的目的。一次一密这样的密钥形式可以对抗重放攻击。

参考答案

（7）D

24. 2016 年下半年试题 11

以下关于认证技术的叙述中，错误的是（ ）。

A.指纹识别技术的利用可以分为验证和识别

B.数字签名是十六进制的字符串

C.身份认证是用来对信息系统中实体的合法性进行验证的方法

D.消息认证能够确定接收方收到的消息是否被篡改过

我能过软考分析：

数字签名与手写签名类似，只不过手写签名是模拟的，因人而异。数字签名是 0 和 1 的数字串，因消息而异。

参考答案

（11）B

25. 2016 年下半年试题 16

数字签名最常见的实现方法是建立在（ ）的组合基础之上。

A.公钥密码体制和对称密码体制

B.对称密码体制和 MD5 摘要算法

C.公钥密码体制和单向安全散列函数算法

D.公证系统和 MD4 摘要算法

我能过软考分析：

数字签名可以利用公钥密码体制、对称密码体制或者公证系统来实现。最常见的的实现方法是建立在公钥密码体制和单向安全散列函数算法的组合基础之上。

参考答案

（16）C

26. 2016 年下半年试题 17

以下选项中，不属手生物识别方法的（ ）。

A.指纹识别　　B.声音识别　　C.虹膜识别　　D.个人标记号识别

我能过软考分析：

本题考查教材 156 页生物特征识别的问题，指纹识别、声音识别、虹膜识别都属于生物识别方法，个人标记号不属于生物识别方法。

参考答案

（17）D

27. 2016 年下半年试题 30

移动用户有些属性信息需要受到保护，这些信息一旦泄露,会对公众用户的生命和财产安全造成威胁.以下各项中，不需要被保护的属性是（ ）。

A.用户身份(ID)　　B.用户位置信息

C.终端设备信息　　D.公众运营商信息

我能过软考分析：

本题考查的是第三章移动隐私保护的内容，公众运营商是公开信息，比如移动公司，不需要被保护。但是可以通过朴素的价值观就可以判断出来。

参考答案

（30）D

28. 2016 年下半年试题 31

以下关于数字证书的叙述中，错误的是（ ）。

A.证书通常由 CA 安全认证中心发放

B.证书携带持有者的公开密钥

C.证书的有效性可以通过验证持有者的签名获知

D.证书通常携带 CA 的公开密钥

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。数字证书通常包含用户身份信息、持有者的公开密钥以及 CA 的数字签名信息等。

参考答案

（31）D

29. 2016 年下半年试题 34

数字信封技术能够（ ）。

A.对发送者和接收者的身份进行认证

B.保证数据在传输过程中的安全性

C.防止交易中的抵赖发生

D.隐藏发送者的身份

我能过软考分析：

数字信封使用私有密钥加密算法并利用接收人的公钥对要传输的数据进行加密，以保证数据信息在传输过程中的安全性。

参考答案

（34）B

30. 2016 年下半年试题 36

甲不但怀疑乙发给他的信遭人篡改，而且怀疑乙的公钥也是被人冒充的。为了消除甲的疑虑，甲和乙决定找一个双方都信任的第三方来签发数字证书，这个第三方是（ ）。

A.国际电信联盟电信标准分部(ITU-T)

B.国家安全局(NSA)

C.认证中心(CA)

D.国际标准化组织(ISO)

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。通信双方

进行保密通信时，通常会通过双方信任的第三方认证中心 CA 来签发数字证书。

参考答案

（36）C

31. 2016 年下半年试题 40

甲收到一份来自乙的电子订单后，将订单中的货物送达到乙时，乙否认自己曾经发送过这份订单，为了解除这种纷争，采用的安全技术是（ ）。

A.数字签名技术　　B.数字证书

C.消息认证码　　D.身份认证技术

我能过软考分析：

本题考查教材 146 页，数字签名的概念。数字签名技术能使签名者事后不能抵赖自己的签名，任何其他人不能伪造签名以及能在公正的仲裁者面前通过验证签名来确认其真伪。

参考答案

（40）A

32. 2016 年下半年试题 60

在 PKI 中，不属于 CA 的任务是（ ）。

A.证书的颁发　B.证书的审批　C.证书的备份　D.证书的加密

我能过软考分析：

PKI 在教材中在 165-168 页，但各个章中也有散落的一些内容，如果有时间可以找一本信息安全概率的教材对这个部分进行一下专题的学习。CA 是 PKI 的信任基础，CA 负责签发证书、管理和撤销证书，包括证书的审批及备份等。

参考答案

（60）D

第 3 章 网络安全基础

1. 2018 年上半年试题 13

网络安全技术可以分为主动防御技术和被动防御技术两大类，以下属于主动防技术的是（ ）。

A.蜜罐技术　　B.入侵检测技术

C.防火墙技术　　D.恶意代码扫描技术

我能过软考分析：

本题在书中第 333 页，蜜罐（Honeypot）技术是一种主动防御技术，是入侵检测技术的一个重要发展方向。 蜜罐是一种在互联网上运行的计算机系统，是专门为吸引并诱骗那些试图非法闯入 他人计算机系统的人而设计的。蜜罐系统是一个包含漏洞的诱骗系统，它通过摸拟一个或多个易受攻击的主机和服务，给攻击者提供一个容易攻击的目标。主动防御是与被动防御相对应的概念，就是在入侵行为对信息系统发生影响之前，能够及时精准预警，实时构建弹性防御体系，避免、转移、降低信息系统面临的风险。其余三种技术都是在对现有信息系统已经发生攻击的情况下，都属于被动防御技术。

参考答案：

（13）A

2. 2018 年上半年试题 21

（ ）是一种通过不断对网络服务系统进行干扰,影响其正常的作业流程,使系统响应减慢甚至瘫痪的攻击方式。

A.暴力攻击　　B.拒绝服务攻击　　C.重放攻击　　D.欺骗攻击

我能过软考分析：

本题在书中第 229 页，拒绝服务攻击是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪。3.3 节提出的各种网络安全威胁在考试中出现概率较大，需要重点关注。

参考答案：

（21）B

3. 2018 年上半年试题 23

下列说法中,错误的是（ ）。

A.数据被非授权地增删、修改或破坏都属于破坏数据的完整性

B.抵赖是一种来自黑客的攻击

C.非授权访问是指某一资源被某个非授权的人,或以非授权的方式使用

D.重放攻击是指出于非法目的,将所截获的某次合法的通信数据进行拷贝而重新发送

我能过软考分析：

本题可以用第一章的知识就可以解答，信息抵赖是发送者对其发送信息进行否认，否认或抵赖曾经完成的操作和承诺，因此抵赖来自于受信的系统用户的行为，并不来自于黑客。

参考答案：

（23）B

4. 2018 年上半年试题 27

以下关于 TCP 协议的描述,错误的是（ ）。

A.TCP 是 Internet 传输层的协议,可以为应用层的不同协议提供服务

B.TCP 是面向连接的协议,提供可靠、全双工的、面向字节流的端到端的服务

C.TCP 使用二次握手来建立连接,具有很好的可靠性

D.TCP 每发送一个报文段,就对这个报文段设置一次计时器

我能过软考分析：

本题来自于书中第 185 页，TCP 是一种面向连接的、可靠的、基于字节流的传输层通信协议，使用三次握手协议建立连接。网络协议是网络安全部分的基础，在考试中出现的频度也比较高。

参考答案：

（27）C

5. 2018 年上半年试题 28

Kerberos 是一种常用的身份认证协议,它采用的加密算法是（ ）。

A. Elgamal　　B. DES　　C. MD5　　D. RSA

我能过软考分析：

本题在书中第 327 页，Kerberos 是一种常用的身份认证协议，它采用数据加密标准（DES）加密算法进行加密。Kerberos 协议做到了将身份的认证与授权相分离，使用的是对称密码体制，虽然书中没有写明使用的算法，但选项种只有 DES 算法是对称密码算法。

参考答案：

（28）B

6. 2018 年上半年试题 37

WI-FI 网络安全接入是一种保护无线网络安全的系统,WPA 加密的认证方式不包括（ ）。

A. WPA 和 WPA2　　B. WEP　　C. WPA-PSK　　D. WPA2-PSK

我能过软考分析：

本题在教材中 325 及 368 页，WPA 有 WPA 和 WPA2 两个标准，是一种保护无线电脑网络（Wi-Fi）安全的系统，有四种认证方式：WPA、WPA-PSK、WPA2 和 WPA2-PSK。这道题其实在我们日常设置个人热点的时候也能遇到。

参考答案：

（37）B

7. 2018 年上半年试题 42

IP 地址分为全球地址和专用地址,以下属于专用地址的是（ ）。

A.192.172.1.2　　B.10.1.2.3　　C.168.1.2.3　　D.172.168.1.2

我能过软考分析：

本题在书中第 173 页，关于 IP 地址需要掌握各类 IP 地址的字段、专用 IP 地址、特别的 IP 地址（例如 127.0.0.1 的回环地址）等等。专用 IP 地址范围：

A 类：10.0.0.0~10.255.255.255，

B 类：172.16.0.0~172.31.255.255，

C 类：192.168.0.0~192.168.255.255。

参考答案：

（42）B

8. 2018 年上半年试题 43

信息安全风险评估是依照科学的风险管理程序和方法,充分地对组成系统的各部分所面临的危险因素进行分析评价,针对系统存在的安全问题,根据系统对其自身的安全需求,提出有效的安全措施,达到最大限度减少风险,降低危害和确保系统安全运行的目的,风险评估的过程包括（ ）四个阶段。

A.风险评估准备、漏洞检测、风险计算和风险等级评价

B.资产识别、漏洞检测,风险计算和风险等级评价

C.风险评估准备、风险因素识别、风险程度分析和风险等级评价

D.资产识别、风险因素识别、风险程度分析和风险等级评价

我能过软考分析：

本题在书中 308 页。信息安全风险评估的过程包括信息安全风险评估准备、风险因素识别、风险程度分析和风险等级评价四个阶段。本题考察的是 3.4 节的内容，攻击的方法和防御的方法是本章的重点，需要重点掌握。

参考答案：

（43）C

9. 2018 年上半年试题 47

攻击者通过对目标主机进行端口扫描可以直接获得（ ）。

A.目标主机的操作系统信息

B.目标主机开放端口服务信息

C.目标主机的登录口令

D.目标主机的硬件设备信息

我能过软考分析：

本题在书中第 310 页，端口扫描，顾名思义，就是逐个对一段端口或指定的端口进行扫描。通过扫描结果可以知道一台计算机上都提供了哪些服务，然后就可以通过所提供的这些服务的已知漏洞就可进行攻击。不同的端口号对应不同的服务，比如 HTTP 在 80 端口等等，在这种情况下就可以通过端口号得到服务器提供的服务信息。

参考答案：

（47）B

10. 2018 年上半年试题 48

WPKI（无线公开密钥体系）是基于无网络环境的一套遵循既定标准的密钥及证书管理平台,该平台采用的加密算法是（ ）。

A.SM4　　B.优化的 RSA 加密算法

C.SM9　　D.优化的椭圆曲线加密算法

我能过软考分析：

本题在书中第 364 页。WPKI 是传统的 PKI 技术应用于无线环境的优化扩展。它采用了优化的 ECC 椭圆曲线加密和压缩的 X.509 数字证书。它同样采用证书管理公钥，通过第三方的可信任机构——认证中心(CA)验证用户的身份，从而实现信息的安全传输。

参考答案：

（48）D

11. 2018 年上半年试题 51

对无线网络的攻击可以分为:对无线接口的攻击、对无线设备的攻击和对无线网络的攻击。以下属于对无线设备攻击的是（ ）。

A.窃听　　B.重放　　C.克隆　　D.欺诈

我能过软考分析：

本题在教材中 352 页，无线网络由于自身特点，面临着比有线网络更多更严重的安全威胁，主要可划分为对无线接口的攻击、对无线设备的攻击以及对无线网络本身的攻击。根据攻击手段和目标，对无线接口的攻击可以分为物理攻击和密码学攻击，包括窃听、篡改、重放、干扰和欺诈等等。攻击无线网络是指针对网络 基础设施进行攻击，也包括内部人员破坏和泄密。针对无线设备的攻击包括克隆、盗窃等等。我们从技巧的角度来讲，只有克隆和盗窃是对设备来做的，其他的都是对信息的攻击。

参考答案：

（51）C

12. 2018 年上半年试题 52

无线局域网鉴别和保密体系 WAPI 是我国无线局域网安全强制性标准,以下关于 WAP 的描述,正确的是（ ）。

A.WAPI 从应用模式上分为单点式、分布式和集中式

B.WAPI 与 WIFI 认证方式类似,均采用单向加密的认证技术

C.WAPI 包括两部分:WAI 和 WPI,其中 WAI 采用对称密码算法实现加、解密操作

D.WAPI 的密钥管理方式包括基于证书和基于预共享秘密两种方式

我能过软考分析：

本题在书中的 364 页，WAPI 采用国家密码管理委员会办公室批准的公开密钥体制的椭圆曲线密码算法和秘密密钥体制的分组密码算法，实现了设备的身份鉴别、链路验证、访问控制和用户信息在无线传输状态下的加密保护。 此外，WAPI 从应用模式上分为单点式和集中式两种，可以彻底扭转目前 WLAN 采用多种安全机制并存且互不兼容的现状，从根本上解决安全问题和兼容性问题。与 WIFI 的单向加密认证不同， WAPI 双向均认证，从而保证传输的安全性。 WAPI 包括两部分 WAI 和 WPI。 WAI 和 WPI 分别实现对用户身份的鉴别和对传输的业务数据加密，其中 WAI 采用公开密钥密码体制，利用公钥证书来对 WLAN 系统中的 STA 和 AP 进行认证 WPI 则采用对称密码算法实现对 MAC 层 MSDU 的加、解密操作。 WAPI 鉴别及密钥管理的方式有两种，即基于证书和基于预共享密钥 PSK。若采用基于证书的方式，整个过程包括证书鉴别、单播密钥协商与组播密钥通告:若采用颈共享密钥的方式，整个过程则为单播密钥协商与组播密钥通告。2018 年中对无线网络安全的部分的关注也比较多，需要引起我们的重视。

参考答案:

（52）D

13. 2018 年上半年试题 55

以下关于 IPSec 协议的叙述中,正确的是（ ）。

A.IPSec 协议是 IP 协议安全问题的一种解决方案

B.IPSec 协议不提供机密性保护机制

C.IPSec 协议不提供认证功能

D.IPSec 协议不提供完整性验证机制

我能过软考分析：

本题在书中 318 页，IPSec 协议是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议网络上进行保密而安全的通讯，是解决 IP 协议安全问题的一种方案，它能提供完整性、保密性、反重播性、不可否认性、认证等功能。IPSec 协议是一种经典的安全协议。需要掌握隧道模式、传输模式以及其工作原理。

参考答案：

（55）A

14. 2018 年上半年试题 57

以下关于网络钓鱼的说法中,不正确的是（ ）。

A.网络钓鱼属于社会工程攻击

B.网络钓鱼与 Web 服务没有关系

C.典型的网络钓鱼攻击是将被攻击者引诱到一个钓鱼网站

D.网络钓鱼融合了伪装、欺骗等多种攻击方式

我能过软考分析：

本题在书中第 252 页，网络钓鱼是通过大量发送声称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（如用户名、口令、帐号 ID、ATM PIN 码或信用卡详细信息）的一种攻击方式，最典型的的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个过程不会让受害者警觉，它是“社会工程攻击”的一种形式。

参考答案：

（57）B

15. 2018 年上半年试题 61

以下关于 VPN 的叙述中,正确的是（ ）。

A.VPN 通过加密数据保证通过公网传输的信息即使被他人截获也不会泄

B.VPN 指用户自己租用线路,和公共网络物理上完全隔离的、安全的线路

C.VPN 不能同时实现对消息的认证和对身份的认证

D.VPN 通过身份认证实现安全目标,不具备数据加密功能

我能过软考分析：

本题在书中在 300 页，VPN 即虚拟专用网，是企业网在因特网等公共网络上的延伸，通过一个私有的通道在公共网络上创建一个临时的、安全的私有连接；能为用户提供加密、认证等安全服务。B 选项实际上是专用网络的特点。C 选项中 VPN 能够同时实现对消息和身份的认证。D 选项中 VPN 不仅能

够确认来源，也能进行数据保密。VPN 可以结合 VPN 使用的协议比如 IPSec 协议来理解。

参考答案：

（61）A

16. 2018 年上半年试题 63

当防火墙在网络层实现信息过滤与控制时,主要针对 TCP/IP 协议中的数据包头制定规则匹配条件并实施过滤,该规则的匹配条件不包括（ ）。

A.IP 源地址　　B.源端口　　C.IP 目的地址　　D.协议

我能过软考分析：

本题在书中 274 页，当防火墙在网络层实现信息过滤与控制时，主要是针对 TCP/IP 协议中的数据包头部制定规则的匹配条件并实施过滤，其规则的匹配条件包括以下内容： IP 源地址，IP 数据包的发送主机地址；IP 目的地址，IP 数据包的接收主机地址；协议，IP 数据包中封装的协议类型，包括 TCP、UDP 或 ICMP 包等。一般情况下，包过滤防火墙不对源端口进行过滤，因为源端口可以进行修改。但在企业希望监控员工行为的防火墙中，有可能对源端口进行过滤防止员工登陆网页、聊微信等行为，但这不在我们传统讨论防火墙的范围。

参考答案：

（63）B

17. 2017 年上半年试题 11

下列攻击中，不能导致网络瘫痪的是（ ）。

A.溢出攻击　　B.钓鱼攻击　　C.邮件炸弹攻击　　D.拒绝服务攻击

我能过软考分析：

本题对 3.3 节的攻击方式进行了综合性的考查，网络钓鱼是通过大量发送声称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（如用户名、口令、帐号 ID 、 ATM PIN 码或信用卡详细信息）的一种攻击方式，不会导致网络瘫痪。一般情况下，基于社会工程学的攻击都不会使得网络瘫痪。

参考答案：

（11）B

18. 2017 年上半年试题 13

网站的安全协议是 https 时，该网站浏览时会进行（ ）处理。

A.增加访问标记　　B.加密　　C.身份隐藏　　D.口令验证

我能过软考分析：

HTTPS 和 HTTP 的区别主要为以下四点： 一、https 协议需要到 ca 申请证书，一般免费证书很少，需要交费。 二、http 是超文本传输协议，信息是明文传输，https 则是具有安全性的 ssl 加密传输协议。 三、http 和 https 使用的是完全不同的连接方式，用的端口也不一样，前者是 80，后者是 443。

四、http 的连接很简单，是无状态的；HTTPS 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议，比 http 协议安全。

参考答案：

（13）B

19. 2017 年上半年试题 14

被动攻击通常包含（ ）。

A.拒绝服务攻击　　B.欺骗攻击　　C.窃听攻击　　D.数据驱动攻击

我能过软考分析：

本题对主动攻击和被动攻击进行了考查，对 3.3 节的内容进行了综合的考查，窃听属于被动攻击方式，拒绝服务攻击、欺骗攻击、数据驱动攻击等都属于主动攻击。被动攻击是指不会对原来的服务产生影响的攻击方式。

参考答案：

（14）C

20. 2017 年上半年试题 15

以下网络攻击方式中，（ ）实施的攻击不是网络钓鱼的常用手段。

A.利用社会工程学　　B.利用虚假的电子商务网站

C.利用假冒网上银行、网上证券网站　　D.利用蜜罐

我能过软考分析：

本题在书中 252 页，利用社会工程学、利用虚假的电子商务网站、利用假冒网上银行、网上证券网站等都是属于网络钓鱼的常用手段；利用蜜罐方式是属于网络安全防御手段。网络钓鱼和网络钓鱼执法是不一样的，注意这点就能很容易得到答案。

参考答案：

（15）D

21. 2017 年上半年试题 22

攻击者通过对目标主机进行端口扫描，可以直接获得（ ）。

A.目标主机的口令　　B.给目标主机种植木马

C.目标主机使用了什么操作系统　　D.目标主机开放了哪些端口服务

我能过软考分析：

本题在书中 308 页，端口扫描，顾名思义，就是逐个对一段端口或指定的端口进行扫描。通过扫描结果可以知道一台计算机上都提供了哪些服务，然后就可以通过所提供的这些服务的已知漏洞就可进行攻击。在 2018 年也对类似知识点进行了考查。

参考答案：

（22）D

22. 2017 年上半年试题 23

以下关于 NAT 的说法中，错误的是（ ）。

A.NAT 允许一个机构专用 Intranet 中的主机透明地连接到公共区域的主机，无需每台内部主机都用有注册的（已经越来越缺乏的）全局互联网地址

B.静态 NAT 是设置起来最简单和最容易实现的一种地址转化方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法地址

C.动态 NAT 主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态 NAT 就会分配给用户一个 IP 地址，当用户断开时，这个 IP 地址就会被释放而留待以后使用

D.动态 NAT 又叫网络地址端口转换 NAPT

我能过软考分析：

动态 NAT 是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址对是不确定的，是随机的，所有被授权访问 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。

网络地址端口转换 NAPT 是人们比较熟悉的一种转换方式。NAPT 普遍应用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。NAPT 与动态地址 NAT 不同，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。总之，NAT 不等同于 NAPT，NAPT 是 IP 加 PORT 的映射，而 NAT 只是 IP 的映射 ，虽说 NAT 也可以增加端口，大部分猫默认的是全部 IP 和端口的映射。

参考答案：

（23）D

23. 2017 年上半年试题 24

应用代理防火墙的主要优点是（ ）。

A.加密强度高　　B.安全控制更细化、更灵活

C.安全服务的透明性更好　　D.服务对象更广泛

我能过软考分析：

本题在书中 281 页，在传统的包过滤防火墙和状态检测防火墙外，书中还介绍了电路层网关和应用层网关两种防火墙。应用代理防火墙的主要优点是可以提供用户认证等用户安全策略，应用层网关可以实现基于内容的信息过滤，安全控制会更细化更灵活；但应用代理防火墙不适用于实时性太高的服务，而且对用户的透明性低。

参考答案：

（24）B

24. 2017 年上半年试题 25

从安全属性对各种网络攻击进行分类，阻断攻击是针对（ ）的攻击

A.机密性　　B.可用性　　C.完整性　　D.真实性

我能过软考分析：

本题是对安全基础知识的考查，从安全属性上来分析，截获攻击是针对机密性的攻击；阻断攻击是针对可用性的攻击。

参考答案：

（25）B

25. 2017 年上半年试题 27

我国制定的关于无线局域网安全的强制标准是（ ）。

A.IEEE 802.11　　B.WPA　　C.WAPI　　D.WEP

我能过软考分析：

本题在书中第一章 28 页就已经提及，在本章种再次讲解。无线局域网鉴别和保密体系（WAPI）是一种安全协议，同时也是中国无线局域网安全强制性标准。

参考答案：

（27）C

26. 2017 年上半年试题 33

通过具有 IPSec 功能的路由器构件 VPN 的过程中，采用的应用模型是（ ）。

A.隧道模型　　B.报名模式　　C.传输模式　　D.压缩模式

我能过软考分析：

本题在书中 318 页，IPSec 有两种模式，即隧道模式和传输模式； 传输模式只能适合 PC 到 PC 的场景；隧道模式可以适用于任何场景，隧道模式虽然可以适用于任何场景，但是隧道模式需要多一层 IP 头（通常为 20 字节长度）开销，所以在 PC 到 PC 的场景，建议还是使用传输模式。题中通过路由器构建

VPN，显然不是 PC 到 PC 的场景，所以需要采用隧道模式。这样的试题每年都会出现，一定要对 IPSec 协议详细了解。

参考答案：

（33）A

27. 2017 年上半年试题 37

有线等效保密协议 WEP 采用 RC4 流满面技术实现保密性，标准的 64 位标准流 WEP 用的密钥和初始向量长度分别是（ ）。

A.32 位和 32 位　　B.48 位和 16 位

C.56 位和 8 位　　D.40 位和 24 位

我能过软考分析：

本题在书中 366 页，考查的内容也比较细，有线等效保密协议 WEP 采用的密钥和初始向量长度分别是 40 位和 24 位。

参考答案：

（37）D

28. 2017 年上半年试题 42

下面关于跨站攻击描述不正确的是（ ）。

A.跨站脚本攻击指的是恶意攻击者向 Web 页里面插入恶意的 Html 代码

B.跨站脚本攻击简称 XSS

C.跨站脚本攻击者也可称作 CSS

D.跨站脚本攻击是主动攻击

我能过软考分析：

本题在书中 266 页。跨站攻击，即 Cross Site Script Execution(通常简写为 XSS)是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。对网站的攻击方式是这些年的一个热点，在书中对 SQL 注入和跨站脚本进行了详细讲解，但理解难度比较大，需要有一定的基础。

参考答案：

（42）D

29. 2017 年上半年试题 43

以下不属于信息安全风险评估中需要识别的对象是（ ）。

A.资产识别　　B.威胁识别　　C.风险识别　　D.脆弱性识别

我能过软考分析：

本题在书中 312 页，了解即可。信息安全风险评估中需要识别的对象包括资产识别、威胁识别、脆弱性识别。

参考答案：

（43）C

30. 2017 年上半年试题 44

安全漏洞扫描技术是一类重要的网络安全技术。当前，网络安全漏洞扫描技术的两大核心技术是（ ）。

A.PINC 扫描技术和端口扫描技术

B.端口扫描技术和漏洞扫描技术

C.操作系统探测和漏洞扫描技术

D.PINC 扫描技术和操作系统探测

我能过软考分析：

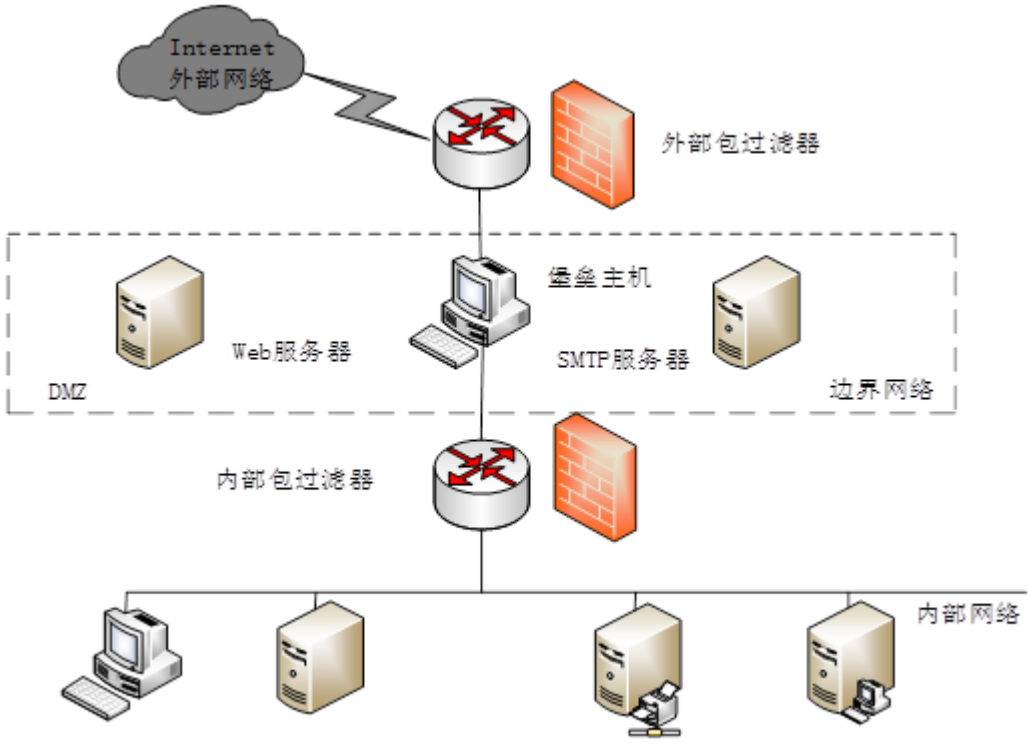
本题在书中 308 页，网络安全扫描技术的两大核心技术就是端口扫描技术与漏洞扫描技术，除此之外还有密码扫描技术。这两种技术广泛运用于当前较成熟的网络扫描器中，如著名的 Nmap 和 Nessus 就是利用了这两种技术。

参考答案：

（44）B

31. 2017 年上半年试题 45

防火墙的经典体系结构主要有三种，下图给出的是（ ）体系结构。



A.双重宿主主机　　B.（被）屏蔽主机

C.（被）屏蔽子网　　D.混合模式

我能过软考分析：

本题在书中 282 页，（被）屏蔽子网体系结构由内、外部包过滤路由器、DMZ 区及堡垒主机构成。双宿主主机结构是指以双宿主主机作为防火墙系统的主题，执行分离外部网络与内部网络的任务。屏蔽主机的模式与屏蔽子网模式类似。

参考答案：

（45）C

32. 2017 年上半年试题 47

IP 地址欺骗的发生过程，下列顺序正确的是（ ）。

①确定要攻击的主机 A；②发现和他有信任关系的主机 B；③猜测序列号；④成功连接，留下后门；⑤将 B 利用某种方法攻击瘫痪。

A.①②⑤③④ B.①②③④⑤ C.①②④③⑤ D.②①⑤③④

我能过软考分析：

本题在书中 256 页 IP 地址欺骗过程：确定要攻击的主机 A；发现和他有信任关系的主机 B；将 B 利用某种方法攻击瘫痪；猜测序列号；成功连接，留下后门。

参考答案：

（47）A

33. 2017 年上半年试题 50

为了防御网络监听，最常用的方法是（ ）。

A.采用物理传输（非网络） B.信息加密

C.无线网 D.使用专线传输

我能过软考分析：

本题在书中 225 页，防御网络监听，有三种方法，一是确保以太网整体的安全性，二是采用加密技术，三是可以考虑 Kerberos 协议。最常用的方法是对信息进行加密保证其机密性。

参考答案：

（50）B

34. 2017 年上半年试题 51

能有效控制内部网络和外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和对不良信息的过滤的安全技术是（ ）。

A.入侵检测　　B.反病毒检测　　C.防火墙　　D.计算机取证

我能过软考分析：

本题在书中 274 页并对各种安全技术进行了综合考查。防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关，从而保护内部网免受非法用户的侵入。

参考答案：

（51）C

35. 2017 年上半年试题 52

包过滤技术防火墙在过滤数据包是，一般不关心（ ）。

A.数据包的原地址　　B.数据包的目的地址

C.数据包的协议类型　　D.数据包的内容

我能过软考分析：

本题在 274 页，也是考查包过滤防火墙。数据包过滤是通过对数据包的 IP 头和 TCP 头或 UDP 头的检查来实现的，不检查数据包的内容。这样的问题多次考察，重复率较高。

参考答案：

（52）D

36. 2017 年上半年试题 57

无线传感器网络容易受到各种恶意攻击，以下关于其防御手段说法错误的是（ ）。

A.采用干扰去内节点切换频道的方式来低于干扰

B.通过向独立多路径发送验证数据来发现异常节点

C.利用中心节点监视网络中其他所有阶段来发现恶意节点

D.利用安全并具有弹性的时间同步协议对抗外部攻击和被俘获节点的影响

我能过软考分析：

本题在书中 373 页，中心节点可以监视，但是如果破解了网络中的节点，然后对网络进行偷窥，就没办法发现恶意节点了；如果切换了频率，而网络中的存在使用原来频率的节点，那这些节点就是异常节点，通过各个节点返回的信息判断这个节点是不是异常的。

参考答案：

（57）C

37. 2017 年上半年试题 58

属于第二层的 VPN 隧道协议是（ ）。

A.IPSeC　　B.PPTP　　C.GRE　　D.IPv4

我能过软考分析：

本题在书中 303 页，PPTP 属于第二层的点对点 VPN 隧道协议，IPSEC 属于第三层的 VPN 隧道协议。L2TP 也是第二层隧道协议。

参考答案：

（58）B

38. 2017 年上半年试题 62

如果在某大型公司本地与异地分公司之间建立一个 VPN 连接，应该建立的 VPN 类型是（ ）。

A.内部 VPN　　B.外部 VPN　　C.外联网 VPN　　D.远程 VPN

我能过软考分析：【有问题】

本题在书中 301 页，在某大型公司本地与异地分公司之间建立一个 VPN 连接，应该建立远程 VPN。远程 VPN 主要解决企业员工或小分支机构等远程用户来安全访问企业内部网。第六章也有该知识点。

远程访问 VPN：Access VPN 面向出差员工。允许出差员工跨越公用网络远程接入公司内部网络。

Intranet VPN（企业内部虚拟专网）：Intranet VPN 通过公用网络进行企业内部各个网络的互连。

Extranet VPN（扩展的企业内部虚拟专网）：Extranet VPN 是指利用 VPN 将企业网延伸至合作伙伴处，使不同企业间通过公网来构筑 VPN。Intranet VPN 和 Extranet VPN 的不同点主要在于访问公司总部网络资源的权限有区别。

参考答案：

（62）A

39. 2017 年上半年试题 63

网络蜜罐技术是一种主动防御技术，是入侵检测技术的一个重要发展方向，以下有关蜜罐说法不正确的是（ ）。

A.蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或者多个易受攻击的主机和服务，给攻击者提供一个容易攻击的目标

B.使用蜜罐技术，可以使目标系统得以保护，便于研究入侵者的攻击行为

C.如果没人攻击，蜜罐系统就变得毫无意义

D.蜜罐系统会直接提高计算机网络安全等级，是其他安全策略不可替代的

我能过软考分析：

本题在书中 333 页，蜜罐系统是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，随时了解针对服务器

发动的最新的攻击和漏洞。还可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社交网络，通常不会提高计算机网络安全等级。

参考答案：

（63）D

40. 2016 年下半年试题 3

以下网络攻击中，（ ）属于被动攻击。

A.拒绝服务攻击　　B.重放　　C.假冒　　D.流量分析

我能过软考分析：

本题在 2018 年重复出现，对被动主动攻击进行了考查。流量分析是指通过一定的技术手段，实时监测用户网络七层结构中各层的流量分布，进行协议、流量的综合分析，从而有效的发现、预防网络流量和应用上的瓶颈，为网络性能的优化提供依据，属于被动攻击。

参考答案：

（3）D

41. 2016 年下半年试题 8

防火墙作为一种被广泛使用的网络安全防御技术，其自身有一些限制,它不能阻止（ ）。

A.内部威胁和病毒威胁　　B.外部攻击

C.外部攻击、外部威胁和病毒威胁　　D.外部攻击和外部威胁

我能过软考分析：

本题在书中 274 页，防火墙是一种位于内部网络与外部网络之间的网络安全系统，内外网络通信时，依照特定的规则，允许或是限制传输的数据通过。它不能防范内部威胁及病毒威胁。

参考答案：

（8）A

42. 2016 年下半年试题 9

以下行为中，不属于威胁计算机网络安全的因素是（ ）。

A.操作员安全配置不当而造成的安全漏洞

B.在不影响网络正常工作情况下，进行截获、窃取、破译以获得重要机密信息

C.安装非正版软件

D.安装蜜罐系统

我能过软考分析：

本题在书中 333 页。蜜罐好比是情报收集系统。好比是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，随时了解针对服务器发动的最新的攻击和漏洞。它是一种防御手段。本题用朴素的好坏理解也能够猜出来。

参考答案：

（9）D

43. 2016 年下半年试题 19

注入语句：http：／／xxx．xxx.xxx/abc.asp?pYY and user>0，不仅可以判断服务器的后台数据库是否为 SQL-SERVER，还可以得到（ ）。

A.当前连接数据库的用户数量　　B.当前连接数据库的用户名

C.当前连接数据库的用户口令　　D.当前连接的数据库名

我能过软考分析：

本题在书中的 261 页，考查的是 SQL 注入，是书上的原语句，这样的题目对于没有学习过数据库的同学难度比较大，但我们至少掌握书中讲过的知识点。注入语句：http：//xxx．xxx.xxx/abc.asp?p=YY and user>0，服务器运行“Select * from 表名 where 字段=YY and user > 0”显然，该语句不能正常执行会出错，从其错误信息中不仅可以获知该服务器的后台数据库是否为 SQL-SERVER，还可以得到当前连接的数据库的用户名。

参考答案：

（19）B

44. 2016 年下半年试题 21

有一种攻击是不断对网络服务系统进行干扰， 改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪。 这种攻击叫做（ ）。

A.重放攻击　　B.拒绝服务攻击

C.反射攻击　　D.服务攻击

我能过软考分析：

本题在书中 229 页，各种攻击的原理和基本特点是需要掌握的内容。拒绝服务攻击是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪。

参考答案：

（21）B

45. 2016 年下半年试题 23

下列说法中，错误的是（ ）。

A.服务攻击是针对某种特定的网络应用的攻击

B.主要的渗入威胁有特洛伊木马和陷阱

C.非服务攻击是针对网络层协议而进行的

D.对于在线业务系统的安全风险评估，应采用最小影响原则

我能过软考分析：

本题考查渗入威胁与植入威胁的区别，了解即可。主要的渗入威胁有假冒、旁路、授权侵犯，主要的植入威胁有特洛伊木马和陷阱。

参考答案：

（23）B

46. 2016 年下半年试题 27

在 IPv4 的数据报格式中，字段（ ）最适合于携带隐藏信息。

A.生存时间　　B.源 IP 地址　　C.版本　　D.标识

我能过软考分析：

本题在书中 171 页，对 IP 协议进行了具体的考查。标识长度为 16 位，为了使分片后的各数据报片最后能准确地重装成为原来的数据报。最适合携带隐藏信息。

参考答案：

（27）D

47. 2016 年下半年试题 28

Kerberos 是一种常用的身份认证协议，它采用的加密算法是（ ）。

A.Elgamal　　B.DES　　C.MD5　　D.RSA

我能过软考分析：

本题在 2018 年也进行了重复的考查。Kerberos 是一种常用的身份认证协议，它采用数据加密标准（DES）加密算法进行加密。

参考答案：

（28）B

48. 2016 年下半年试题 37

WI-FI 网络安全接入是一种保护无线网络安全的系统，WPA 加密的认证方式不包括（ ）。

A.WPA 和 WPA2　　B.WPA-PSK　　C.WEP　　D.WPA2-PSK

我能过软考分析：

本题也在 2018 年进行了重复的考查。WPA 有 WPA 和 WPA2 两个标准，是一种保护无线电脑网络（Wi-Fi）安全的系统，有四种认证方式：WPA、WPA-PSK、WPA2 和 WPA2-PSK。

参考答案：

（37）C

49. 2016 年下半年试题 42

IP 地址分为全球地址和专用地址,以下属于专用地址的是（ ）。

A.172.168.1.2　　B.10.1.2.3　　C.168.1.2.3　　D.192.172.1.2

我能过软考分析：

本题在 18 年也进行了考查。对于各类 IP 地址的内容应当认真掌握。专用 IP 地址范围：

A 类：10.0.0.0~10.255.255.255，

B 类：172.16.0.0~172.31.255.255，

C 类：192.168.0.0~192.168.255.255。

参考答案：

（42）B

50. 2016 年下半年试题 45

以下对 OSI（开放系统互联）参考模型中数据链路层的功能叙述中描述最贴切的是（ ）。

A.保证数据正确的顺序、无差错和完整

B.控制报文通过网络的路由选择

C.提供用户与网络的接口

D.处理信号通过介质的传输

我能过软考分析：

本题在书中 179 页的图中，数据链路层最基本的服务是将源计算机网络层来的数据可靠的传输到相邻节点的目标计算机的网络层。为达到这一目的，数据链路层必须具备一系列相应的功能，主要有：1、如何将数据组合成数据块（在数据链路层中将这种数据块称为帧，帧是数据链路层的传送单位）；2、如何控制帧在物理信道上的传输，包括如何处理传输差错，如何调节发送速率以使之与接收方相匹配；3、在两个网路实体之间提供数据链路通路的建立、维持和释放管理。OSI 和 TCP/IP 体系结构都应该认真掌握。

参考答案：

（45）A

51. 2016 年下半年试题 48

以下不属于网络安全控制技术的是（ ）。

A.防火墙技术 B.访问控制技术C.入侵检测技术 D.差错控制技术

我能过软考分析：

本题考查书中 3.4 节各种安全技术，网络安全控制技术包括防火墙技术、入侵检测技术、访问控制技术等；差错控制技术是在数字通信过程中利用编码的方法对错误进行控制，以提高数字传输的准确性，不属于网络安全控制技术。

参考答案：

（48）D

52. 2016 年下半年试题 53

入侵检测系统放置在防火墙内部所带来的好处是（ ）。

A.减少对防火墙的攻击

B.降低入侵检测系统的误报率

C.增加对低层次攻击的检测

D.增加检测能力和检测范围

我能过软考分析：

本题对应书中 292 页，本题可以通过对防火墙与入侵检测系统的分析来得到，IDS 实时检测可以及时发现一些防火墙没有发现的入侵行为，发行入侵行为的规律，这样防火墙就可以将这些规律加入规则之中，提高防火墙的防护力度，降低入侵检测系统的误报率。我们从一个简单的角度来理解，将 IDS 放在防火墙里，防火墙过滤了一部分数据，到达 IDS 的数据包就少了，误报的可能性就小了。

参考答案：

（53）B

53. 2016 年下半年试题 55

以下关于 IPSec 协议的叙述中，正确的是（ ）。

A.IPSec 协议是解决 IP 协议安全问题的一种方案

B.IPSec 协议不能提供完整性

C.IPSec 协议不能提供机密性保护

D.IPSec 协议不能提供认证功能

我能过软考分析：

本题在书中 318 页，IPSec 协议是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议网络上进行保密而安全的通讯，是解决 IP 协议安全问题的一种方案，它能提供完整性、保密性、反重播性、不可否认性、认证等功能。BCD 三项把不能改成能够就是正确选项。

参考答案：

（55）A

54. 2016 年下半年试题 57

以下关于网络钓鱼的说法中，不正确的是（ ）。

A.网络钓鱼融合了伪装、欺骗等多种攻击方式

B.网络钓鱼与 Web 服务没有关系

C.典型的网络钓鱼攻击将被攻击者引诱到一个通过精心设计的钓鱼网站上

D.网络钓鱼是“社会工程攻击”的一种形式

我能过软考分析：

本题在书中 252 页，网络钓鱼是通过大量发送声称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（如用户名、口令、帐号 ID 、 ATM PIN 码或信用卡详细信息）的一种攻击方式，最典型的的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个过程不会让受害者警觉，它是“社会工程攻击”的一种形式。本题在 2018 年的题目中又进行了考查。

参考答案：

（57）B

55. 2016 年下半年试题 58

以下关于隧道技术说法不正确的是（ ）。

A.隧道技术可以用来解决 TCP/IP 协议的某些安全威胁问题

B.隧道技术的本质是用一种协议来传输另一种协议

C.IPSec 协议中不会使用隧道技术

D.虚拟专用网中可以采用隧道技术

我能过软考分析：

本题在书中第 318 页，对各种安全协议进行了集中的考查，隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式，使用隧道传递的数据（或负载）可以是不同协议的数据帧或包，隧道协议将其它协议的数据帧或包重新封装然后通过隧道发送。协议包括：PPTP 协议、L2TP 协议、IPSec 协议、VPN 协议等。IPSec 中有 AH 头和 ESP 头两种，也有隧道模式和传输模式两种。

参考答案：

（58）C

56. 2016 年下半年试题 61

以下关于 VPN 的叙述中，正确的是（ ）。

A.VPN 指的是用户通过公用网络建立的临时的、安全的连接

B.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

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，不能提供数据加密的功能

我能过软考分析：

本题是重复出现的题目，与 2018 年 61 题基本相同。说明了这个知识点非常重要。VPN 即虚拟专用网，是企业网在因特网等公共网络上的延伸，通过一个私有的通道在公共网络上创建一个临时的、安全的私有连接。

参考答案：

（61）A

57. 2016 年下半年试题 62

扫描技术（ ）。

A. 只能作为攻击工具

B. .只能作为防御工具

C. 只能作为检查系统漏洞的工具

D.既可以作为攻击工具，也可以作为防御工具

我能过软考分析：

本题在书中 308 页，通常的扫描技术采用两种策略：被动式和主动式。被动式策略是基于主机的，主动式策略是基于网络的，它通过网络对远程的目标主机建立连接，并发送请求，分析其返回信息，从而分析远程主机漏洞。既可以作为攻击工具，也可以作为防御工具。一般情况下，能够用来攻击的技术，都可以被防御者来使用，检查系统漏洞。

参考答案：

（62）D

58. 2016 年下半年试题 63

包过滤技术防火墙在过滤数据包时，一般不关心（ ）。

A.数据包的源地址　　B.数据包的协议类型

C.数据包的目的地址　　D.数据包的内容

我能过软考分析：

本题在书中 274 页，防火墙是保护信息系统免遭攻击的一项基本技术，常见的有包过滤防火墙和状态检测防火墙，数据包过滤是通过对数据包的 IP 头和 TCP 头或 UDP 头的检查来实现的，不检查数据包的内容。

参考答案：

（63）D

第 4 章 信息系统安全基础

1. 2018 年上半年试题 10

恶意软件是目前移动智能终端上被不法分子利用最多、对用户造成危害和损失最大的安全成胁类型。数据显示，目前安卓平台恶意软件主要有（ ）四种类型。

A.远程控制木马、话费吸取类、隐私窃取类和系统破坏类

B.远程控制木马、话费吸取类、系统破坏类和硬件资源消耗类

C.远程控制木马、话费吸取类、隐私窃取类和恶意推广

D.远程控制木马、话费吸取类、系统破坏类和恶意推广

我能过软考分析

本题在书中 512 页，考查内容比较细，了解即可，恶意病毒还需要掌握命名规则。恶意软件是目前移动智能终端上被不法分子利用最多、对用户造成危害和损失最大的安全威胁类型。智能终端操作系统的多任务特性，为恶意软件在后台运行提供了条件，而用户对恶意软件的运行毫不知情。数据显示目前 Android 平台恶意软件主要有四种类型:远程控制木马、话费吸取类、隐私窃取类和系统破坏类。

参考答案:

（10）A

2. 2018 年上半年试题 18

计算机取证是将计算机调查和分析技术应用于对潜在的,有法律效力的证据的确定与提取.以下关于计算机取证的描述中,错误的是（ ）。

A.计算机取证包括保护目标计算机系统、确定收集和保存电子证据,必须在开机的状态下进行

B.计算机取证围绕电子证据进行,电子证据具有高科技性、无形性和易破坏性等特点

C.计算机取证包括对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档

D.计算机取证是一门在犯罪进行过程中或之后收集证据的技术

我能过软考分析

本题在书中 490 页，计算机取证包括保护目标计算机系统、确定电子证据、收集电子证据和保存电子证据。对现场计算机的部分通用处理原则有：已经开机的计算机不要关机，关机的计算机不要开机。

参考答案:

（18）A

3. 2018 年上半年试题 22

在访问因特网时,为了防止 Web 页面中恶意代码对自己计算机的损害,可以采取的防范措施是（ ）。

A.将要访间的 Web 站点按其可信度分配到浏览器的不同安全区域

B.利用 SSL 访问 Web 站点

C.在浏览器中安装数字证书

D.利用 IP 安全协议访问 Web 站点

我能过软考分析

本题对应的书中 520 页的知识点，本题考查点是因特网中防止 Web 页面的恶意代码对自己计算机的损害而采取的防范措施。为了防止 Web 页面中恶意代码对自己计算机的损害，可以将要访问的 Web 站点按其可信度分配到浏览器的不同安全区域。划分不同安全区域是浏览器为保护用户计算机免受恶意代码的危害而采取的一种技术。通常浏览器将 Web 站点按其可信度分配到不同的区域，针对不同的区域指定不同的文件下载方式。

参考答案：

（22）A

4. 2018 年上半年试题 25

电子邮件已经成为传播恶意代码的重途径之一,为了有效防止电子邮件中的恶意代码,应该用（ ）的方式阅读电子邮件。

A.应用软件　　B.纯文本　　C.网页　　D.在线

我能过软考分析

本题在书中 474 页，恶意代码网络传播的方式，文本文件通常不会受电子邮件中的恶意代码的感染或携带恶意代码。在电子邮件中，附件或者是带有恶意程序的邮件正文是传播方式。

参考答案：

（25）B

5. 2018 年上半年试题 38

特洛伊木马攻击的威胁类型属于（ ）。

A.旁路控制威胁　　B.网络欺骗　　C.植入威胁　　D.授权侵犯威胁

我能过软考分析

本题在书中 476 页，主要的渗入威胁有假冒、旁路、授权侵犯，主要的植入威胁有特洛伊木马和陷阱。

参考答案：

（38）C

6. 2018 年上半年试题 41

计算机病毒是指一种能够通过自身复制传染,起破坏作用的计算机程序,目前使用的防杀病毒软件的主要作用是（ ）。

A.检查计算机是否感染病毒,清除已感染的任何病毒

B.杜绝病毒对计算机的侵害

C.查出已感染的任何病毒,清除部分已感染病毒

D.检查计算机是否感染病毒,清除部分已感染病毒

我能过软考分析

本题在书中 486 页，防杀毒软件的作用是检查计算机是否感染已知病毒并清除它们，而对于那未知的或者是更高级的病毒无能为力。这一部分需要了解病毒的基本原理和反病毒方法。

参考答案：

（41）D

7. 2018 年上半年试题 45

操作系统的安全审计是指对系统中有关安全的活动进行记录、检查和审核的过程，为了完成审计功能，审计系统需要包括（ ）三大功能模块。

A.审计数据挖掘,审计事件记录及查询、审计事件分析及响应报警

B.审计事件特征提取、审计事件特征匹配、安全响应报警

C.审计事件收集及过滤、审计事件记录及查询,审计事件分析及响应报警系统

D.日志采集与挖掘、安全事件记录及查询、安全响应报警

我能过软考分析

本题在书中 437 页，操作系统的安全审计是指对系统中有关安全的活动进行记录、检查和审核的过程，现有的审计系统包括审计事件收集及过滤、审计事件记录及查询、审计事件分析及响应报警三大功能模块。

参考答案：

（45）C

8. 2018 年上半年试题 46

计算机犯罪是指利用信息科学技术且以计算机为犯罪对象的犯罪行为,与其他类型的犯罪相比,具有明显的特征,下列说法中错误的是（ ）。

A.计算机犯罪有高智能性,罪犯可能掌握一些高科技手段

B.计算机犯罪具有破坏性

C.计算机犯罪没有犯罪现场

D.计算机犯罪具有隐蔽性

我能过软考分析

本题考查了计算机犯罪，在很多章都有涉及，在本章中这部分出现在 490 页计算机取证的部分。计算机犯罪现场是指计算机犯罪嫌疑人实施犯罪行为的地点和遗留有与计算机犯罪有关的痕迹、物品（包括电子数据、电子设备等）或其他物证的场所。

参考答案：

（46）C

9. 2018 年上半年试题 49

文件型病毒不能感染的文件类型是（ ）。

A. B.EXE 类型 C.COM 型 D.HTML 型

我能过软考分析

本题考查书中 467 页的恶意代码。文件型病毒系计算机病毒的一种，主要通过感染计算机中的可执行文件（.exe）和命令文件(.com)。把所有通过操作系统的文件系统进行感染的病毒都称作文件病毒；可以感染所有标准的 DOS 可执行文件：包括批处理文件、DOS 下的可加载驱动程序（.SYS）文件以及普通的 COM/EXE 可执行文件。当然还有感染所有视窗操作系统可执行文件的病毒，可感染文件的种类包括：视窗 3.X 版本，视窗 9X 版本，视窗 NT 和视窗 2000 版本下的可执行文件，后缀名是 EXE、DLL 或者 VXD、SYS。

参考答案：

（49）D

10. 2018 年上半年试题 56

不属于物理安全威胁的是（ ）。

A.电源故障 B.物理攻击 C.自然灾害 D.字典攻击

我能过软考分析

本题考查书中 388 页，物理安全是指在物理媒介层次上对存储和传输的信息加以保护，它是保护计算机网络设备、设施免遭地震、水灾、火灾等环境事故以及人为操作错误或各种计算机犯罪行为而导致破坏的过程。

字典攻击在 P727 有较详细的介绍。字典攻击是攻击者使用一个攻击者认为可能会用在口令中的单词字典，攻击者试图 重现这种口令选择的方法，从输入字典中抽出单词并且使用各种变形规则对输入的单词 进行处理，用经过变形后的单词进一步匹配目标口令。对于一个成功的字典攻击它需要 最原始的单词成为攻击者的输入字典，并且攻击者对字典使用正确的字处理规则。

参考答案：

（56）D

11. 2018 年上半年试题 58

Bell-LaPadual 模型(简称 BLP 模型)是最早的一种安全模型,也是最著名的多级安全策略模型,BLP 模型的简单安全特性是指（ ）。

A.不可上读　　B.不可上写　　C.不可下读　　D.不可下写

我能过软考分析

本题考查书中 409 页的安全模型。Bell-LaPadula 模型(简称 BLP 模型〉是 D.Elliott Bell 和 Leonard J.LaPadula 于 1973 年提出的对应于军事类型安全密级分类的计算机操作系统模型。 BLP 模型是最早的一种计算机多级安全模型，也是受到公认最著名的状态机模型。其特性是不可下写；其简单安全性是指不可上读。各种安全模型的特点都需要理解。

参考答案：

（58）A

12. 2017 年上半年试题 8

计算机取证主要是对电子证据的获取、分析、归档和描述的过程，而电子证据需要在法庭上作为证据展示，就行计算机取证时应当充分考虑电子证据的真实性和电子证据的证明里，除了相关准备之外，计算机取证步骤通常不包括（ ）。

A.保护目标计算机系统　　B.确定电子证据

C.收集电子数据、保护电子证据　　D.清除恶意代码

我能过软考分析

本题考查 490 页计算机取证技术。计算机取证技术的步骤通常包括：保护目标计算机系统、确定电子证据、收集电子证据、保全电子证据。不包括清除恶意代码。

参考答案：

（8）D

13. 2017 年上半年试题 20

工控系统广泛应用于电力、石化、医药、航天等领域，已经成为国家关键基础设施的重要组成部分。作为信息基础设施的基础，电力工控系统安全面临的主要威胁不包括（ ）。

A.内部人为风险　　B.黑客攻击　　C.设备损耗　　D.病毒破坏

我能过软考分析

本题考查书中 514 页工控系统安全问题，考查的内容较细，可以通过技巧判断，设备损耗是设备日常使用带来的，与安全威胁无关。电力工控系统安全面临的主要威胁包括：内部人员风险、黑客攻击、病毒破坏及预设陷阱等，不包括设备损耗。

参考答案：

（20）C

14. 2017 年上半年试题 28

以下恶意代码中，属于宏病毒的是（ ）。

A.Macro.MelissA　　B.Trojan.huigezi.A

C.Worm.Blaster.g　　D.Backdoor.Agobot.frt

我能过软考分析

本题考查书中 471 页计算机病毒的内容。宏病毒的前缀是：Macro；Macro.MelissA 属于宏病毒。Trojan 是特洛伊木马，Worm 是蠕虫，Backdoor 是后门程序。

参考答案：

（28）A

15. 2017 年上半年试题 29

容灾的目的和实质是（ ）。

A.实现对系统数据的备份　　B.提升用户的安全预期

C.保持信息系统的业务持续性　　D.信息系统的必要补充

我能过软考分析

本题考查书中 403 页容灾技术的内容，容灾可以分为数据容灾和应用容灾两类。容灾的实质是保持信息系统的业务持续性。

参考答案：

（29）C

16. 2017 年上半年试题 30

安卓的系统架构从上层到下层包括：应用程序层、应用程序框架层、系统库和安卓运行时、Linux 内核。其中，文件访问控制的安全服务位于（ ）。

A.应用程序层　　B.应用程序架构层

C.系统库和安卓运行时　　D.Linux 内核

我能过软考分析

本题考查书中 833 页，关于智能终端的体系结构。安卓的系统架构从上层到下层包括应用程序层、应用程序框架层、系统库和安卓运行时、Linux 内

核。Android 是基于 Linux2.6 内核，其核心系统服务如安全性、内存管理、进程管理、网路协议以及驱动模型都依赖于 Linux 内核。

参考答案：

（30）D

17. 2017 年上半年试题 34

安全策略表达模型是一种对安全需求与安全策略的抽象概念模型，一般分为自主访问控制模型和强制访问控制模型。以下属于自主访问控制模型的是（ ）。

A.BLP 模型　　B.HRU 模型

C.BN 模型　　D.基于角色的访问控制模型

我能过软考分析

本题考查书中 409 页关于安全策略的问题。70 年代末，M. A. Harrison，W. L. Ruzzo 和 J. D. UIIman 就对自主访问控制进行扩充，提出了客体主人自主管理该客体的访问和安全管理员限制访问权限随意扩散相结合的半自主式的 HRU 访问控制模型。1992 年，Sandhu 等人为了表示主体需要拥有的访问权限，将 HRU 模型发展为 TAM（Typed Access Matrix）模型。随后，为了描述访问权限需要动态变化的系统安全策略，TAM 发展为 ATAM（Augmented TAM）模型。各种安全策略访问控制模型都需要认真理解。

参考答案：

（34）B

18. 2017 年上半年试题 38

文件类型病毒不能感染的文件类型是（ ）。

A.COM 类型　　B.HTML 类型　　C.SYS 类型　　D.EXE 类型

我能过软考分析

本题在 2018 年重复考察。文件型病毒系计算机病毒的一种，主要通过感染计算机中的可执行文件（.exe）和命令文件(.com)。文件型病毒是对计算机的源文件进行修改，使其成为新的带毒文件。一旦计算机运行该文件就会被感染，从而达到传播的目的。当然还有感染所有视窗操作系统可执行文件的病毒，可感染的文件类型包括后缀名是 EXE、DLL 或者 VXD、SYS。本题需要了解文件的后缀名和文件类型。

参考答案：

（38）B

19. 2017 年上半年试题 40

操作系统的安全审计是指对系统中有关安全的活动进行记录、检查和审核的过程，现有的审计系统包括（ ）三大功能模块。

A.审计事件收集及过滤、审计事件记录及查询、审计事件分析及响应报警

B.审计书籍挖掘、审计事件记录及查询、审计事件分析及响应报警

C.系统日志采集与挖掘、安全时间记录及查询、安全响应报警

D.审计事件特征提取、审计事件特征匹配、安全响应报警

我能过软考分析

本题也在 2018 年考试题目中重复考察。操作系统的安全审计是指对系统中有关安全的活动进行记录、检查和审核的过程，现有的审计系统包括审计事件收集及过滤、审计事件记录及查询、审计事件分析及响应报警三大功能模块。

参考答案：

（40）A

20. 2017 年上半年试题 41

计算机病毒的生命周期一般包括（ ）四个阶段。

A.开发阶段、传播阶段、发现阶段、清除阶段

B.开发阶段、潜伏阶段、传播阶段、清除阶段

C.潜伏阶段、传播阶段、发现阶段、清除阶段

D.潜伏阶段、传播阶段、触发阶段、发作阶段

我能过软考分析

本题考查书中 471 页计算机病毒。计算机病毒的生命周期一般包括潜伏阶段、传播阶段、触发阶段、发作阶段四个阶段。

参考答案：

（41）D

21. 2017 年上半年试题 48

以下不属于网络安全控制技术的是（ ）。

A.防火墙技术　　B.数据备份技术

C.入侵检测技术　　D.访问控制技术

我能过软考分析

防火墙技术、入侵检测技术和访问控制技术是在第三章讲解的网络安全防御技术，数据备份技术是在本章中讲解的内容。数据备份是容灾的基础，是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程，其不属于网络安全控制技术。

参考答案：

（48）B

22. 2017 年上半年试题 70

强制访问控制（MAC）是一种不允许主体干涉的访问控制类型。根据 MAC 的安全基本，用户与访问的信息的读写关系有四种类型，其中能保证数据完整性的读写组合方式是（ ）。

A.上读-下写　　B.上读-上写

C.下读-下写　　D.下读-上写

我能过软考分析

本题考查书中 416 页的安全模型。上读下写方式保证了数据的完整性；上写下读方式则保证了信息的秘密性。各种安全模型的特点都需要了解。

参考答案：

（70）A

23. 2016 年下半年试题 18

计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与提取。以下关于计算机取证的描述中，错误的是（ ）。

A.计算机取证包括对以磁介质编码信塞方式存储韵计算机证据的保护、确认、提取和归档

B.计算机取证围绕电子证据进行，电子证据具有高科技性、无形性和易破坏性等特点

C.计算机取证包括保护目标计算机系统、确定收集和保存电子证据，必须在开机的状态下进行

D.计算机取证是上门在犯罪进行过程中或之后收集证据的技术

我能过软考分析

本题考查书中 490 页计算机取证的内容，也在 2018 年进行了重复考察。计算机取证包括保护目标计算机系统、确定电子证据、收集电子证据和保存电

子证据。对现场计算机的部分通用处理原则有：已经开机的计算机不要关机，关机的计算机不要开机。

参考答案：

（18）C

24. 2016 年下半年试题 25

电子邮件是传播恶意代码的重要途径，为了防止电子邮件中的恶意代码，应该用（ ）方式阅读电子邮局件。

A.网页　　B.纯文本　　C.程序　　D.会话

我能过软考分析

本题也在 2017 年进行了重复考查。文本文件通常不会受电子邮件中的恶意代码的感染或携带恶意代码。

参考答案：

（25）B

25. 2016 年下半年试题 38

特洛伊木马攻击的威胁类型属于（ ）。

A.授权侵犯威胁　　B.渗入威胁

C.植入威胁　　D.旁路控制威胁

我能过软考分析

本题也进行过重复考察，主要的渗入威胁有假冒、旁路、授权侵犯，主要的植入威胁有特洛伊木马和陷阱。

参考答案：

（38）C

26. 2016 年下半年试题 41

目前使用的防杀病毒软件的作用是（ ）。

A.检查计算机是否感染病毒；清除已感染的任何病毒

B.杜绝病毒对计算机的侵害

C.查出已感染的任何病毒，清除部分已感染病毒

D.检查计算机是否感染病毒，清除部分已感染病毒

我能过软考分析

本题考查书中 486 页的反病毒技术。防杀毒软件的作用是检查计算机是否感染已知病毒并清除它们，而对于那未知的或者是更高级的病毒无能为力。

参考答案：

（41）D

27. 2016 年下半年试题 49

病毒的引导过程不包含（ ）。

A.保证计算机或网络系统的原有功能

B.窃取系统部分内存

C.使自身有关代码取代或扩充原有系统功能

D.删除引导扇区

我能过软考分析

本题考查书中 474 页的计算机病毒的内容。病毒的引导过程包括：

（1）驻留内存病毒若要发挥其破坏作用，一般要驻留内存。为此就必须开辟所用内存空间或覆盖系统占用的部分内存空间，有的病毒不驻留内存。

（2）窃取系统控制权在病毒程序驻留内存后，必须使有关部分取代或扩充系统的原有功能，并窃取系统的控制权。此后病毒程序依据其设计思想，隐蔽自己，等待时机，在条件成熟时，再进行传染和破坏。

（3）恢复系统功能病毒为隐蔽自己，驻留内存后还要恢复系统，使系统不会死机，只有这样才能等待时机成熟后，进行感染和破坏的目的。

参考答案：

（49）D

28. 2016 年下半年试题 51

安全备份的策略不包括（ ）。

A.所有网络基础设施设备的配置和软件

B.所有提供网络服务的服务器配置

C.网络服务

D.定期验证备份文件的正确性和完整性

我能过软考分析

本题考查了对备份的理解。网络服务是指一些在网络上运行的、面向服务的、基于分布式程序的软件模块，通常采用 HTTP 和 XML 等互联网通用标准，使人们可以在不同的地方通过不同的终端设备访问 WEB 上的数据，如网上订票，查看订座情况。

参考答案：

（51）C

29. 2016 年下半年试题 54

智能卡是指粘贴或嵌有集成电路芯片的一种便携式卡片望胶，智能卡的片内操作系统(COS)是智能卡苍片内的一个监控软件，以下不属于 COS 组成部分的是（ ）。

A.通讯管理模块　　B.数据管理模块

C.安全管理模块　　D.文件管理模块

我能过软考分析

本题考查书中 500 页智能卡的内容，考查相对较细。智能卡的片内操作系统（COS）包括通讯管理模块、安全管理模块、文件管理模块及应用管理模块等四个模块。

参考答案：

（54）B

30. 2016 年下半年试题 56

不属于物理安全威胁的是（ ）。

A.自然灾害　　B.物理攻击　　C.硬件故障　　D.系统安全管理人员培训不够

我能过软考分析

1. 本题考查书中 388 页物理安全的内容，后来也进行了重复考查。
2. 物理安全是指在物理媒介层次上对存储和传输的信息加以保护，它是保护计算机网络设备、设施免遭地震、水灾、火灾等环境事故以及人为操作错误或各种计算机犯罪行为而导致破坏的过程。
3. 物理攻击：可以从两方面理解，1 是直接损坏，这属于物理安全威胁。2 是基于物理的攻击，它是利用密码系统实现时泄露的额外信息，推导出密码系统中的秘密参数，主要方法包括：功耗攻击、电磁场攻击和时间攻击。核心是泄露。
4. 系统安全管理人员的培训属于人员安全管理。

参考答案：

（56）D

第 5 章 应用系统安全基础

1. 2018 年上半年试题 8

面向数据挖掘的隐私保护技术主要解高层应用中的隐私保护问题，致力于研究如何根据不同数据挖掘操作的特征来实现对隐私的保护，从数据挖的角度,不属于隐私保护技术的是（ ）。

A.基于数据分析的隐私保护技术　　B.基于微据失真的隐私保护技术

C.基于数据匿名化的隐私保护技术　　D.基于数据加密的隐私保护技术

我能过软考分析：

本题在书中的第 595 页，从数据挖掘的角度，目前的隐私保护技术主要可以分为三类：（1）基于数据失真的隐私保护技术；（2）基于数据加密的隐私保护技术；（3）基于数据匿名化的隐私保护技术。基于数据分析的技术可以说是一种对隐私进行攻击的技术。

参考答案：

（8）A

2. 2018 年上半年试题 20

数字水印技术通过在多媒体数据中嵌入隐蔽的水印标记,可以有效实现对数字多媒体数据的版权保护等功能。以下不属于数字水印在数字版权保护中必须满足的基本应用需求的是（ ）。

A.保密性　　B.隐蔽性　　C.可见性　　D.完整性

我能过软考分析：

本题在书中 568 页，数字水印技术在数字版权保护中必须满足的基本应用需求是保密性、隐蔽性、完整性。绝大多数数字水印都是不可见的。

参考答案：

（20）C

3. 2018 年上半年试题 30

移动用户有些属性信息需要受到保护,这些信息一旦泄露,会对公众用户的生命财产安全造成威胁.以下各项中,不需要被保护的属性是（ ）。

A.终端设备信息　　B.用户通话信息

C.用户位置信息　　D.公众运营商信息

我能过软考分析：

本题考查对隐私保护的理解。公众运营商是公开信息，比如移动公司，不需要被保护。

参考答案：

（30）D

4. 2018 年上半年试题 33

典型的水印攻击方式包括:鲁棒性攻击、表达攻击、解释攻击和法律攻击.其中鲁棒性攻击是指在不损害图像使用价值的前提下减弱、移去或破坏水印的一类攻击方式.以下不属于鲁棒性攻击的是（ ）。

A.像素值失真攻击　　B.敏感性分析攻击

C.置乱攻击　　D.梯度下降攻击

我能过软考分析：

本题在书中 557 页，鲁棒性是指加入国像中的水印必须能够承受施加于图像的变换操作(如:加入噪声、 滤波、有损压缩、重采样、 D/A 或 AID 转换等)，不会因变换处理而丢失，水印信息经检验提取后应清晰可辨；水印攻击方法可以分为 4 类：健壮性攻击、表达攻击、解释攻击和合法攻击，其中前三类可归类为技术攻击；健壮性攻击以减少或消除数字水印的存在为目的，包括像素值失真攻击、敏感性分析攻击和梯度下降攻击等；这些方法并不能将水印完全除去，但可能充分损坏水印信息，属于鲁棒性攻击方式。置乱攻击是指在将水印图像提交水印检测器之前，先对图像的像素值进行置乱，通过水印检测器之后再进行逆置乱，这种方式可以将置乱的图像作为秘密信息再进行隐藏，可以很大限度的提高隐蔽载体的鲁棒性。

参考答案：

（33）C

5. 2018 年上半年试题 40

SSL 协议是对称密码技术和公钥密码技术相结合的协议,该协议不能提供的安全服务是（ ）。

A.可用性　　B.完整性　　C.保密性　　D.可认证性

我能过软考分析：

本题在书中 548 页，SSL 安全套接层是为网络通信提供安全及数据完整性的一种安全协议。其提供的安全服务包括：1、认证用户和服务器，确保数据发送到正确的客户机和服务器；2、加密数据以防止数据中途被窃取；3、维护数据的完整性，确保数据在传输过程中不被改变。可用性的保证一般要靠提高网络结构的鲁棒性来实现。

参考答案：

（40）A

6. 2018 年上半年试题 59

安全电子交易协议 SET 是由 VISA 和 Mastercard 两大信用卡组织联合开发的电子商务安全协议,以下关于 SET 的叙述中,正确的是（ ）。

A. SET 通过向电子商务各参与方发放验证码来确认各方的身份,保证网上支付的安全性

B. SET 不需要可信第三方认证中心的参与

C. SET 要实现的主要目标包括保障付款安全、确定应用的互通性和达到全球市场的可接受性

D. SET 协议主要使用的技术包括:流密码、公钥密码和数字签名等

我能过软考分析：

本题在书中 532 页，SET 协议是应用层的协议，是一种基于消息流的协议，一个基于可信的第三方认证中心的方案。SET 改变了支付系统中各个参与者之间交互的方式，电子支付始于持卡人。重点掌握 SET 的特点和处理流程。

参考答案：

（59）C

7. 2017 年上半年试题 9

数字水印是通过数字信号处理的方法，在数字化的多媒体数据中，嵌入隐蔽的水印标记。其应用领域不包括（ ）。

A.版权保护　　B.票据防伪

C.证据篡改鉴定　　D.图像数据

我能过软考分析：

本题在书中 557 页，数字水印的应用领域包括版权保护、加指纹、标题与注释、篡改提示、使用控制等。不包括图像数据。

参考答案：

（9）D

8. 2017 年上半年试题 32

SSL 协议是对称密码和公钥密码技术相结合的协议，该协议不能提供的安全服务是（ ）。

A.保密性　　B.可用性　　C.完整性　　D.可认特性

我能过软考分析：

本题在书中 548 页，在 2018 年进行了重复考察，SSL(安全套接层)，是为网络通信提供安全及数据完整性的一种安全协议，它能提供保密性、完整性、可认证性等安全服务，但不能提供可用性。

参考答案：

（32）B

9. 2017 年上半年试题 59

信息隐藏主要研究如何将机密信息秘密隐藏于另一公开的信息中。以下关于利用多媒体数据来隐藏机密信息的叙述中，错误的是（ ）。

A.多媒体信息本身有很大的冗余性

B.多媒体信息本身编码效率很高

C.人眼或人耳对某些信息由一定的掩蔽效应

D.信息嵌入到多媒体信息中不影响多媒体本身的传送和使用

我能过软考分析：

本题在书中 557 页，由于多媒体信息本身有很大的冗余性，一般多媒体信息本身编码效率不高。

参考答案：

（59）B

10. 2017 年上半年试题 69

面向数据挖掘的隐私保护技术主要解决高层应用中的隐私保护问题，致力于研究如何根据不同数据挖掘操作的特征来实现对隐私的保护。从数据挖掘的角度看，不属于隐私保护技术的是（ ）。

A.基于数据失真的隐私保护技术

B.基于数据匿名化的隐私保护技术

C.基于数据分析的隐私保护技术

D.基于数据加密的隐私保护技术

我能过软考分析：

本题在 2018 年进行了重复性考查，从数据挖掘的角度，目前的隐私保护技术主要可以分为三类：

（1）基于数据失真的隐私保护技术；

（2）基于数据加密的隐私保护技术；

（3）基于数据匿名化的隐私保护技术。

参考答案：

（69）C

11. 2016 年下半年试题 20

数字水印技术通过在数字化婀多媒体数据中嵌入隐蔽的水印标志，可以有效实现对数字多媒体数据的版权保护等功能。以下各项中，不属于数字水印在数字版权保护中必须满足的其本应用需求的是（ ）。

A.安全性　　B.隐蔽性　　C.鲁棒性　　D.可见性

我能过软考分析：

本题在 17、18 年都进行了重复性考察，数字水印必须满足的基本应用需求是安全性、隐蔽性、鲁棒性。

参考答案：

（20）D

12. 2016 年下半年试题 52

以下关于安全套接字层协议(SSL)的叙述中，错误的是（ ）。

A.是一种应用层安全协议　　B.为 TCP/IP 口连接提供数据加密

C.为 TCP/IP 连接提供服务器认证　　D.提供数据安全机制

我能过软考分析：

本题在书中 548 页，SSL 位于应用层和传输层之间，它可以为任何基于 TCP 等可靠连接的应用层协议提供安全性保证。

参考答案：

（52）A

13. 2016 年下半年试题 59

安全电子交易协议 SET 是由 VISA 和 MasterCard 两大信用卡组织联合开发的电子商务安全协议。以下关于 SET 的叙述中，正确的是（ ）。

A. SET 是一种基于流密码的协议

B. SET 不需要可信的第三方认证中心的参与

C. SET 要实现的主要目标包括保障付款安全、确定应用的互通性和达到全球市场的可接受性

D. SET 通过向电子商务各参与方发放验证码来确认各方的身份，保证网上支付的安全性

我能过软考分析：

本题在 2018 年进行了重复性考查。SET 协议是应用层的协议，是一种基于消息流的协议，一个基于可信的第三方认证中心的方案。SET 改变了支付系统中各个参与者之间交互的方式，电子支付始于持卡人。

参考答案：

（59）C

14. 2016 年下半年试题 10

电子商务系统除了面临一般的信息系统所涉及的安全威胁之外，更容易成为不法分子的攻击目标，其安全性需求普遍高于一般的信息系统。电子商务系统中的电子交易安全需求不包括（ ）。

A.交易的真实性

B.交易的保密性和完整性

C.交易的可撤销性

D.交易的不可抵赖性

试题分析

电子商务交易安全需求包括交易的保密性、完整性、真实性、不可抵赖性。交易的可撤销性不属于电子商务交易安全需求。

试题答案

（10）C

第 6 章 网络安全技术与产品

1. 2018 年上半年试题 9

从网络安全的角度看，以下原则中不属于网络安全防护体系在设计和实现时需要遵循的基本原则的是（ ）。

A.最小权限原则　　B.纵深防御原则

C.安全性与代价平衡原则　　D.Kerckhoffs 原则

我能过软考分析：

本题在教材 621 页，从网络安全角度看，网络安全防护系统的设计与实现应按照以下原则:最小权限原则、纵深防御原则、防御多样性原则、防御整体性原则、安全性与代价平衡原则、网络资源的等级性原则。密码学上的柯克霍夫原则（Kerckhoffs's principle）系由奥古斯特·柯克霍夫在 19 世纪提出：即使密码系统的任何细节已为人悉知，只要密匙（key，又称密钥或密钥）未泄漏，它也应是安全的。

试题答案：

（9）D

2. 2018 年上半年试题 12

对信息进行均衡、全面的防护，提高整个系统“安全最低点”的全性能，这种安全原则被称为（ ）。

A.最小特权原则　　B.木桶原则

C.等级化原则　　D.最小泄露原则

我能过软考分析：

本题在书中 621 页，“木桶原则”，即，对信息均衡、全面地进行保护。 “木桶的最大容积取决于最短的一块木板”，攻击者必然在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测（包括模拟攻击），是设计信息安全系统的必要前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段；根本目标是提高整个系统的“安全最低点”的安全性能。

“整体性原则”，即，安全防护、监测和应急恢复。 没有百分之百的网络系统信息安全，因此要求在网络被攻击、破坏事件的情况下，必须尽可能快地恢复网络的服务，减少损失。所以信息安全系统应该包括三种机制：安全防护机制；安全监测机制；安全恢复机制。安全防护机制是根据具体系统存在的各种安全漏洞和安全威胁采取相应的防护措施，避免非法攻击的进行；安全监测机制是监测系统的运行情况，及时发现和制止对系统进行的各种攻击；安全恢复机制是在安全防护机制失效的情况下，进行应急处理和尽量、及时地恢复信息，减少攻击的破坏程度。

“等级性”，即，安全层次和安全级别。 良好的信息安全系统必然是分为不同级别的，包括：对信息保密程度分级（绝密、机密、秘密、普密）；对用户操作权限分级（面向个人及面向群组），对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、链路层等），从而针对不同级别的安全对象，提供全面的、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

“动态化”原则，即，整个系统内尽可能引入更多的可变因素，并具有良好的扩展性。 被保护的信息的生存期越短、可变因素越多，系统的安全性能就越高。安全系统要针对网络升级保留一定的冗余度，整个系统内尽可能引入更多的可变因素。

试题答案：

（12）B

3. 2018 年上半年试题 29

人为的安全威胁包括主动攻击和被动攻击,以下属于被动攻击的是（ ）。

A.流量分析　　B.后门　　C.拒绝服务攻击　　D.特洛伊木马

我能过软考分析：

本题是对 3.3 节知识和第 6 章 629 页内容的综合考察，流量分析是指通过一定的技术手段，实时监测用户网络七层结构中各层的流量分布，进行协议、流量的综合分析，从而有效的发现、预防网络流量和应用上的瓶颈，为网络性能的优化提供依据，属于被动攻击。

试题答案：

（29）A

4. 2018 年上半年试题 44

深度流检测技术是一种主要通过判断网络流是否异常来进行安全防护的网络安全技术,深度流检测系统通常不包括（ ）。

A.流特征提取单元　　B.流特征选择单元

C.分类器　　D.响应单元

我能过软考分析：

本题在书中 634 页，深度流检测技术主要分为三部分：流特征选择、流特征提取、分类器。

试题答案：

（44）D

5. 2018 年上半年试题 64

以下关于网络流量监控的叙述中,不正确的是（ ）。

A.网络流量监控分析的基础是协议行为解析技术

B.数据采集探针是专门用于获取网络链路流量数据的硬件设备

C.流量监控能够有效实现对敏感数据的过滤

D.流量监测中所监测的流量通常采集自主机节点、服务器、路由器接口、链路和路径等

我能过软考分析：

本题在书中 629 页，流量监控是一种被动攻击的方式，流量监控指的是对数据流进行的监控，通常包括出数据、入数据的速度、总流量。不能过滤敏感数据。

试题答案：

（64）C

6. 2017 年上半年试题 18

ISO 制定的安全体系结构描述了 5 种安全服务，以下不属于这 5 种安全服务的是（ ）。

A.鉴别服务　　B.数据报过滤　　C.访问控制　　D.数据完整性

我能过软考分析：

本题在书中 618 页。ISO 安全体系结构的 5 种安全服务包括：鉴别服务、访问控制、数据完整性、数据保密性、抗抵赖性。ISO 的安全体系需要重点掌握。

试题答案：

（18）B

7. 2017 年上半年试题 21

对日志数据进行审计检查，属于（ ）类控制措施。

A.预防　　B.检测　　C.威慑　　D.修正

我能过软考分析：

本题在书中 713 页，对日志数据进行审计检查是属于检测类的控制措施。

审计系统的目标至少包括：确定和保持系统活动中每个人的责任；确认重建事件的 发生；评估损失；监测系统问题区；提供有效的灾难恢复依据；提供阻止不正当使用系 统行为的依据；提供案件侦破证据。

审计通过对所关心的事件进行记录和分析来实现。因此审计过程包括审计发生器、 日志记录器、日志分析器和报告机制几部分。

安全操作系统的审计记录一般应包括如下信息：事件的日期和时间、代表正在进行 事件的主体的唯一标识符、事件的类型、事件的成功与失败等。对于标识与鉴别事件，

审计记录应该记录事件发生的源地点（如终端标识符)。对于将一个客体引入某个用户地址空间的事件以及删除客体的事件，审计记录应该包括客体名以及客体的安全级。

审计日志是存放审计结果的二进制结构文件。每次审计进程开启后，都会按照已设 定好的路径和命名规则产生一个新的日志文件。

试题答案：

（21）B

8. 2016 年下半年试题 12

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.动态化原则　　B.木桶原则　　C.等级性原则　　D.整体原则

我能过软考分析：

本题在 2018 年进行了重复性考查。“木桶原则”，即，对信息均衡、全面地进行保护。 “木桶的最大容积取决于最短的一块木板”，攻击者必然在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测（包括模拟攻击），是设计信息安全系统的必要前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段；根本目标是提高整个系统的“安全最低点”的安全性能。

“整体性原则”，即，安全防护、监测和应急恢复。 没有百分之百的网络系统信息安全，因此要求在网络被攻击、破坏事件的情况下，必须尽可能快地恢复网络的服务，减少损失。所以信息安全系统应该包括三种机制：安全防护机制；安全监测机制；安全恢复机制。安全防护机制是根据具体系统存在的各种安全漏洞和安全威胁采取相应的防护措施，避免非法攻击的进行；安全监测机制是监测系统的运行情况，及时发现和制止对系统进行的各种攻击；安全恢复机制是在安全防护机制失效的情况下，进行应急处理和尽量、及时地恢复信息，减少攻击的破坏程度。

“等级性”，即，安全层次和安全级别。 良好的信息安全系统必然是分为不同级别的，包括：对信息保密程度分级（绝密、机密、秘密、普密）；对用户操作权限分级（面向个人及面向群组），对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、链路层等），从而针对不同级别的安全对象，提供全面的、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

“动态化”原则，即，整个系统内尽可能引入更多的可变因素，并具有良好的扩展性。 被保护的信息的生存期越短、可变因素越多，系统的安全性能

就越高。安全系统要针对网络升级保留一定的冗余度，整个系统内尽可能引入更多的可变因素。

试题答案：

（12）B

9. 2016 年下半年试题 43

下列报告中，不属于信息安全风险评估识别阶段输出报告的是（ ）。

A.资产价值分析报告　　B.风险评估报告

C.威胁分析报告　　D.已有安全措施分析报告

我能过软考分析：

本题在书中 677 页，风险评估报告属于信息安全风险分析阶段的输出报告。在网络安全风险评估实施这个部分需要了解各个阶段的主要工作、输出的报告。

试题答案：

（43）B

10. 2016 年下半年试题 46

深度流检测披术就是以流为基本研究对象，判断网络流是否异常的一种网络安全技术，其主要组成部分通常不包括（ ）。

A.流特征选择　　B.流特征提取

C.分类器　　D.响应

我能过软考分析：

这道题在 2018 年进行了重复性的考查。深度流检测技术主要分为三部分：流特征选择、流特征提取、分类器。

试题答案：

（46）D

11. 2016 年下半年试题 64

以下关于网络流量监控的叙述中，不正确的是（ ）。

A.流量监测中所监测的流量通常采集自主机节点、服务器、路由器接口、链路和路径等

B.数据采集探针是专门用于获取网络链路流量数据的硬件设备

C.流量监控能够有效实现对敏感数据的过滤

D.网络流量监控分析的基础是协议行为解析技术

我能过软考分析：

本题在书中 629 页，也是在 2018 年进行了重复考察。流量监控指的是对数据流进行的监控，通常包括出数据、入数据的速度、总流量。不能过滤敏感数据。

试题答案：

（64）C

第 7 章 信息系统安全工程

1. 2018 年上半年试题 19

在缺省安装数据库管理系统 MySQL 后，root 用户拥有所有权限且是空口令，为了安全起见，必须为 root 用户设置口令，以下口令设置方法中，不正确的是（ ）。

A.使用 MySQL 自带的命令 mysqladmin 设置 root 口令

B.使用 setpassword 设置口令

C.登录数据库,修改数据库 mysql 下 user 表的字段内容设置口令

D.登录数据库,修改数据库 mysql 下的访问控制列表内容设置口令

我能过软考分析：

本题在书中 775 页，后几章的内容容易出现在主观题中，需要背记的东西较多。有 3 种方式为 root 账户指定密码：使用 SET PASSWORD 语句；使用 mysqladmin 命令行客户端程序；使用 UPDATE 语句，使用 UPDATE 直接修改 user 表。

参考答案：

（19）D

2. 2018 年上半年试题 24

Linux 系统的运行日志存储的目录是（ ）。

A./var/log　　B./usr/log　　C./etc/log　　D./tmp/log

我能过软考分析：

本题在书中 773 页，Linux 系统所有的日志文件都在/var/log 目录下。Linux 的操作相对比较复杂，重点掌握书中讲到的内容，在做题中适当拓展。

参考答案：

（24）A

3. 2017 年上半年试题 6

在信息安全防护体系设计中，保证“信息系统中数据不被非法修改、破坏、丢失等”是为了达到防护体系的（ ）目标。

A.可用性　　B.保密性　　C.可控性　　D.完整性

我能过软考分析：

本题再次考查信息安全五元组的美容。完整性是指所有资源只能由授权方或以授权的方式进行修改，即信息未经授权不能进行改变的特性。信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

参考答案：

（6）D

4. 2017 年上半年试题 10

信息系统安全测评方法中模糊测试时一种黑盒测试技术，它将大量的畸形数据输入到目标程序中，通过监测程序的异常来发现被测程序中可能存在的安全漏洞、关于模糊测试，一下说法错误的是（ ）。

A.与白盒测试相比，具有更好的适用性

B.模糊测试是一种自动化的动态漏洞挖掘技术，不存在误报，也不需要人工进行大量的逆向分析工作

C.模糊测试不需要程序的源代码就可以发现问题

D.模糊测试受限于被测系统的内容实现细节和复杂度

我能过软考分析：

本题在书中 785 页，模糊测试是属于黑盒测试，黑盒测试不受限于被测系统的内部实现细节和复杂度。黑盒测试可以理解为在不知道软件内部构造的前提下，对软件进行测试，白盒测试是已知软件实现细节的前提下进行的测试。

参考答案：

（10）D

5. 2017 年上半年试题 12

（ ）是一种通过对信息进行均衡、安全的防护，体改整个系统最低安全性能的原则。

A.木桶原则　　B.保密原则　　C.等级化原则　　D.最小特权原则

我能过软考分析：

从技术角度来说，确定具体信息系统的安全策略主要有：木桶原则、整体原则、有效性与实用性原则、安全性评价原则、等级性原则和动态化等 6 项原则。其中，木桶原则是指对信息均衡、全面地进行安全保护，提高整个系统的“安全最低点”的安全性能。

参考答案：

（12）A

6. 2017 年上半年试题 19

在使用复杂度不高的口令时，容易产生弱口令的安全脆弱性，被攻击者利用，从而破解用户账户，下列设置的口令中，（ ）具有最好的口令复杂度。

A.morrison　　B.Wm.$*F2m5@　C.27776394　　D.wangjing1977

我能过软考分析：

本题在书中 724 页，现在网站要求密码复杂性必须符合下列最低要求：不能包含用户的账户名；不能包含用户姓名中超过两个连续字符的部分；至少有六个字符长；密码总必须包含一下 4 类字符中的三类字符：

1、英文大写字母（A-Z）

2、英文小写字母(a-z)

3、10 个基本数字（0-9）

4、特殊符号（！@#￥%等）。

参考答案：

（19）B

7. 2017 年上半年试题 64

以下不属于代码静态分析的方法是（ ）。

A.内存扫描　　B.模式匹配　　C.定理证明　　D.模型检测

我能过软考分析：

本题在书中 793 页，代码静态分析的方法包括模式匹配、定理证明、模型检测等，不包括内存扫描。内存扫描是通过在程序执行过程中内存的变化来分析代码，属于动态分析的方法。

参考答案：

（64）A

8. 2016 年下半年试题 22

在访问因特网时，为了防止 Web 页面中恶意代码对自己计算机的损害，可以采取的防范措施是（ ）。

A.将要访问的 Web 站点按其可信度分配到浏览器的不同安全区域

B.在浏览器中安装数字证书

C.利用 IP 安全协议访问 Web 站

D.利用 SSL 访问 Web 站点

我能过软考分析：

本题在书中 804 页。本题考查点是因特网中防止 Web 页面的恶意代码对自己计算机的损害而采取的防范措施。为了防止 Web 页面中恶意代码对自己计算机的损害，可以将要访问的 Web 站点按其可信度分配到浏览器的不同安全区域。划分不同安全区域是浏览器为保护用户计算机免受恶意代码的危害而采取的一种技术。通常浏览器将 Web 站点按其可信度分配到不同的区域，针对不同的区域指定不同的文件下载方式。

参考答案：

（22）A

9. 2016 年下半年试题 47

一个全局的安全框架必须包含的安全结构因素是（ ）。

A.审计、完整性、保密性、可用性

B.审计、完整性、身份认证、保密性，可用性、真实性

C.审计、完整性、身份认证、可用性

D.审计、完整性、身份认证、保密性

我能过软考分析：

本题在书中 748 页。一个全局的安全框架必须包含的安全结构因素有审计、完整性、身份认证、保密性，可用性、真实性。

参考答案：

（47）B

张老师的信息安全工程师课程：

第二部分　案例分析分类解析

考点 1：密码学案例分析

1. 2019 年上半年试题 2

阅读下列说明和表，回答问题 1 至问题 3,将解答填入答题纸的对应栏内。

[说明]

密码学作为信息安全的关键技术，在信息安全领域有着广泛的应用。密码学中，根据加密和解密过程所采用密钥的特点可以将密码算法分为两类:对称密码算法和非对称密码算法。此外，密码技术还用于信息鉴别、数据完整性检验、数字签名等。

[问题 1] (6 分)

信息安全的基本目标包括真实性、保密性、完整性、不可否认性、可控性、可用性、可审查性等。密码学的三大安全目标 CIA 分别表示什么?

[问题 2] (5 分)

仿射密码是一种典型的对称密码算法。仿射密码体制的定义如下:

令明文和密文空间 M=C=Z26，密钥空间 K={(k1,k2)∈Z26*Z26:gcd(k1,26)= 1}。对任意的密钥 key= (k1,k2)∈K, x∈M,y∈C，定义加密和解密的过程如下:

加密: ekey (x) = (k1x, k2’)mod26

解密: dkey (x) =$k1^{-1}$(y- k2)mod26

其中 $k1^{-1}$ 表示 k1 在 Z26 中的乘法逆元，即 $k1^{-1}$ 乘以 k1 对 26 取模等于 1, gcd(k1,26)=1 表示 k 与 26 互素。

设已知仿射密码的密钥 Key=(11, 3)，英文字符和整数之间的对应关系如表 2.1。则:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(1)整数 11 在 Z26 中的乘法逆元是多少?

(2)假设明文消息为“SEC"，相应的密文消息是什么?

[问题 3] (2 分)

根据表 2.1 的对应关系，仿射密码中，如果已知明文“E"对应密文“C"，明文“T”对应密文“F”，则相应的 key=(k1, k2)等于多少?

参考答案:

答案

[问题 1]

保密性、完整性和可用性。

[问题 2]

(1) 19

(2) TVZ

[问题 3]

K1=21; K2=22

试题分析

[问题 1]

密码学的三大安全目标 CIA 分别表示:

(1) 保密性:保密性是确保信息仅被合法用户访问，而不被地露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。

(2)完整性:完整性是指所有资源只能由授权方或以授权的方式进行修改,即信息未经授权不能进行改变的特性。信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

(3)可用性:可用性是指所有资源在适当的时候可以由授权方访问，即信息可被授权实体访问并按需求使用的特性。信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

[问题 2]

(1) 由 $K*K^{-1}\equiv 1 \bmod (26)$，将 11 代入式中，计算 $11*K^{-1} \bmod (26)=1$; K^{-1} 为 19。

(2) 将 SEC 所对应的数字代入加密表达式可得:

(11*18+3) mod (26) =19=T;

(11*4+3) mod (26) =21=V;

(11*2+3) mod (26) =25=Z。

[问题 3] .

根据表中，明文 E、T 所对应的数字为 4、19; 密文 C、F 所对应的数字为 2、5,代入加密表达式组成二元一次方程组:

(K1*4+K2) mod (26) =2;

(K1*19+K2) mod (26) =5;

求解方程组可得，K1=21; K2=22

2. 2019 年上半年试题 3

阅读下列说明，回答问题 1 至问题 5,将解答填入答题纸的对应栏内。

[说明]

假设用户 A 和用户 B 为了互相验证对方的身份,设计了如下通信协议:

1.A→B: RA

2.B→A: f（PAB||RA)IIRB

3.A→B: f（PAB||____）

其中:RA、RB 是随机数，PAB 是双方事先约定并共享的口令，“||”表示连接操作。f 是哈希函数。

[问题 1](2 分)

身份认证可以通过用户知道什么、用户拥有什么和用户的生理特征等方法来验证。请问上述通信协议是采用哪种方法实现的?

[问题 2](2 分)

根据身份的互相验证需求，补充协议第 3 步的空白内容。

[问题 3](2 分)

通常哈希函数需要满足下列性质:单向性、抗弱碰撞性、抗强碰撞性。如果某哈希函数具备:找到任何满足 f(x)=f(y)的偶对(x，y)在计算上是不可行的，请说明其满足哪条性质。

[问题 4] (2 分)

上述协议不能防止重放攻击，以下哪种改进方式能使其防止重放攻击?

(1)在发送消息加上时间参量。

(2)在发送消息加上随机数。

[问题 5] (4 分)

如果将哈希函数替换成对称加密函数,是否可以提高该协议的安全性?为什么?

试题分析

[问题 1]

口令是接收双方预先约定的秘密数据，它用来验证用户知道什么。

[问题 2]

第 3 步中用户 A 将共享口令 PAB 和随机值 RB 用 hash 函数加密后，发送给用户 B，以便用户 B 对其身份进行验证。

[问题 3]

Hash 函数满足以下性质:

单向性:对任何给定的 hash 函数值 h，找到满足 H(x)等于 h 的 x 在计算上是不可行的。

抗弱碰撞性:对任何给定的分组 x，找到满足 y 不等于 x 且 H(x)=H(y)的 y 在计算上是不可行的。

抗强碰撞性:找到任何满足 H(x)=H(y)的偶对(x,y)在计算上是不可行的。

[问题 4]

重放攻击是指入侵者从网络上截取主机 A 发送给主机 B 的报文，并把由 A 加密的报文发送给 B,使主机 B 误以为入

侵者就是主机 A，然后主机 B 向伪装成 A 的入侵者发送应当发送给 A 的报文。防止重放攻击的方法是使用不重数;

如加随机数、加时间戳、加流水号等。

[问题 5]

对称加密体制中，密钥的管理和分发非常困难,不够安全。在数据传送前，发送方和接收方必须商定好密钥，然后双方都必须要保存好密钥，如果一方的密钥被泄露，那么加密信息也就不安全了。另外,每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一密钥，这会使得收、发双方所拥有的钥匙数量巨大，密钥管理成为双方的负担。

参考答案

[问题 1]

通过用户知道什么来验证。

[问题 2]

RB

[问题 3]

抗强碰撞性。

[问题 4]

(1) (2)

[问题 5]

不能。对称加密算法不具备单向性、抗弱碰撞性、抗强碰撞性，且密钥的管理和分发非常困难，不够安全。

3. 2018 年上半年试题 2

阅读下列说明和图,回答问题 1 至问题 3,将解答填入答题纸的对应栏内。

【说明】

密码学的基本目标是在有攻击者存在的环境下,保证通信双方(A 和 B)之间能够使用不安全的通信信道实现安全通信。密码技术能够实现信息的保密性、完整性、可用性和不可否认性等安全目标。一种实用的保密通信模型往往涉及对称加密、公钥密码、Hash 函数、数字签名等多种密码技术。

在以下描述中,M 表示消息,H 表示 Hash 函数,E 表示加密算法,D 表示解密算法,K 表示密钥,SKA 表示 A 的私钥,PKA 表示 A 的公钥,SKB 表示 B 的私钥,PKB 表示 B 的公钥,||表示连接操作。

【问题 1】（6 分）

用户 AB 双方采用的保密通信的基本过程如图 2-1 所示。

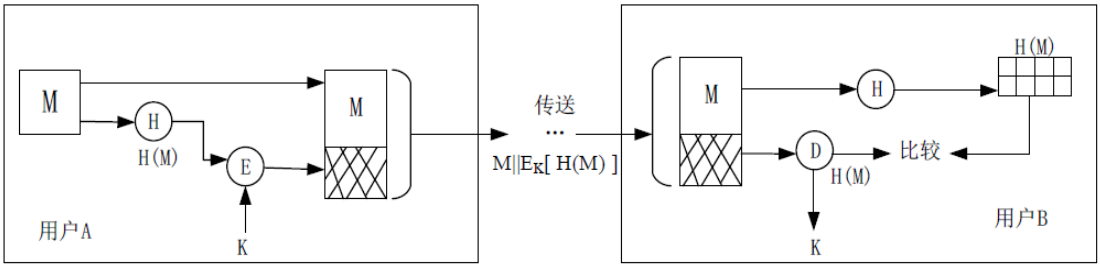


图 2-1 保密通信模型一

请问图 2-1 所设计的保密通信模型能实现信息的哪些安全目标?图 2-1 中的用户 A 侧的 H 和 E 能否互换计算顺序?如果不能互换请说明原因:如果能互换请说明对安全目标的影响。

【问题 2】（4 分）

图 2-2 给出了另一种保密通信的基本过程：

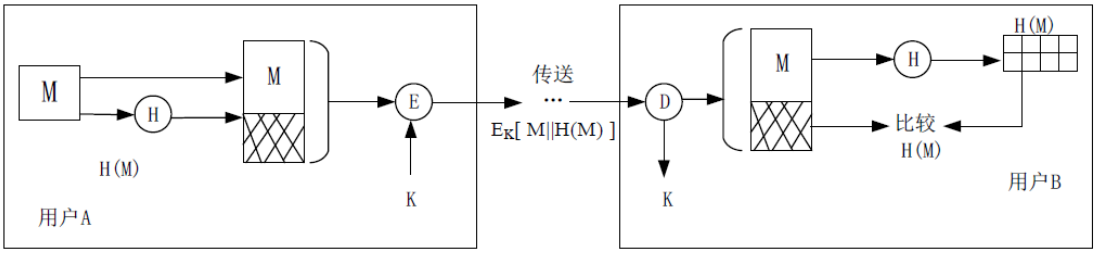


图 2-2 保密通信模型二

请问图 2-2 设计的保密通信模型能实现信息安全的哪些特性?

【问题 3】（5 分）

为了在传输过程中能够保障信息的保密性、完整性和不可否认性,设计了一个安全通信模型结构如图 2-3 所示：

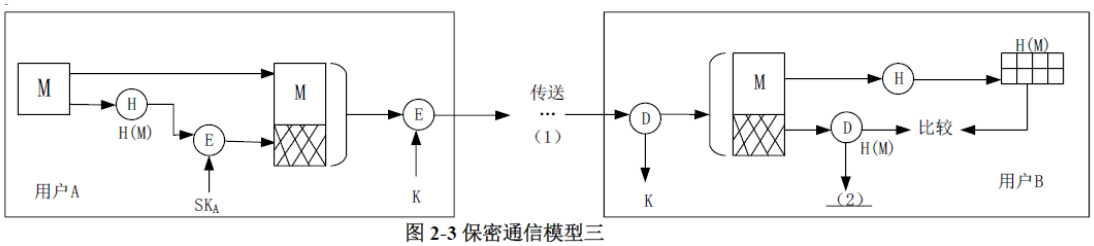


图 2-3 保密通信模型三

请问图 2-3 中（1），（2）分别应该填什么内容?

我能过软考分析：

本题实质在考查保密通信模型。对称密码系统存在事先需要共享秘密信息的问题。非对称密码系统的加密速度有比较慢。可以通过将两者相结合的方式实现方便的共享秘密信息和加密速度之间的一个均衡。典型的系统就是 PGP。对保密通信模型的各类考题都可以看作一个简易版的 PGP。所以认真分析一下 PGP 协议对我们解答这类试题十分有益。

【问题 1】

通过以上保密通信方式，接收方可以相信报文未被修改。如果攻击者改变了报文，因为己假定攻击者不知道密钥 K，所以他不知道如何对 Ek[H（M）]作相应修改。这将使接收方计算出的 H（M）将不等于接收到的 H（M）。

如果只调整 A 用户的处理机制，B 用户的处理方式不变，也就是说，接收方接收到 H[Ek（M）]后再使用共享密钥对其解密得到的结果，与 H（M）无论怎样都不可能相同，也就无法判断信息传输过程中有无被篡改，这样则不能互换计算顺序；

如果 B 用户的处理机制也做相应调整，接收方对接收到的明文也采用同样的方式，先用共享密钥加密，再对其进行 hash 运算，得到的结果与接收到的 H[Ek（M）]进行对比；如此改变其计算顺序，因攻击者不知道密钥 K，且 hash 函数的单向性和抗弱碰撞性，攻击者也很难对 H[Ek（M）]作相应修改；这样则可以互换计算顺序，通过互换同样也可达到以上安全目标。

由于 AB 两端使用的密钥相同，因此不能满足不可否认性的目标。

由于 M 直接传递的是明文，因此不能满足保密性。

【问题 2】

通过双方共享的密钥 K 对 M 和 H（M）进行加密后，可以在保证信息完整性的基础上进一步实现信息的保密性。

在这里，由于 hash 值的存在，能够防止部分数据传丢导致的完整性损害。

【问题 3】

其安全通信模型基本流程为：发送方先对明文 M 进行 hash 运算，对结果 H（M）进行签名，即 $SK_A(H(M)$，接着用收发双方的共享密钥 K 对明文 M 和签名摘要 $SK_A(H(M))$进行加密，得到 $Ek[M||SK_A(H(M))]$，将其传送给接收方；接收方接收该内容后，首先使用同样的共享密钥 K 进行解密，得到明文 M 和签名摘要 $SK_A(H(M)$，然后再使用 A 的公钥 PK_A 对签名摘要 $SK_A(H(M))$进行验证，若验证成功，则得到 H(M)，接着对接收到的明文 M 进行同样的 Hash 运算，将其结果与接收到的 H(M)进行对比，以验证信息的完整性。

参考答案：

【问题一】

实现完整性。

【问题二】能实现保密性和完整性。

【问题三】

（1）$E_k[M||(E_{SKA}(H(M))]$

（2）PK_A

4. 2017 年上半年试题 5

试题五（共 10 分）

阅读下列说明，回答问题 1 和问题 2，将解答写在答题纸的对应栏内。

【说明】

在公钥体制中，每一用户 U 都有自己的公开密钥 PK_u 和私钥 SK_u 。如果任意两个用户 A 和 B 按以下方式通信：

A 发给 B 消息 $[E_{pKB}(m)，A]$。

其中 $E_k(m)$代表用密钥 K 对消息 m 进行加密。

B 收到以后，自动向 A 返回消息【$E_{PkA}(m),B$】，以使 A 知道 B 确实收到消息 m。

【问题 1】 (4 分)

用户 C 怎样通过攻击手段获取用户 A 发送给用户 B 的消息 m。

【问题 2】(6 分)

若通信格式变为:

A 给 B 发消息:$E_{PKB}(E_{SKA}(m)，m，A)$

B 给 A 发消息: $E_{pKA}(E_{sKN}(m)，m，B)$

这时的安全性如何?请分析 A， 此时是如何相互认证并传递消息的。

我能过软考分析：

本题考察的实际上是中间人攻击的攻击方法和预防手段。在问题一的解析中详细写明了中间人攻击的具体方法。

【问题 1】

1. 用户 C 首先截获消息：（E_{PKB}（m），A）

2. 然后将用户标识信息改为 C 自己的标识信息，让用户 B 以为这条消息就是 C 发过来的。即： C(“B”)--->B: （E_{PKB}（m），C）

3. 用户 B 将自己的身份标识及用 C 的公钥加密的信息一起发送给用户 C。即：B--->C:（E_{PKC}（m），B）

4. 用户 C 用私钥成功解密，最后得到明文 m。

【问题 2】

在经过了这样的改变以后，由于 A 发给 B 的整个数据都在 B 的公钥的保护之下，中间人 C 没有办法进行篡改，同时 A 对 M 的部分进行了签名，这样 B 就可以通过验证 A 的签名的方法确认信息来源，就可以有效地杜绝中间人攻击的方法。同时也确保了信息的不可否认性。

参考答案:

【问题 1】

攻击用户 C 可以通过以下手段获取报文 m:

1. 用户 C 截获消息: （E_{PKB}（m），A）

2. 用户 C 篡改消息: （E_{PKB}（m），C）

3. 用户 B 返回消息: （E_{PKC}（m）， B）

4. 用户 C 成功解密，最后得到明文 m。

问题 2

安全性提高了，能实现加密和认证的双重任务。

第一步，A 发给 B 消息是 A 首先用自己的秘密钥 SKA 对消息 m 加密，用于提供数字签名，再用接收方的公钥 PKB 第 2 次加密，密文中包括明文的信息和 A 的身份信息。

第二步，接收方 B 收到密文，用自己的私钥先解密，再用对方的公钥验证发送方的身份是 A，实现了 B 对 A 的认证，并获取了明文。

第三步，B 发给 A 消息是 B 首先用自己的私钥 SKB 对消息 m 加密并签名， 再用 A 的公开钥 PKA 第 2 次加密，文中包括明文的信息和 A 的身份信息，还有 B 对接收的 m 的签名密文。

第四步，只有 A 才能用自己的私钥打开 B 送过来的密文，并且验证是 B 的签名，实现了 A 对 B 的认证，当 A 看见原样返回的 m，就知道 B 收到了 A 发送的明文 m 了。

5. 2017 年上半年试题 4

阅读下列说明，回答问题 1 至问题 5，将解答写在答题纸的对应栏内。

【说明】

DES 是一种分组密码，已知 DES 加密算法的某个 S 盒如表 4-1 所示。

表 4-1 S 盒

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	(1)	1	2	8	5	11	12	4	15
1	13	8	11	5	(2)	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	(3)	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	(4)	12	7	2	14

【问题 1】 (4 分)

请补全该 S 盒，填补其中的空(1) - (4) ，将解答写在答题纸的对应栏内。

【问题 2】 (2 分)

如果该 S 盒的输入为 110011，请计算其二进制输出。

【问题 3】（6 分）

DES 加密的初始置换表如下：

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

置换时，从左上角的第一个元素开始，表示输入的铭文的第 58 位置换成输出的第 1 位，输入明文的第 50 位置换成输出的第 2 位，从左至右，从上往下，依次类推。DES 加密时，对输入的 64 位明文首先进行初始置换操作。若置换输入的明文 M=0123456789ABCDEF（16 进制），请计算其输出（16 进制表示）。

【问题 4】（2 分）

如果有简化的 DES 版本，其明文输入为 8 比特，初始置换表 IP 如下：

IP：2 6 3 1 4 8 5 7

请给出其逆初始置换表。

【问题 5】（2 分）

DES 加密算法存在一些弱点和不足，主要有密钥太短和存在弱密钥。请问，弱密钥的定义是什么?

我能过软考分析：

本题考查的是 DES 算法的具体计算问题。DES 算法是在考试中很常见的一种算法，在选择题部分和分析题部分都会有所涉及。本题从 DES 算法的各个部分都进行了考查，需要认真领会。

【问题 1】

DES 算法中的每个 S 盒都是由 4 行 16 列的矩阵构成，每行都是 0 到 15 这 16 个数字，从上表中可以分析得出，第,0 行缺少 10，第 1 行缺少 6，第 3 行缺少 1，第 4 行缺少 11。

【问题 2】S 盒的运算规则：设输入为 110011，第一位和第六位数字组成的二进制数为 11=（3）$_{10}$；表示选中该 S 盒中的行号为 3 的那一行，其余 4 位数字组成的二进制数为 1001=（9）$_{10}$；表示选中该 S 盒中列号为 9 的那一列。交点处的数字为 4，则 S 盒中的输出为 0100。

【问题 3】

首先将 M=(0123456789ABCDEF)$_{16}$ 表示成二进制形式，即 1 位 16 进制数字可表示为 4 位二进制，即 M = (00000001 00100011 01000101 01100111 10001001 10101011 11001101 11101111)$_2$

然后按照初始置换表进行置换，基本置换规则为：原始数据中的第 58 位放在第一位；第 50 位放第二位；第 42 位放第三位

其余依次类推。置换后的结果为：

M’ =（11001100 00000000 11001100 11111111 11110000 10101010 11110000 10101010）$_2$=（CC00CCFFF0AAF0AA）$_{16}$

【问题 4】

逆初始置换是在初始置换的基础上进行逆置换；比如原始数据顺序为 1 2 3 4 5 6 7 8；经过初始置换之后变成：2 6 3 1 4 8 5 7；则逆初始置换是要将其顺序进行还原，比如，原始数据中第一位数据经初始置换之后放到了第 4 位，那么逆初始置换就要将初始置换后的第 4 位放到第 1 位，即逆初始置换表第一位为 4；原始数据中第二位数据经初始置换之后放到了第 1 位，那么逆初始置换就要将初始置换后的第 1 位放到第 2 位，即逆初始置换表第二位为 1；其余依次类推，得出该逆初始置换表为 4 1 3 5 7 2 8 6。

【问题 5】

DES 算法中存在弱密钥和半弱密钥。

弱密钥 K：即对于各层的子密钥中 K1=K2=…=K16；弱密钥不受任何循环移位的影响，并且只能得到相同的子密钥，存在 4 个弱密钥。对于弱密钥而言，

$DES_K(DES_K(X))=X$ $DES_{K^{-1}}(DES_{K^{-1}}(X))=X$

即用 k 对明文 x 加密两次或者脱密两次都可以恢复出明文 x。在弱密钥下，加密运算和脱密运算没有区别。

半弱密钥 K：有些种子密钥只能生成两个不同的子密钥， K1，K2，…，K16 一共就只有两种取法。这样的种子密钥 K 称为半弱密钥，DES 至少存在 12 个半弱密钥。半弱密钥将导致把明文加密成相同的密文。DES 的 12 个半弱密钥中，按互逆关系成对出现。组成六对湖迷的半弱密钥，对于每对互逆的半弱密钥 k’ 和 k” ，有

$DES_{K'}(DES_{K''}(X))=X$ $DES_{K'^{-1}}(DES_{K''^{-1}}(X))=X$

参考答案：

【问题 1】

（1）10　　（2）6　　（3）1　　（4）11

【问题 2】

0100

【问题 3】

M=（0123456789ABCDEF）$_{16}$=（00000001 00100011 01000101 01100111 10001001　10101011 11001101 11101111）$_{2,}$ 经过 IP 置换，结果为：M’ =（11001100 00000000 11001100 11111111　11110000 10101010 11110000 10101010）$_{2}$=（CC00CCFFF0AAF0AA）$_{16}$

【问题 4】

4　1　3　5　7　2　8　6

【问题 5】

对初始密钥 k，若通过密钥生成算法生成的圈（子）密钥都相同，则称 k 为弱密钥。

6. 2016 年下半年试题 1

阅读下列说明和图，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

【说明】

研究密码编码的科学称为密码编码学，研究密码破译的科学称为密码分析学，密码编码学和密码分析学共同组成密码学。密码学作为信息安全的关键技术，在信息安全领域有着广泛的应用。

【问题 1】（9 分）

密码学的安全目标至少包括哪三个方面？具体内涵是什么？

【问题 2】（3 分）

对下列违规安全事件，指出各个事件分别违反了安全目标中的哪些项？

(1)小明抄袭了小丽的家庭作业。

(2)小明私自修改了自己的成绩。

(3)小李窃取了小刘的学位证号码、登陆口令信息，并通过学位信息系统更改了小刘的学位信息记录和登陆口令，将系统中小刘的学位信息用一份伪造的信息替代，造成小刘无法访问学位信息系统。

【问题 3】（3 分）

现代密码体制的安全性通常取决于密钥的安全，为了保证密钥的安全，密钥管理包括哪些技术问题？

【问题 4】（5 分）

在图 1-1 给出的加密过程中，M_i,i=1,2，…，n 表示明文分组，C_i,i=1,2，…，n 表示密文分组，Z 表示初始序列，K 表示密钥，E 表示分组加

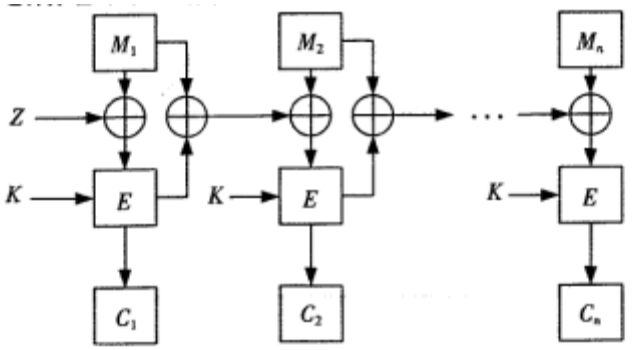


图1-1

密过程。该分组加密过程属于哪种工作模式？这种分组密码的工作模式有什么缺点?

我能过软考分析：

本题对密码学的基础知识进行了考查。信息安全的基本要素和各种要素的保护技术需要对应掌握。

【问题 1】

密码学作为信息安全的关键技术，其安全目标主要包括三个非常重要的方面：保密性、完整性和可用性。保密性：保密性是确保信息仅被合法用户访问，而不被地露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。完整性：完整性是指所有资源只能由授权方或以授权的方式进行修改，即信息未经授权不能进行改变的特性。信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、

伪造、乱序、重放、插入等破坏和丢失的特性。可用性：可用性是指所有资源在适当的时候可以由授权方访问，即信息可被授权实体访问并按需求使用的特性。信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

【问题 2】

根据保密性、完整性及可用性分析，抄袭作业是属于违反保密性，修改成绩是属于违反完整性，更改信息记录和登录口令导致无法访问属于违反可用性、完整性、保密性。

【问题 3】

密码体制的安全应当只取决于密钥的安全，而不取决于对密码算法的保密。密钥管理包括密钥的产生、存储、分配、组织、使用、停用、更换、销毁等一系列技术问题。每个密钥都有其生命周期，要对密钥的整个生命周期的各个阶段进行全面管理。对称密码密钥的存储技术主要包括密钥的分级管理和密钥的分散存储。生存周期管理对密钥管理也有重要的意义。在非对称密码的密钥管理中还存在 PKI 的建立、CA 的信任等问题。

【问题 4】

明密文链接模式：设明文 M=（M_1，M_2，…，M_n）,相应的密文 C=(C_1，C_2，…，C_n),而

$$C_i = \begin{cases} E(M_i \oplus Z, K), & i=1 \\ E(M_i \oplus M_{i-1} \oplus C_{i-1}, K), & i=2,\ldots,n \end{cases}$$

其中 Z 为初始化向量。

根据上式可知，即使 $M_i = M_j$，但因一般都有 $M_{i-1} \oplus C_{i-1} \neq M_{j-1} \oplus C_{j-1}$，从而使 $C_i \neq C_j$，从而掩盖了名文中的数据模式。同样根据上式可知加密时，当 M_i 或 C_i 中发生一位错误时，自此以后的密文全都发生错误。这种现象称为错误传播无界。

解密时有

$$M_i = \begin{cases} D(C_i, K) \oplus Z, & i=1 \\ D(C_i, K) \oplus M_{i-1} \oplus C_{i-1}, & i=2,\ldots,n \end{cases}$$

同样，解密时也是错误传播无界。

其缺点：当 M_i 或 C_i 中发生一位错误时，自此以后的密文全都发生错误，即具有错误传播无界的特性，不利于磁盘文件加密。并且要求数据的长度是密码分组长度的整数倍，否则最后一个数据块将是短块，这时需要特殊处理。

（自己可以再总结一下分组密码的工作模式，把其他几种的表达式、框图、错误传播进行分析。也可以将总结的结果发到群里。）

参考答案：

【问题一】

密码学的安全目标至少包括保密性、完整性和可用性。具体含义如下：

（1）保密性：保密性是确保信息仅被合法用户访问，而不被地露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。

（2）完整性：完整性是指所有资源只能由授权方或以授权的方式进行修改，即信息未经授权不能进行改变的特性。信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性

（3）可用性：可用性是指所有资源在适当的时候可以由授权方访问，即信息可被授权实体访问并按需求使用的特性。信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

【问题二】

（1）保密性（2）完整性（3）可用性、完整性、保密性

【问题三】

密钥管理包括密钥的产生、存储、分配、组织、使用、停用、更换、销毁等一系列技术问题。

(这段话来自于书中，建议再总结一些具体密钥管理的方法比如分散存储、分级管理、生存周期管理、密钥分配方法等等。)

【问题四】

明密文链接模式。

缺点：当 M_i 或 C_i 中发生一位错误时，自此以后的密文全都发生错误，即具有错误传播无界的特性，不利于磁盘文件加密。并且要求数据的长度是密码分组长度的整数倍，否则最后一个数据块将是短块，这时需要特殊处理。

7. 2016 年下半年试题 4

阅读下列说明，回答问题 l 至问题 4，将解答填入答题纸的对应栏内。

【说明】

用户的身份认证是许多应用系统的第一道防线，身份识别对确保系统和数据的安全保密极及其重要。以下过程给出了实现用户 B 对用户 A 身份的认证过程。

1.A->B：A

2.B->A：{B,Nb}pk(A)

3.A->B：h(Nb)

此处 A 和 B 是认证的实体，Nb 是一个随机值，pk(A)表示实体 A 的公钥，{B,Nb}pk(A)表示用 A 的公钥对消息 B，Nb 进行加密处理，h(Nb)表示用哈希算法 h 对 Nb 计算哈希值。

【问题 1】（5 分）

认证与加密有哪些区别?

【问题 2】（6 分）

（1）包含在消息 2 中的“Nb”起什么作用?

（2）“Nb“的选择应满足什么条件?

【问题 3】（3 分）

为什么消息 3 中的 Nb 要计算哈希值?

【问题 4】（4 分）

上述协议存在什么安全缺陷？请给出相应的解决思路。

我能过软考分析：

本题考察的是对于身份认证的过程。在身份认证中，需要注意的就是随机数的应用，抗重放攻击的方法和中间人攻击的方法。主要就是非对称密码的应用。可以结合 hash 和非对称密码进行考查。

【问题 1】

认证又称鉴别或确认，它是证实某事是否名副其实或是否有效的一个过程，认证和加密的区别在于：加密用以确保数据的保密性，阻止对手的被动攻击，比如发送方给接收方发送信息为确保信息在传输过程中不被别人看到，可以对该信息进行加密；而认证用以确保报文发送者和接收者的真实性以及报文的完整性，比如发送方防止在发送上述信息时被别人篡改，就可以采用认证方法。

【问题 2】

（1）Nb 是一个随机值，用户 B 在验证用户 A 的身份时，首先会生成一个随机数，然后将该随机数和自己的身份信息一起用用户 A 的公钥加密发送给用户 A，用户 A 接收后再将该随机数发送给用户 B，因此，随机值 Nb 是验证的关键，并且该随机值只有发送方 B 和 A 知道，可以起到抗重放攻击作用。

（2）在验证身份时，该随机值是关键，不仅要求传输的安全性，而且还要保证该数值的随机性且不易被猜测，因为一旦被猜出来，就可能假冒用户 A 的身份。

【问题 3】

哈希算法是具有单向性的，经过哈希值运算之后的随机数，即使被攻击者截获也无法对该随机数进行还原，获取该随机数 Nb 的产生信息，可以保障 Nb 在传输过程中的保密性。

【问题 4】

上述验证过程中，用户 A 收到随机数后，直接将哈希后的随机数发过去，会存在很大的漏洞，因为任何人都可以通过截获 h（Nb）冒充用户 A 的身份给用户 B 发送 h（Nb），而用户 B 在验证时无法确定该随机数是否为用户 A 发过来的。可以通过如下方式：用户 A 通过将 A 的标识和随机数 Nb 进行哈希运算，将其哈希值 h（A，Nb）发送给用户 B，用户 B 接收后，利用哈希函数对自己保存的用户标识 A 和随机数 Nb 进行加密，并与接收到的 h（A，Nb）进行比较。若两者相等，则用户 B 确认用户 A 的身份是真实的，否则认为用户 A 的身份是不真实的。答案中给出的是一个相对比较复杂的办法，而实际上只要进行一个简单的签名就能解决这个问题。

参考答案：

【问题一】

认证和加密的区别在于：加密用以确保数据的保密性，阻止对手的被动攻击，如截取，窃听等；而认证用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等。

【问题二】

（1）Nb 是一个随机值，只有发送方 B 和 A 知道，起到抗重放攻击作用。

（2）应具备随机性，不易被猜测。

【问题三】

哈希算法具有单向性，经过哈希值运算之后的随机数，即使被攻击者截获也无法对该随机数进行还原，获取该随机数 Nb 的产生信息。

【问题四】

攻击者可以通过截获 h（Nb）冒充用户 A 的身份给用户 B 发送 h（Nb）。

解决思路：用户 A 通过将 A 的标识和随机数 Nb 进行哈希运算，将其哈希值 h（A，Nb）发送给用户 B，用户 B 接收后，利用哈希函数对自己保存的用户标识 A 和随机数 Nb 进行加密，并与接收到的 h（A，Nb）进行比较。若两者相等，则用户 B 确认用户 A 的身份是真实的，否则认为用户 A 的身份是不真实的。

考点 2：网络安全案例分析

1. 2019 年上半年下午真题试题 4

阅读下列说明和表，回答问题 1 至问题 4,将解答填入答题纸的对应栏内。

[说明]

防火墙类似于我国古代的护城河，可以阻挡敌人的进攻。在网络安全中，防火墙主要用于逻辑隔离外部网络与受保护的内部网络。防火墙通过使用各种安全规则来实现网络的安全策略。

防火墙的安全规则由匹配条件和处理方式两个部分共同构成。网络流量通过防火墙时，根据数据包中的某些特定字段进行计算以后如果满足匹配条件，就必须采用规则中的处理方式进行处理。

[问题 1] (5 分)

假设某企业内部网(202 114 63.0/24)需要通过防火墙与外部网络互连，其防火墙的过滤规则实例如表 4.1 所示。

表 4.1

序号	源地址	源端口	目的地址	目的端口	协议	ACK	动作（处理方式）
A	202.114.63.0/24	>1024	*	80	TCP	*	accept
B	*	80	202.114.63.0/24	>1024	TCP	Yes	accept
C	*	>1024	202.114.64.125	80	TCP	*	accept
D	202.114.64.125	80	*	>1024	TCP	Yes	accept
E	202.114.63.0/24	>1024	*	（1）	UDP	*	accept
F	*	53	202.114.63.0/24	>1024	UDP	*	accept
G	*	*		*	*	*	（2）

表中*"表示通配符，任意服务端口都有两条规则。

请补充表 4.1 中的内容(1)和(2)，并根据上述规则表给出该企业对应的安全需求。

[问题 2] (4 分)

一般来说，安全规则无法覆盖所有的网络流量。因此防火墙都有一条缺省(默认）规则，该规则能覆盖事先无法预料的网络流量。请问缺省规则的两种选择是什么?

[问题 3] (6 分)

请给出防火墙规则中的三种数据包处理方式。

[问题 4] (4 分)

防火墙的目的是实施访问控制和加强站点安全策略，其访问控制包含四个方面的内容:服务控制、方向控制、用户控制和行为控制。请问表 4. 1 中，规则 A 涉及访问控制的哪几个方面的内容?

答案

[问题 1]

(1) 53 (2) Drop

其安全需求为: (1）允许内部用户访问外部网络的网页服务器; (2）允许外部用户访问内部网络的网页服务器(202.114.64.125); (3）除 1 和 2 外，禁止其他任何网络流量通过该防火墙。

[问题 2]

默认拒绝或者默认允许。

[问题 3]

(1) Accept (2) Reject (3) Drop ;

[问题 4]

服务控制、方向控制和用户控制。

试题分析

[问题 1]

规则 A 和 B 允许内部用户访问外部网络的网页服务器。规则 C 和 D 允许外部用户访问内部网络的网页服务器。规则 E 和 F 允许内部用户访问域名服务器。规则 G 是缺省拒绝的规则。规则 E 中目的端口为 53;规则 G 中动作为 Drop。

其安全需求为:①允许内部用户访问外部网络的网页服务器:②允许外部用户访问内部网络的网页服务器

(202.114.64.125);③除 1 和 2 外，禁止其他任何网络流量通过该防火墙。

[问题 2]

缺省规则有两种选择默认拒绝或者默认允许。默认拒绝是指一切未被允许的就是禁止的，其安全规则的处理方式一般为 Accept;默认允许是指一切未被禁止的就是允许的。其安全规则的处理方式-般为 Reject 或 Drop.

[问题 3]

防火墙规则中的处理方式主要包括以下几种:

(1) Accept: 允许数据包或信息通过。

(2) Reject 拒绝数据包或信息通过，并且通知信息源该信息被禁止。

(3) Drop: 直接将数据包或信息丢弃,并且不通知信息源。

[问题 4]

防火墙的目的是实施访问控制和加强站点安全策略，其访问控制包含四个方面或层次的内容:

(1)服务控制:决定哪些服务可以被访问，无论这些服务是在内部网络还是在外部网络。常见的网络服务有邮件服务、网页服务、代理服务、文件服务等，这些服务往往是系统对外的功能。在计算机网络中,服务往往就是指 TCP/IP 协议中的端口值，如 25 是指 SMTP 服务，110 是指 POP3 服务，80 是指网页服务等。当然，服务控制也包括服务的位置控制，如 E 地址。

(2)方向控制:决定在哪些特定的方向上服务请求可以被发起并通过防火墙，也就是服务是位于内部网络还是外部网络。通过规则控制，可以限定一个方向的服务，也可以同时限定两个方向的服务。

(3)用户控制:决定哪些用户可以访问特定服务。该技术既可以应用于防火墙网络内部的用户(本地用户)，也可议被应用到来自外部用户的访问。可以采用用户名、主机的 IP、主机的 MAC 等标识用户。

(4)行为控制:决定哪些具体的服务内容是否符合安全策略。如防火墙可以通过过滤邮件来清除垃圾邮件，以及网络流量中是否含有计算机病毒、木马等恶意代码。

2. 2018 年上半年试题 5

阅读下列说明和图,回答问题 1 至问题 5,将解答写在答题纸的对应栏内。

【说明】

入侵检测系统(IDS)和入侵防护系统(IPS)是两种重要的网络安全防御手段,IDS 注重的是网络安全状况的监管,IPS 则注重对入侵行为的控制。

【问题 1】（2 分）

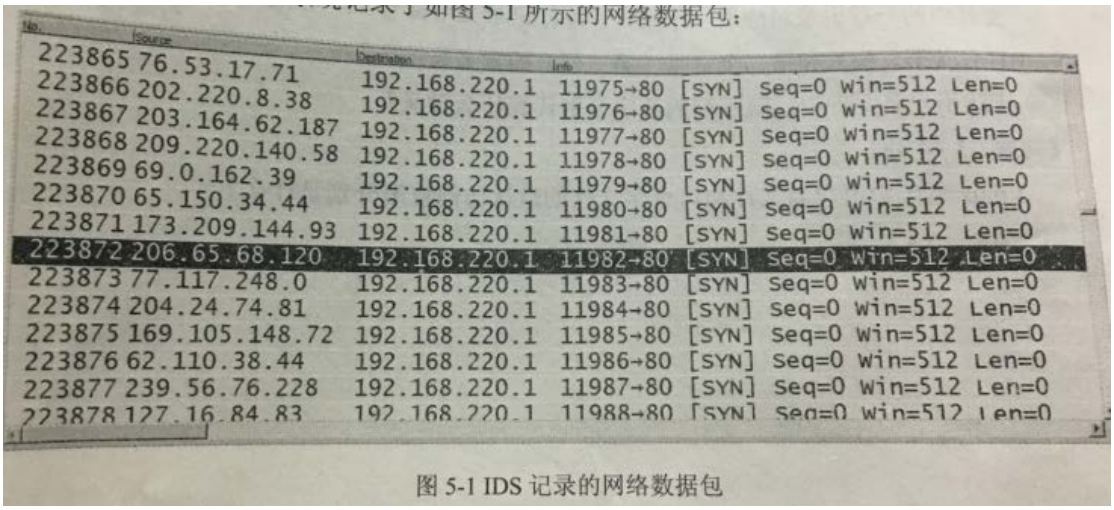
网络安全防护可以分为主动防护和被动防护,请问 IDS 和 IPS 分别属于哪种防护?

【问题 2】（4 分）

入侵检测是动态安全模型(P2DR)的重要组成部分。请列举 P2DR 模型的 4 个主要组成部分。

【问题 3】（2 分）

假如某入侵检测系统记录了如图 5-1 所示的网络数据包：



No.	Source	Destination	Info
223865	76.53.17.71	192.168.220.1	11975→80 [SYN] Seq=0 Win=512 Len=0
223866	202.220.8.38	192.168.220.1	11976→80 [SYN] Seq=0 Win=512 Len=0
223867	203.164.62.187	192.168.220.1	11977→80 [SYN] Seq=0 Win=512 Len=0
223868	209.220.140.58	192.168.220.1	11978→80 [SYN] Seq=0 Win=512 Len=0
223869	69.0.162.39	192.168.220.1	11979→80 [SYN] Seq=0 Win=512 Len=0
223870	65.150.34.44	192.168.220.1	11980→80 [SYN] Seq=0 Win=512 Len=0
223871	173.209.144.93	192.168.220.1	11981→80 [SYN] Seq=0 Win=512 Len=0
223872	206.65.68.120	192.168.220.1	11982→80 [SYN] Seq=0 Win=512 Len=0
223873	77.117.248.0	192.168.220.1	11983→80 [SYN] Seq=0 Win=512 Len=0
223874	204.24.74.81	192.168.220.1	11984→80 [SYN] Seq=0 Win=512 Len=0
223875	169.105.148.72	192.168.220.1	11985→80 [SYN] Seq=0 Win=512 Len=0
223876	62.110.38.44	192.168.220.1	11986→80 [SYN] Seq=0 Win=512 Len=0
223877	239.56.76.228	192.168.220.1	11987→80 [SYN] Seq=0 Win=512 Len=0
223878	127.16.84.83	192.168.220.1	11988→80 [SYN] Seq=0 Win=512 Len=0

图 5-1 IDS 记录的网络数据包

请问图中的数据包属于哪种网络攻击?该攻击的具体名字是什么?

【问题 4】（4 分）

入侵检测系统常用的两种检测技术是异常检测和误用检测,请问针对图中所描述的网络攻击应该采用哪种检测技术?请简要说明原因。

【问题 5】（3 分）

Snort 是一款开源的网络入侵检测系统,它能够执行实时流量分析和 IP 协议网络的数据包记录.

Snort 的配置有 3 种模式,请给出这 3 种模式的名字。

我能过软考分析

本题主要考查 IDS、IPS；入侵检测的 PD2R 模型；同步包洪泛攻击；入侵检测两种检测技术（异常检测和误用检测）；Snort。

【问题 1】

入侵检测技术(IDS)注重的是网络安全状况的监管，通过监视网络或系统资源， 寻找违反安全策略的行为或攻击迹象，并发出报警。因此 IDS 系统属于被动防护。入侵防护系统（IPS)则倾向于提供主动防护，注重对入侵行为的控制。其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失。

【问题 2】

P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具，如防火墙、操作系统身份认证、加密等手段的同时，利用检测工具，如漏溺评估、入侵检测等系统了解和评估系统的安全状态，通过适当的响应将系统调整到"最安全"和"风险最低"的状态。防护、检测和自由应组成了一个完整的、动态的安全循环。

【问题 3】

SYN 洪泛攻击通过创建大量"半连接"来进行攻击，任何连接收到 Intenet 上并提供基于 TCP 的网络服务的主机或路由器都可能成为这种攻击的目标；同步包风暴是当前最流行的 DoS（拒绝服务攻击)与 DDoS （分布式拒绝服务攻击）的方式之一，利用 TCP 协议缺陷发送大量伪造的 TCP 连接请求，使得被攻击者资源耗尽。三次握手，进行了两次(SYN)(SYN/ACK)，不进行第三次握手

（ACK）,连接队列处于等待状态，大量的这样的等待，占满全部队列空间，系统挂起。

【问题 4】

误用检测技术的核心是维护一个入侵规则库；对于已知的攻击，它可以详细、准确的报告出攻击类型，但是对未知攻击却效果有限，而且入侵模式库必须不断更新。

异常检测方法依赖于正常行为模型的建立，通过观测到的一组测量值偏离度来预测用户行为的变化，然后作出决策判断的检测技术，是一种基于行为模式的检测方法。

防范 SYN 洪泛攻击，可以采用基于行为模式的异常检测算法对目标服务器的网络流量进行检测，通过实时跟踪 TCP 服务器连接的状态机协商过程，能够有效区分攻击流量和正常流量，从而精确阻断攻击流量。

【问题 5】

Snort 的配置有 3 个主要模式：嗅探（Sniffer)、包记录（PacketLogger)和网络入侵检测。

嗅探模式主要是读取网络上的数据包并在控制台上用数据流不断地显示出来；

包记录模式把数据包记录在磁盘上；

网络入侵监测模式是最复杂最难配置的，它可以分析网流量与用户定义的规则设置进行匹配然后根据结果执行相应的操作。

参考答案

【问题 1】

入侵检测技术 (IDS)属于被动防护；入侵防护系统 (IPS)属于主动防护。

【问题 2】

P2DR 模型包含 4 个主要组成部分包括：Policy （安全策略）、Protection （防护)、 Detection （检测)和 Response （响应)。

【问题 3】

属于拒绝服务攻击；具体为 SYN 洪泛攻击。

【问题 4】

应该采用异常检测技术；采用基于行为模式的异常检测算法对目标服务器的网络流量进行检测，通过实时跟踪 TCP 服务器连接的状态机协商过程，能够有效区分攻击流量和正常流量，从而精确阻断攻击流量。

【问题 5】

Snort 的配置的 3 个主要模式：嗅探（Sniffer)、包记录（PacketLogger)和网络入侵检测。

3. 2017 年上半年试题 6

阅读下列说明，回答问题 1 至问题 4 ，将解答写在答题纸的对应栏内。

【说明】

基于 Windows32 位系统分析下列代码，回答相关问题 。

```
void Challenge(char *str)
{
    char temp[9]={0};
    strncpy(temp，str，8);
```

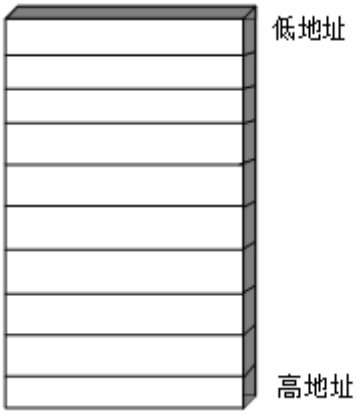
```
        printf("temp=%s\n", temp);
        if(strcmp(temp"Please!@")==0){
                printf("KEY: ****");
        }
}
int main(int argc, char *argv[ ])
{
        Char buf2[16];
        Int check=1;
        Char buf[8];
        Strcpy (buf2, "give me key! !");
        strcpy(buf, argv[1]);
       if(check==65)  {
              Challenge(buf);
        }
       else {
            printf("Check is not 65 (%d) \n Program terminated!!\n",
check);
        }
       Return  0;
   }
```

【问题 1】(3 分)

main 函数内的三个本地变量所在的内存区域称为什么?它的两个最基本操作是什么?

【问题 2】（3 分）

画出 buf，check，buf2 三个变量在内存的布局图。



【问题 3】（2 分）

应该给程序提供什么样的命令行参数值（通过 argv 变量传递）才能使程序执行流程进入判断语句 If（check=65）然后调用 challenge( )函数。

【问题 4】（4 分）

上述代码所存在的漏洞名字是什么，针对本例代码，请简要说明如何修正上述代码以修补次漏洞。

我能过软考分析

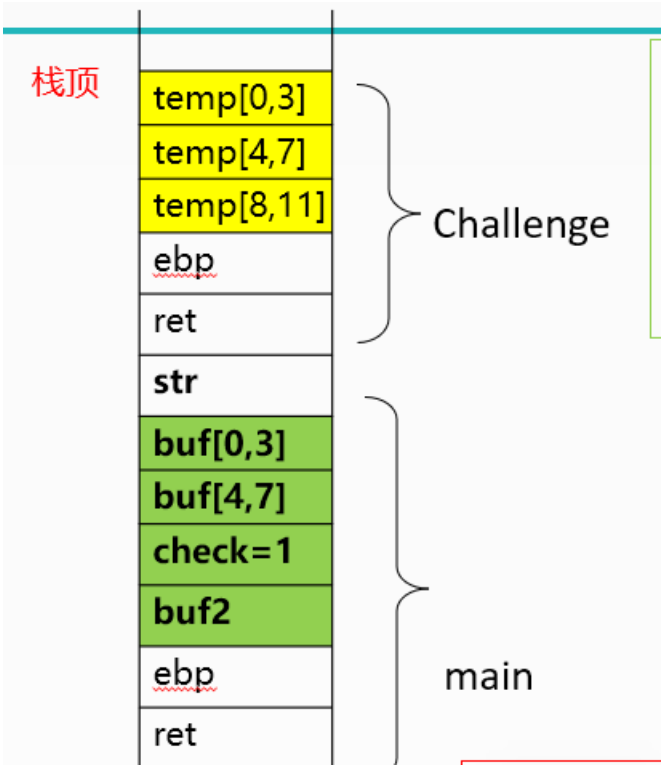
本题主要考查内存结构、堆栈的基本操作；局部变量入栈的顺序；缓冲区溢出；以及防止缓冲区溢出的解决方案。本题需要重点了解。

【问题 1】

一个程序在内存中分为程序段、数据段和堆栈三部分。程序段里放着程序的机器码和只读数据；数据段放程序中的静态数据；动态数据则通过堆栈来存放，也就是说，变量存在的内存区域是堆栈；堆栈的特性是后进先出(LIFO)，即先进入堆栈的对象最后出来，最后进入堆栈的对象最先出来。堆栈两个最重要的操作是 PUSH 和 POP 将对象放入堆栈顶端(最外边，内存高端)；POP 操作实现一个逆向过程，把顶端的对象取出来。

【问题 2】

首先根据 3 个变量定义的先后顺序，buf2 先压入堆栈（在最底下），然后是 check，最后是 buf（最上面）；空间大小根据 C 语言语法即可确定。buf2 是 16 个字节，check 是整型变量占用 4 个字节，buf 是字符数组，有 8 个字符，每个字符占一个字节，共占用 8 个字节。所以 buf、check、buf2 三个变量在内存的布局图如下所示：



【问题 3】

该代码按正常流程走下来，因 check 的值为 1，不满足 check==65，所以会执行 else 语句，所以这道题的关键在于通过什么样的方式来改变 check 的值，使其等于 65，满足条件然后调用 Challenge（）函数。

再来分析 strcpy() 函数这个函数，该用来复制字符串，其原型为：

char *strcpy(char *dest, const char *src);

【参数】dest 为目标字符串指针，src 为源字符串指针。

注意：src 和 dest 所指的内存区域不能重叠，且 dest 必须有足够的空间放置 src 所包含的字符串（包含结束符 NULL）。

【返回值】成功执行后返回目标数组指针 dest。

strcpy() 把 src 所指的由 NULL 结束的字符串复制到 dest 所指的数组中，返回指向 dest 字符串的起始地址。

注意：如果参数 dest 所指的内存空间不够大，可能会造成缓冲溢出。

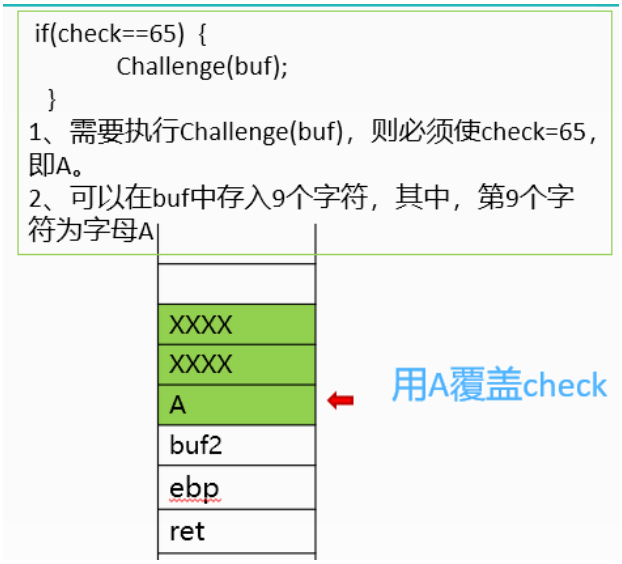
主函数在执行时会接收用户输入信息放入指针数组 argv 中，而指针数组存放的信息又会通过 strcpy 复制到 buf 数组里面，buf 数组的长度为 8 个字符，一旦用户输入数据长度大于 8 个字符就会溢出，溢出部分就会覆盖其他变量的值，从上面堆栈中的数据存储方式可以看出，buf 数组一旦溢出，溢出部分就会覆盖 check 的值；根据题目意思，只要令溢出部分的值为 65 即可令 check=65，从而满足条件。所以可以先任意输入 8 个字符堆满 buf 数组，再输入时就是溢出部分，可以输入大写字母 A，因 check 为整形数据，所以将字符赋给整形变量时，会按其 ASCII 码值进行处理，即 A 的 ASICC 值为 65，从而可以把 check 值变成 65 满足条件。

前面分析 strcpy() 函数，当其参数 dest 所指的内存空间不够大，可能会造成缓冲溢出。

而 strncpy()用来复制字符串的前 n 个字符，其原型为：

char * strncpy(char *dest, const char *src, size_t n);

【参数说明】dest 为目标字符串指针，src 为源字符串指针。 strncpy()会将字符串 src 前 n 个字符拷贝到字符串 dest。



【问题 4】

在编写程序时通常用 strncpy（）函数来取代 strcpy（）函数防止缓冲区溢出。

参考答案

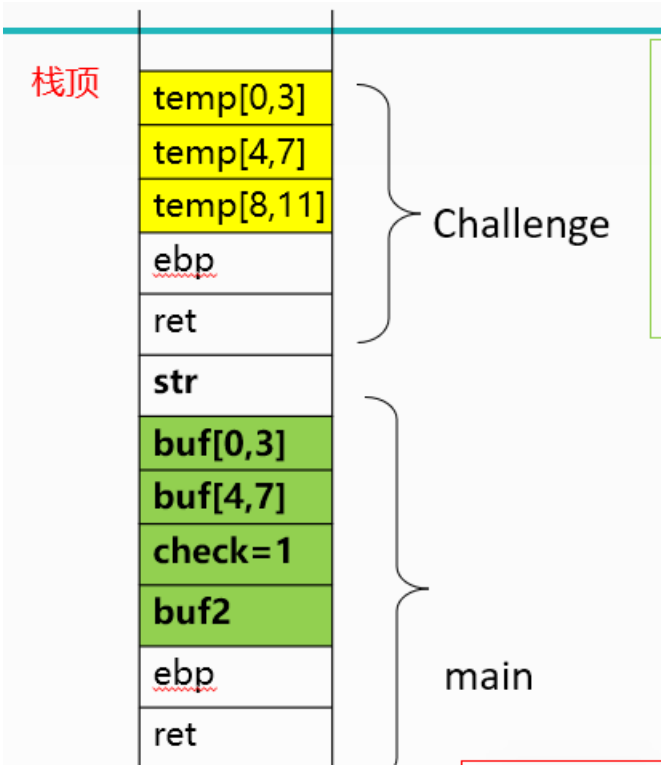
【问题 1】

1、堆栈。

2、PUSH 和 POP。

【问题 2】

变量的先后关系、每个变量所占空间、增长方向（数组）



【问题 3】

用户输入 9 个字符的字符串，使其满足条件：前 8 个字符为任意字符和第 9 个字符为大写字母 A；

【问题 4】

缓冲区溢出。对输入参数的长度进行检查；使用安全函数 strncpy（）来代替 strcpy（）函数。


免费试看

4. 2016 年下半年试题 3

阅读下列说明和图，回答问题 l 至问题 3，将解答填入答题纸的对应栏内。

【说明】

防火墙是一种广泛应用的网络安全防御技术，它阻挡对网络的非法访问和不安全的数据传递，保护本地系统和网络免于受到安全威胁。

图 3-1 给出了一种防火墙的体系结构。

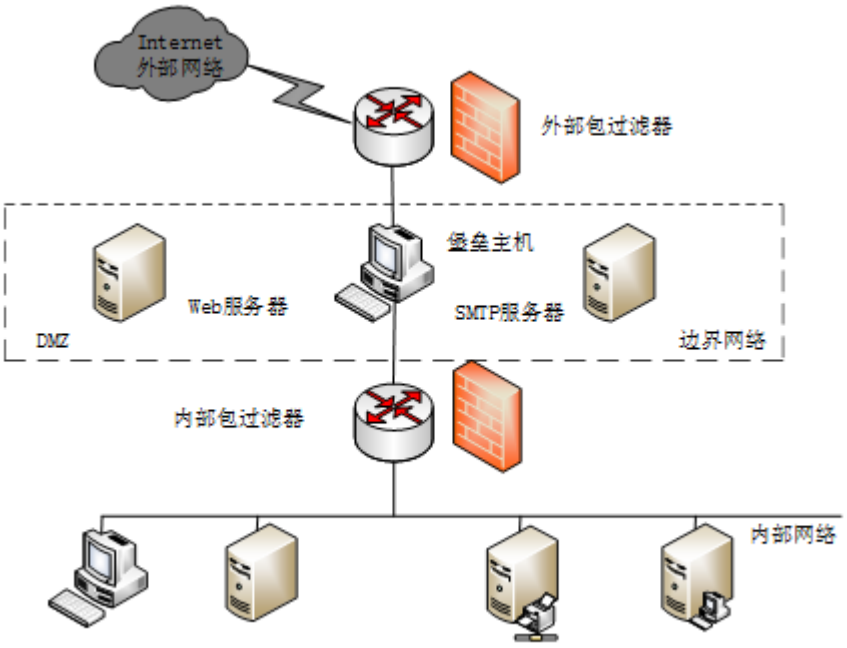


图 3-1

【问题 1】（6 分）

防火墙的体系结构主要有：

(1)双重宿主主机体系结构；

(2)（被）屏蔽主机体系结构；

(3)（被）屏蔽子网体系结构；

请简要说明这三种体系结构的特点。

【问题 2】（5 分）

(1)图 3-1 描述的是哪一种防火墙的体系结构?

(2)其中内部包过滤器和外部包过滤器的作用分别是什么?

【问题 3】（8 分）

设图 3-1 中外部包过滤器的外部 IP 地址为 10.20.100.1，内部 IP 地址为 10.20.100.2;

内部包过滤器的外部 IP 地址为 10.20.100.3，内部 IP 地址为 192.168.0.1,DMZ 中 Web 服务器 IP 为 10.20.100.6,SMTP 服务器 IP 为 10,20.100.8。

关于包过滤器，要求实现以下功能：不允许内部网络用户访问外网和 DMZ，外部网络用户只允许访问 DMZ 中的 Web 服务器和 SMTP 服务器。内部包过滤器规则如表 3-1 所示。请完成外部包过滤器规则表 3-2，将对应空缺表项的答案填入答题纸对应栏内。

表 3-1 内部包过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	动作	方向
1	*	*	*	*	*	拒绝	*

表 3-2 外部包过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	动作	方向
1	TCP	*	10.20.100.6	> 1024	80	允许	入
2	TCP	10.20.100.6	*	80	> 1024	允许	出
3	TCP	（1）	（2）	> 1024	25	允许	入
4	TCP	（3）	（4）	25	> 1024	允许	出
5	（5）	（6）	*	> 1024	53	允许	入
6	（7）	*	（8）	53	>1024	允许	出
7	*	*	*	*	*	拒绝	*

我能国软考分析

本题考查防火墙体系结构和包过滤规则表。需重点掌握。

1、防火墙的经典体系结构主要有三种形式：双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构。

双重宿主主机体系结构：双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络与内部网络的任务。

被屏蔽主机体系结构：被屏蔽主机体系结构是指通过一个单独的路由器和内部网络上的堡垒主机共同构成防火墙，主要通过数据包过滤实现内外网络的隔离和对内网的保护。

被屏蔽子网体系结构：被屏蔽子网体系结构将防火墙的概念扩充至一个由两台路由器包围起来的周边网络，并且将容易受到攻击的堡垒主机都置于这个周边网络中。其主要由四个部件构成，分别为:周边网络、外部路由器、内部路由器以及堡垒主机。

2、（1）图中网络拓扑结构中包含有周边网络、外部路由器、内部路由器以及堡垒主机这四个部件，属于被屏蔽子网体系结构或屏蔽子网体系结构。

（2）内部路由器：内部路由器用于隔离周边网络和内部网络，是屏蔽子网体系结构的第二道屏障。在其上设置了针对内部用户的访问过滤规划，对内部用户访问周边网络和外部网络进行限制。

外部路由器：外部路由器的主要作用在于保护周边网络和内部网络，是屏蔽子网体系结构的第一道屏障。在其上设置了对周边网络和内部网络进行访问的过滤规则，该规则主要针对外网用户。

3、规则号 3 和 4 配置 SMTP 服务器安全策略，入方向：源地址为*，目的地址为 SMTP 服务器地址：10.20.100.8 ，出方向源地址为 10.20.100.8，目的地址为*。

由端口号 53 得知，规则号 5 和 6 配置 DNS 安全策略，

入方向：协议为 UDP，源地址为 10.20.100. *，出方向：协议为 UDP，目的地址为 10.20.100. *。

参考答案

【问题一】

双重宿主主机体系结构：双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络与内部网络的任务。

被屏蔽主机体系结构：被屏蔽主机体系结构是指通过一个单独的路由器和内部网络上的堡垒主机共同构成防火墙，主要通过数据包过滤实现内外网络的隔离和对内网的保护。

被屏蔽子网体系结构：被屏蔽子网体系结构将防火墙的概念扩充至一个由两台路由器包围起来的周边网络，并且将容易受到攻击的堡垒主机都置于这个周边网络中。其主要由四个部件构成，分别为:周边网络、外部路由器、内部路由器以及堡垒主机。

【问题二】

（1） 屏蔽子网体系结构。

（2） 内部路由器：内部路由器用于隔离周边网络和内部网络，是屏蔽子网体系结构的第二道屏障。在其上设置了针对内部用户的访问过滤规划，对内部用户访问周边网络和外部网络进行限制。

外部路由器：外部路由器的主要作用在于保护周边网络和内部网络，是屏蔽子网体系结构的第一道屏障。在其上设置了对周边网络和内部网络进行访问的过滤规则，该规则主要针对外网用户。

【问题三】

（1）*　　（2）10.20.100.8　（3）10.20.100.8　（4）*

（5）UDP　（6）10.20.100.*　（7）UDP　　（8）10.20.100.*

5. 2016 年下半年试题 5

阅读下列说明和代码，回答问题 1 和问题 2，将解答写在答题纸的对应栏内。

【说明】

某本地口令验证函数（C 语言环境，X86 32 指令集）包含如下关键代码；某用户的口令保存在字符数组 origPassword 中，用户输入的口令保存在字符数组 userPassword 中，如果两个数组中的内容相同则允许进入系统。

……

[….]

char origPassword[12]= “Secret”；

char origPassword[12];

[…]

gets(userPassword);　　/* 读取用户输入的口令*/

[…]

If(strncmp(origPassword,userPassword,12)!=0)

{

printf(“Password,doesn’ t match!/n”);

exit(-1);

}

[…]

/* 口令认证通过时允许用户访问*/

[…]

……

【问题 1】（4 分）

用户在调用 gets()函数时输入什么样式的字符串，可以在不知道的原始口令“Secret”的情况下绕过该口令验证函数的限制？

【问题 2】（4 分）

上述代码存在什么类型的安全隐患？请给出消除该安全隐患的思路。

我能过软考分析

本题考查缓冲区溢出以及防患措施。需重点掌握。

1、函数 strncmp（str1，str2，n）

【参数】str1, str2 为需要比较的两个字符串，n 为要比较的字符的数目。字符串大小的比较是以 ASCII 码表上的顺序来决定，此顺序亦为字符的值。Strncmp（）首先将 s1 第一个字符值减去 s2 第一个字符值，若差值为 0 则再继续比较下个字符，直到字符结束标志'\0'，若差值不为 0，则将差值返回。

【返回值】若 str1 与 str2 的前 n 个字符相同，则返回 0；若 s1 大于 s2，则返回大于 0 的值；若 s1 若小于 s2，则返回小于 0 的值。

程序中在定义两个数组时，会分配两个连续的 12 位地址空间，origPassword 在前，userPassword 在后，gets（）函数中，当 userPassword 输入位数大于 12 位时，就会溢出，多出来的字符将被写入到堆栈中，这就覆盖了堆栈原先的内容，根据函数的作用，只要 userPassword 的

值和 origPassword 的值一致则可绕过该口令验证函数的机制；当输入长度为 24 的字符串时，其中 12 位会产生溢出，根据堆栈的后进先出原理，当读取 userPassword 的值时，溢出的 12 位会读取到 userPassword 中，而在读取 origPassword 的值时会读取到原先 userPassword 中的值，如此两个数组的值就会一致，从而绕过该口令验证函数的限制。

2、gets（）函数可以无上限的读取，而且不会判断上限，因此，gets（）函数必须保证输入长度不会超过缓冲区，一旦大于该缓冲区就会造成溢出。可以使用安全函数来代替 gets（）函数，比如 fgets（）函数，或者对用户输入进行检查和校对，可通过 if 条件语句判断用户输入是否越界。

参考答案

【问题一】

只要输入长度为 24 的字符串，其前 12 个字符和后 12 个字符一样即可。

【问题二】

gets（）函数必须保证输入长度不会超过缓冲区，一旦输入大于 12 个字符的口令就会造成缓冲区溢出。

解决思路：使用安全函数来代替 gets（）函数，或者对用户输入进行检查和校对，可通过 if 条件语句判断用户输入是否越界。

考点 3：网络安全技术与产品案例分析

1. 2017 年上半年试题 3

阅读下列说明，回答问题 1 至问题 7，将解答写在答题纸的对应栏内。

【说明】

扫描技术是网络攻防的一种重要手段，在攻和防当中都有其重要意义。nmap 是一个 开放源码的网络扫描工具，可以查看网络系统中有哪些主机在运行以及哪些服务是开放 的。 namp 工具的命令选项: ss 用于实现 SYN 扫描，该扫描类型是通过观察开放端口和关闭端口对探测分组的响应来实现端口扫描的。

图3-1是在执行命令nmap-sS***时所捕获到的网络分组

97	192.168.220.129	192.168.220.1	64442 →	143	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
100	192.168.220.1	192.168.220.129	143 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0
101	192.168.220.129	192.168.220.1	64442 →	135	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
102	192.168.220.1	192.168.220.129	135 →	64442	{SYN,ACK} Seq=0 ACK=1 Win=8192 Len=0
103	192.168.220.129	192.168.220.1	64442 →	135	{RST} Seq=0 Win=0 Len=0
104	192.168.220.129	192.168.220.1	64442 →	139	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
105	192.168.220.1	192.168.220.129	139 →	64442	{SYN,ACK} Seq=0 ACK=1 Win=8192 Len=0
106	192.168.220.129	192.168.220.1	64442 →	139	{RST} Seq=0 Win=0 Len=0
107	192.168.220.129	192.168.220.1	64442 →	133	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
108	192.168.220.1	192.168.220.129	133 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0
109	192.168.220.129	192.168.220.1	64442 →	146	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
110	192.168.220.1	192.168.220.129	146 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0
111	192.168.220.129	192.168.220.1	64442 →	150	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
112	192.168.220.1	192.168.220.129	150 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0
113	192.168.220.129	192.168.220.1	64442 →	130	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
114	192.168.220.1	192.168.220.129	130 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0
115	192.168.220.129	192.168.220.1	64442 →	138	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
116	192.168.220.1	192.168.220.129	138 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0
117	192.168.220.129	192.168.220.1	64442 →	141	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
118	192.168.220.1	192.168.220.129	141 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0
119	192.168.220.129	192.168.220.1	64442 →	140	{SYN} Seq=0 Win=1024 Len=0 MSS=1460
120	192.168.220.1	192.168.220.129	140 →	64442	{RST,ACK} Seq=1 ACK=1 Win=0 Len=0

请根据图 3-1 回答下列问题

【问题 1】 (2 分)

此次扫描的目标主机的 IP 地址是多少?

【问题 2】(2 分)

SYN 扫描采用的传输层协议名字是什么?

【问题 3】 (2 分)

SYN 的含义是什么?

【问题 4】 (4 分)

目标主机开放了哪几个端口?简要说明判断依据。

【问题 5】(3 分)

每次扫描有没有完成完整的三次握手?这样做的目的是什么?

【问题 6】(5 分)

补全表 3-1 所示的防火墙过滤器规则的空(1) - (5) ， 达到防火墙禁止此类扫描流量进入和处出网络 ， 同时又能允许网内用户访问外部网页服务器的目的。

表 3-1 防火墙过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	ACK	动作
1	TCP	*	192.168.220.1/24	*	*	（4）	拒绝
2	TCP	192.168.220.1/24	*	> 1024	（3）	*	允许
3	（1）	192.168.220.1/24	*	> 1024	53	*	允许
4	UDP	*	192.168.220.1/24	53	> 1024	（5）	允许
5	（2）	*	*	*	*	*	拒绝

【问题 7】 (2 分)

简要说明为什么防火墙需要在进出两个方向上对据数据包进行过滤。

我能过软考分析

这道题在考查端口扫描与防火墙技术。解答端口扫描这类问题，判断源和目的最常用的方法就是看三次握手的发起方，在 TCP SYN 扫描中，不会建立完整的 tcp 连接，也就是只会出现两次握手。解题需要掌握 tcp 协议的过程和

防火墙的技术。如果对防火墙部分不理解的同学，可以再翻看一下书中 P279 的表格。

【问题 1】

TCP SYN 扫描，也叫半打开扫描。这种扫描方法并没有建立完整的 TCP 连接。客户端首先向服务器发送 SYN 分组发起连接。从图中可以看出，源主机地址为 192.168.220.129；目标主机为 192.168.220.1。

【问题 2】

TCP SYN 扫描是基于 TCP 协议的三次握手机制进行的。

【问题 3】

SYN（synchronous）：同步信号，是 TCP/IP 建立连接时使用的握手信号。在客户机和服务器之间建立正常的 TCP 网络连接时，客户机首先发出一个 SYN 消息，服务器使用 SYN+ACK 应答表示接收到了这个消息，最后客户机再以 ACK 消息响应。这样在客户机和服务器之间才能建立起可靠的 TCP 连接，数据才可以在客户机和服务器之间传递。

【问题 4】

TCP SYN 扫描，也叫半打开扫描。这种扫描方法并没有建立完整的 TCP 连接。客户端首先向服务器发送 SYN 分组发起连接，如果收到一个来自服务器的 SYN/ACK 应答，那么可以推断该端口处于监听状态。如果收到一 RST/ACK 分组则认为该端口不在监听。而客户端不管收到的是什么样的分组，都向服务器发送一个 RST/ACK 分组，这样并没有建立一个完整的 TCP 连接。

【问题 5】

半连接（SYN）扫描是端口扫描没有完成一个完整的 TCP 连接，在扫描主机和目标主机的一指定端口建立连接时候只完成了前两次握手，在第三步时，扫描主机中断了本次连接，使连接没有完全建立起来。这样即使日志中对扫描有所记录，但是尝试进行连接的记录也要比全扫描少得多；这样做的目的是防止对方主机的系统和防火墙记录此类扫描行为。

【问题 6】

第 1 条规则，拒绝从外网往内网发送的请求连接信息，所以 ACK=0；如填 ACK=*，也可以认为是正确的，*是通配符，包含 0 和 1。实际上，要拒绝任何的建立链接申请，ACK=0 就可以，***张老师（QQ66728193）建议填 0。***

第 2、3、4 条规则，配置允许内网用户访问外部网页服务器。

第 2 条规则，允许内网往外网服务器 80 端口发送的请求连接和应答信息，所以目的端口为 80；

第 3 条规则，允许内网向外网域名服务器发送的请求连接和应答信息，所以协议为 UDP；

第 4 条规则，允许外网域名服务器发往内网的应答信息，由于采用 UDP 协议方式，所以 ACK=*；有些答案认为 ACK=1，但张老师建议大家填*。

参考 P279，表 3-8，规则 E 和 F 的 ACK 值。

表 3-8　包过滤的实例

序号	源地址	源端口	目标地址	目标端口	协议	ACK	动作
A	202.114.63.0/24	>1024	*	80	TCP	*	accept
B	*	80	202.114.63.0/24	>1024	TCP	Yes	accept
C	*	>1024	202.114.64.125	80	TCP	*	accept
D	202.114.64.125	80	*	>1024	TCP	Yes	accept
E	202.114.63.0/24	>1024	*	53	UDP	*	accept
F	*	53	202.114.63.0/24	>1024	UDP	*	accept
G	*	*	*	*	*	*	drop

第 5 条规则，其他流量一律不允许进出内外部网络，所以协议为*。

【问题 7】

防火墙是一种位于内部网络与外部网络之间的网络安全系统，依照特定的规则，允许或是限制传输的数据通过，需要在进出两个方向对防火墙进行过滤设置，在进入方向过滤是为了防止被人攻击，而在出口方向过滤则是为了防止自己成为攻击的源头或者跳板。

参考答案

【问题 1】 192.168.220.1

【问题 2】 TCP 协议

【问题 3】同步信号，是 TCP/IP 建立连接时使用的握手信号。

【问题 4】

目标主机开放的端口为：135 端口，139 端口。判断依据：如果端口开放，目标主机会响应扫描主机的 SYN/ ACK 连接请求；如果端口关闭，则目标主机回向扫描主机发送 RST 的响应。

【问题 5】

没有完成；

第三个握手包没有发送，不完成整个握手协议过程，是避免扫描行为被目标主机记录在案，逃避检测，实现隐蔽扫描。

【问题 6】

（1）UDP　　（2）*　　（3）80　　（4）0　　**(5) ***

【问题 7】

在进入方向过滤是为了防止被人攻击，而在出口方向过滤则是为了防止自己成为攻击的源头或者跳板。

考点 4：信息系统安全基础案例分析

1. 2018 年上半年试题 1

阅读下列说明,回答问题 1 至问题 4,将解答填入答题纸的对应栏内。

【说明】

恶意代码是指为达到恶意目的专门设计的程序或者代码。常见的恶意代码类型有特洛伊木马、蠕虫、病毒、后门、Rootkit、僵尸程序、广告软件。

2017 年 5 月,勒索软件 WanaCry 席卷全球,国内大量高校及企事业单位的计算机被攻击,文件及数据被加密后无法使用,系统或服务无法正常运行,损失巨大。

【问题 1】（2 分）

按照恶意代码的分类,此次爆发的恶意软件属于哪种类型?

【问题 2】（2 分）

此次勒索软件针对的攻击目标是 Windows 还是 Linux 类系统?

【问题 3】（6 分）

恶意代码具有的共同特征是什么?

【问题 4】（5 分）

由于此次勒索软件需要利用系统的 SMB 服务漏洞(端口号 445)进行传播,我们可以配置防火墙过滤规则来阻止勒索软件的攻击,请填写表 1-1 中的空（1）-（5）,使该过滤规则完整。

注:假设本机 IP 地址为:1.2.3.4,”*”表示通配符。

表 1-1 防火墙过滤规则表

规则号	源地址	目的地址	源端口	目的端口	协议	ACK	动作
1	（1）	1.2.3.4	（2）	（3）	（4）	（5）	拒绝
…	…	…	…	…	…	…	…
…	*	*	*	*	*	*	拒绝

我能过软考分析

本题是对当年的热点结合进行了考查，虽然结合了当年的热点，但大部分还是可以在书中找到的知识点。

【问题 1】

WannaCry，一种“蠕虫式”的勒索病毒软件，大小 3.3MB，由不法分子利用 NSA 泄露的危险漏洞“EternalBlue”（永恒之蓝）进行传播。该恶意软件会扫描电脑上的 TCP445 端口(Server Message Block/SMB)，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。

【问题 2】

主要是利用 windows 操作系统中存在的漏洞。

【问题 3】

恶意代码是指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码。具有如下共同特征：（1） 恶意的目的（2） 本身是计算机程序（3） 通过执行发生作用。

【问题 4】

拒绝从外网往内网通过 445 端口传播的信息；源地址为*；源端口号为>1024,目的端口为 445，SMB 协议是基于 TCP 协议基础之上的，协议类型为 TCP，ACK=0。

参考答案

【问题一】蠕虫类型

【问题二】Windows 操作系统

【问题三】

恶意代码具有如下共同特征 p467：

1）恶意的目的 2） 本身是计算机程序 3） 通过执行发生作用。

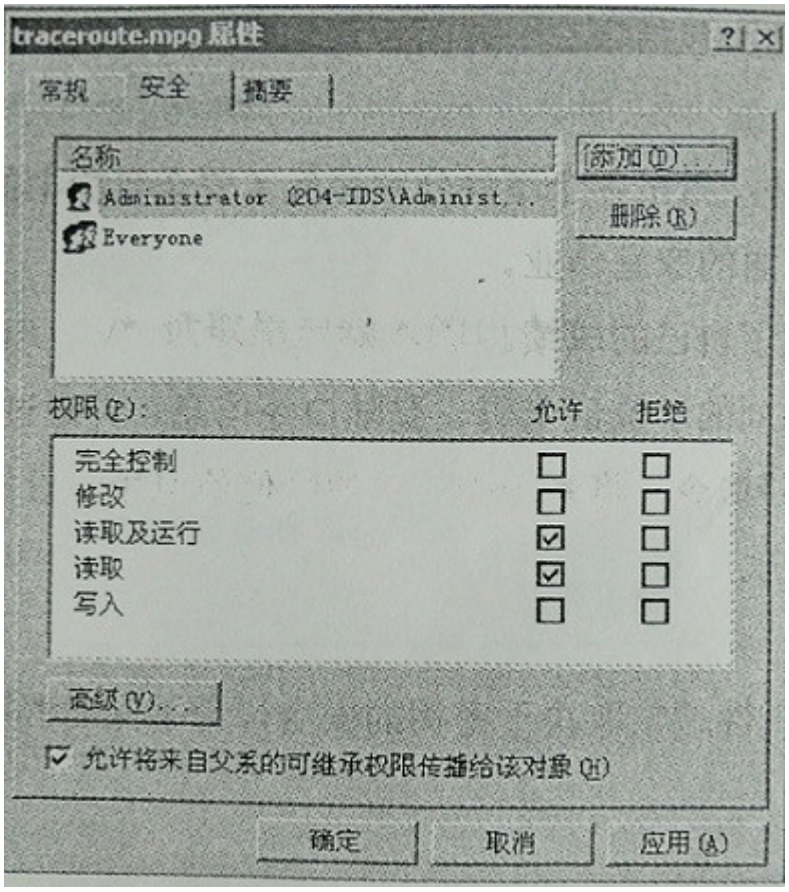
【问题四】（1）* （2）>1024 （3）445（4）TCP （5）0

2. 2016 年下半年试题 2

阅读下列说明和图，周答问题 1 至问题 2，将解答填入答题纸的对应栏内占

【说明】

访问控制是对信息系统资源进行保护的重要措施。适当的访问控制能够阻止未经授权的用户有意或者无意地获取资源。访问控制一般是在操作系统的控制下，按照事先确定的规则决定是否允许用户对资源的访问。图 2-1 给出了某系统对客体 traceroute.mpg 实施的访问控制规则。



【问题 1】（3 分）

针对信息系统的访问控制包含哪些基本要素?

【问题 2】（7 分）

分别写出图 2-1 中用户 Administrator 对应三种访问控制实现方法，即能力表、访问控制表和访问控制矩阵下的访问控制规则。

我能过软考分析

访问控制是在操作系统中保持文件的机密性和完整性的一种很重要的手段，有有不同的访问控制模型。本题的答案在书中 P423 的部分。

【问题 1】

访问控制的三个要素，即主体、客体和授权访问。

主体：一个主动的实体，该实体造成了信息的流动和系统状态的改变，它包括商户、用户组、终端、主机或一个应用，主体可议访问客体。

客体：指一个包含或接受信息的被动实体，对客体的访问要受控。它可以是一个字节、字段、记录、程序、文件，或者是一个处理器、存储器、网络节点等。

授权访问：指主体访问客体的允许，授权访问对每一对主体和客体来说是给定的，决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源。例如，授权访问有读写、执行，读写客体是直接进行的，而执行是搜索文件、执行文件。对用户的授权访问是由系统的安全策略决定的。

【问题 2】

能力表：以用户为中心建立权能表，表中规定了该用户可访问的文件名及访问能力。利用权能表可以很方便查询一个主体的所有授权访问。

即：（主体）Administrator <（客体）traceroute.mpg：读取，运行>

访问控制表：访问控制表是以文件为中心建立访问权限表。表中登记了该文件的访问用户名及访问权隶属关系。利用访问控制表，能够很容易地判断出对于特定客体的授权访问，哪些主体可以访问并有哪些访问权限。

即：（客体）traceroute.mpg<（主体）Administrator ：读取，运行>

访问控制矩阵：利用二维矩阵规定了任意主体和任意客体间的访问权眼。矩辞中的行代表主体的访问权限属性，矩阵中的列代表客体的访问权限属性，矩阵中的每一格表示所在行的主体对所在列的客体的访问授权。

即：

	（客体）traceroute.mpg
（主体）Administrator	读取，运行

参考答案

【问题一】　主体、客体、授权访问

【问题二】

能力表：

（主体）Administrator<（客体）traceroute.mpg：读取，运行>

访问控制表：

（客体）traceroute.mpg<（主体）Administrator：读取，运行>

访问控制矩阵：

	（客体）traceroute.mpg
（主体）Administrator	读取，运行

考点 5：信息系统安全工程案例分析

1. 2019 年上半年下午试题 1

阅读下列说明，回答问题 1 至问题 3,将解答填入答题纸的对应栏内。

[说明]

访问控制是保障信息系统安全的主要策略之一，其 主要任务是保证系统资源不被非法使用和非常规访问。访问控制规定了主体对客体访问的限制，并在身份认证的基础上，对用户提出的资源访问请求加以控制。当前，主要的访问控制模型包括:自主访问控制(DAC) 模型和强制访问控制(MAC) 模型。

[问题 1] (6 分)

针对信息系统的访问控制包含哪三个基本要素?

[问题 2] (4 分)

BLP 模型是一种强制访问控制模型，请问:

(1) BLP 模型保证了信息的机密性还是完整性?

(2) BLP 模型采用的访问控制策略是上读下写还是下读上写?

[问题 3] (4 分)

Linux 系统中可以通过 Is 命令查看文件的权限，例如:文件 net.txt 的权限属性如下所示:

----1- root root 5025 May 25 2019 /home/abc/net.txt

请问:

(1)文件 net. txt 属于系统的哪个用户?

(2)文件 net. txt 权限的数字表示是什么?

答案

[问题 1]

主体、客体、授权访问

[问题 2]

(1)机密性

(2) 下读上写

[问题 3]

(1) root 用户

(2) 700

试题分析

[问题 1]

访问控制的三个要素，即主体、客体和授权访问。

主体:一个主动的实体，该实体造成了信息的流动和系统状态的改变，它包括商户、用户组、终端、主机或-个应

用，主体可议访问客体。

客体:指一个包含或接受信息的被动实体，对客体的访问要受控。它可以是一个字节、字段、记录、程序、文件，

或者是一个处理器、 存储器、网络节点等。

授权访问:指主体访问客体的允许，授权访问对每一对主体和客体来说是给定的， 决定了谁能够访问系统，能访问

系统的何种资源以及如何使用这些资源。例如，授权访问有读写、执行，读写客体是直接进行的，而执行是搜索文

件、执行文件。对用户的授权访问是由系统的安全策略决定的。

[问题 2]

(1) BLP 模型是最早的一种安全模型，也是最著名的多级安全策略模型，属于状态机模型，采用线性排列安全许可

的分类形式来保证信启的保密性。

(2)上读- -下写方式保证了数据的完整性;上写一下读方式则保证了信息的秘密性。

[问题 3]

Linux 系统是一种典型的多用户系统，不同的用户处于不同的地位，拥有不同的权限。为了保护系统的安全性，Linux

系统对不同的用户访问同一文件(包括目录文件)的权限做了不同的规定。

-MWX--___-_ 1 root root 5025 May 25 2019 /home/abc/net.txt

在 Linux 中第一个字符代表这个文件是目录、 文件或链接文件等等。

当为[d]则是目录

当为[-]则是文件;

若是[1]则表示为链接文档(link file);

若是[b]则表示为装置文件里面的可供储存的接口设备(可随机存取装置);

若是[c]则表示为装置文件里面的串行端口设备，例如键盘、鼠标(- -次性读取装置)。

接下来的字符中，以三个为- -组，且均为「rwxJ 的三个参数的组合。其中，[r]代表可读(read)、[W]代表可写(write)、[x]代表可执行(execute), [-]代表没有权限。

每个文件的属性由左边第一部分的 10 个字符来确定 ，如下图所示:

从左至右用 0-9 这些数字来表示。

第 0 位确定文件类型，第 1-3 位确定属主(该文件的所有者)拥有该文件的权限。

第 4-6 位确定属组(所有者的同组用户)拥有该文件的权限，第 7-9 位确定其他用户拥有该文件的权限。其中，第 1、

4、7 位表示读权限，如果用"r"字符表示，则有读权限，如果用"-"字符表示，则没有读权限;

第 2、5、8 位表示写权限，如果用"w"字符表示，则有写权限，如果用” "字符表示没有写权限;第 3、6、9 位表示可

执行权限，如果用"x"字符表示，则有执行权限，如果用"-"字符表示，则没有执行权限。

在以上实例中，文件/net txt 的属主和属组都为 root 用户。

Linux 文件属性有两种设置方法，一种是数字， 一种是符号;文件的权限字符为: -----_ ，这九个权限是三个

三个- -组的，也可以使用数字来代表各个权限，各权限的分数对照表如下:

R: 4

W: 2

X: 1

:0

每种身份(owner/group/others)各自的三个权限(r/Wx)分数是需要累加的，例如当权限为: [----__ 分数则是:

owner= rWX= 4+2+1=7 ;

group= --= 0+0+0=0

others= --= 0+0+0= 0

所以设定权限的变更时，该文件的权限数字就是 700。

2. 2018 年上半年试题 3

阅读下列说明,答问题 1 至问题 3,将解答填入答题纸的对应栏内。

【说明】

在 Linux 系统中,用户账号是用户的身份标志,它由用户名和用户口令组成。

【问题 1】（4 分）

Linux 系统将用户名和口令分别保存在哪些文件中?

【问题 2】（7 分）

Linux 系统的用户名文件通常包含如下形式的内容:

root:x:0:0:root:root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

hujw:x:500:500:hujianwei:/home/hujw:/bin/bash

文件中的一行记录对应着一个用户,每行记录用冒号(:)分隔为 7 个字段,请问第 1 个冒号(第二列)和第二个冒号(第三列)的含义是什么?上述用户名文件中,第三列的数字分别代表什么含义?

【问题 3】（4 分）

Linux 系统中用户名文件和口令字文件的默认访问权限分别是什么?

我能过软考分析

Linux 和 windows 是最常见的两个操作系统，大多数人对 windows 并比较熟悉，但是对 linux 却不太了解。下面对 linux 的口令文件进行一个介绍。

在所有的类 unix 操作系统中都使用雷同的口令文件格式，linux 也不例外，在传统的 linux 系统中使用 passwd 文件加密存储口令，但问题在于 passwd 文件是全局可读的，加密算法是公开的，如果有恶意用户取得 passwd 文件，他就可以用穷举所有可能的明文通过相同的算法计算密文进行比较，直到相同，于是，他就破解了口令，针对这个问题，linux 和 unix 广泛采用了 shadow（影子）机制，将加密的口令转移到 shadow 文件里，shadow 文件只有 root 用户可读，同时在 passwd 文件的密文域显示为 x，从而最大限度减少密文泄露的机会。

【问题 1】

Linux 系统中，系统用户名是存放在/etc/passwd 文件中，口令是以加密的形式存放在/etc/shadow 文件中。

【问题 2】

在 Linux 系统中，系统用户名是存放在/etc/passwd 文件中，口令是以加密的形式存放在/etc/shadow 文件中。

/etc/passwd 文件介绍：

一般/etc/passwd 中一行记录对应着一个用户，每行记录又被冒号(:)分隔为 7 个字段，其格式和具体含义如下：

用户名:口令:用户标识号:组标识号:注释性描述:主目录:登录 Shell

用户名(login_name):是代表用户账号的字符串。通常长度不超过 8 个字符，并且由大小写字母和/或数字组成。登录名中不能有冒号(:)，因为冒号在这里是分隔符。为了兼容起见，登录名中最好不要包含点字符(.)，并且不使用连字符(-)和加号(+)打头。

口令(passwd):一些系统中，存放着加密后的用户口令字。虽然这个字段存放的只是用户口令的加密串，不是明文，但是由于/etc/passwd 文件对所有用户都可读，所以这仍是一个安全隐患。因此，现在许多 Linux 系统（如 SVR4）都使用了 shadow 技术，把真正的加密后的用户口令字存放到/etc/shadow 文件中，而在/etc/passwd 文件的口令字段中只存放一个特殊的字符，例如“x”或者“*”。

用户标识号(UID):是一个整数，系统内部用它来标识用户。一般情况下它与用户名是一一对应的。如果几个用户名对应的用户标识号是一样的，系统内部将把它们视为同一个用户，但是它们可以有不同的口令、不同的主目录以及

不同的登录 Shell 等。取值范围是 0-65535。0 是超级用户 root 的标识号，1-99 由系统保留，作为管理账号，普通用户的标识号从 100 开始。在 Linux 系统中，这个界限是 500。

组标识号(GID):字段记录的是用户所属的用户组。它对应着/etc/group 文件中的一条记录。

注释性描述(users):字段记录着用户的一些个人情况，例如用户的真实姓名、电话、地址等，这个字段并没有什么实际的用途。在不同的 Linux 系统中，这个字段的格式并没有统一。在许多 Linux 系统中，这个字段存放的是一段任意的注释性描述文字，用做 finger 命令的输出。

主目录(home_directory):也就是用户的起始工作目录，它是用户在登录到系统之后所处的目录。在大多数系统中，各用户的主目录都被组织在同一个特定的目录下，而用户主目录的名称就是该用户的登录名。各用户对自己的主目录有读、写、执行（搜索）权限，其他用户对此目录的访问权限则根据具体情况设置。

登录 Shell(Shell):用户登录后，要启动一个进程，负责将用户的操作传给内核，这个进程是用户登录到系统后运行的命令解释器或某个特定的程序，即 Shell。Shell 是用户与 Linux 系统之间的接口。Linux 的 Shell 有许多种，每种都有不同的特点。常用的有 sh(BourneShell),csh(CShell),ksh(KornShell),tcsh(TENEX/TOPS-20typeCShell),bash(BourneAgainShell)等。系统管理员可以根据系统情况和用户习惯为用户指定某个 Shell。如果不指定 Shell，那么系统使用 sh 为默认的登录 Shell，即这个字段的值为/bin/sh。

我们用个例子来看：

格式：注册名：口令：用户标识：用户组表示：默认目录：shell

Nobody：x：99：99：nobody：/

Usser1：x：501：501：/home/user1：/bin/bash

User2：x：503：503：/home/user2：/bin/bash

从 passwd 文件中能够看到，有两个用户，user1 和 user2，没有口令，分属不同的用户组。

/etc/shadow 文件介绍：

/etc/shadow 文件格式与/etc/passwd 文件格式类似，同样由若干个字段组成，字段之间用“:”隔开。

文件中字段主要含义为：登录名:加密口令:最后一次修改时间:最小时间间隔:最大时间间隔:警告时间:不活动时间:失效时间:标志

1、“登录名”是与/etc/passwd 文件中的登录名相一致的用户账号

2、“口令”字段存放的是加密后的用户口令字：

如果为空，则对应用户没有口令，登录时不需要口令；

星号代表帐号被锁定；

双叹号表示这个密码已经过期了；

6开头的，表明是用 SHA-512 加密；

1表明是用 MD5 加密；

2 是用 Blowfish 加密；

5 是用 SHA-256 加密；

3、“最后一次修改时间”表示的是从某个时刻起，到用户最后一次修改口令时的天数。时间起点对不同的系统可能不一样。例如在 SCOLinux 中，这个时间起点是 1970 年 1 月 1 日。

4、“最小时间间隔”指的是两次修改口令之间所需的最小天数。

5、“最大时间间隔”指的是口令保持有效的最大天数。

6、“警告时间”字段表示的是从系统开始警告用户到用户密码正式失效之间的天数。

7、“密码过期的宽限期”表示的是用户到期没有修改密码但账号仍能保持有效的最大天数。

（也有说包含账户活动期和账户最长生存期的说法）

用户标识号(UID)是一个整数，系统内部用它来标识用户。其取值范围是 0-65535。0 是超级用户 root 的标识号，1-99 由系统保留，作为管理账号，普通用户的标识号从 100 开始。在 Linux 系统中，这个界限是 500。

Shadow 文件

格式：用户：密码：上一次修改日期：密码不可改天数：密码需要修改期限：修改期限前 n 天发出警告：密码过期的宽限期：保留字段

Nobody：11：13675：0：9999：7：：：

User1：：13675：0：90：28：：

User1 用户，没有密码，上一次修改密码的日期距离 1970-1-1 日 13675 天，密码可以立刻修改，密码 90 天内需要修改，密码到期前 28 天通知。

User2：：13765：0：9999：7：：

User2 用户，没有密码，上一次修改密码的日期距离 1970-1-1 日 13675 天，密码可以立刻修改，密码永远不需要修改，密码到期前 7 天通知。

各字段值及含义：

密码字段：！！密码已经过期 *账户被锁定 6开头：sha-512 加密 1开头：MD5 加密 2开头：Blowfish 加密 5 sha-256 加密 空白表示没有密码

上一次修改密码的日期：上一次修改日期距离 1970 年 1 月 1 日的日期

密码需要修改期限：9999 表示永远不需要修改

【问题 3】

用户名/etc/passwd 文件，其文件所属用户有读和写的权限，文件所属组具有读的限权，其他的用户有读的限权，表示为 rw- r-- r--；口令字 /etc/shadow 文件，其文件所属用户有读的权限，文件所属组和其他的用户没有限权，表示为 r-- --- --- 。

参考答案

【问题 1】

用户名是存放在/etc/passwd 文件中，口令是以加密的形式存放在/etc/shadow 文件中

【问题 2】

第一个冒号的第二列代表口令；第二个冒号的第三列代表用户标识号。

root 用户 id 为 0；bin 用户 id 为 1；hujw 用户 id 为 500。

【问题 3】

用户名文件默认访问权限为 rw- r-- r--；

口令字文件的默认访问权限为 r-- --- ---。

3. 2018 年上半年试题 4

阅读下列说明和 C 语言代码,回答问题 1 至问题 4,将解答写在答题纸的对应栏内。

【说明】

在客户服务器通信模型中,客户端需要每隔一定时间向服务器发送数据包,以确定服务器是否掉线,服务器也能以此判断客户端是否存活,这种每隔固定时间发一次的数据包也称为心跳包。心跳包的内容没有什么特别的规定,一般都是很小的包。

某系统采用的请求和应答两种类型的心跳包格式如图 4-1 所示。

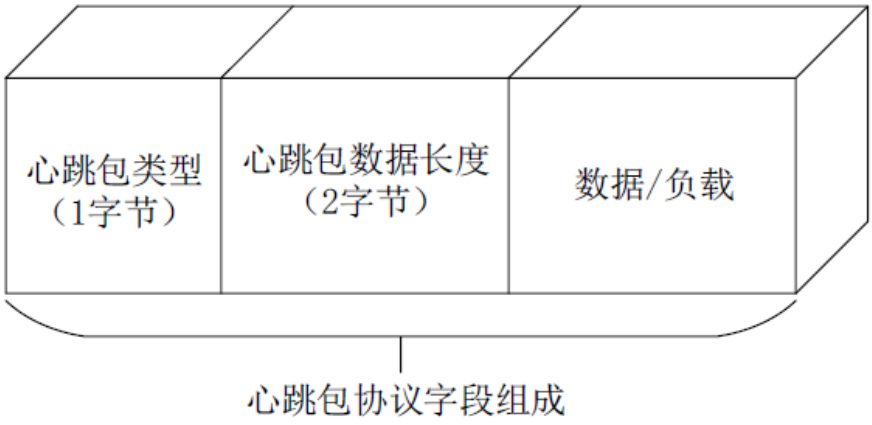


图 4-1 协议包格式

心跳包类型占 1 个字节，主要是请求和响应两种类型；

心跳包数据长度字段占 2 个字节，表示后续数据或者负载的长度。

接收端收到该心跳包后的处理函数是 process_heartbeat__(4)__,其中参数 p 指向心跳包的报文数据,s 是对应客户端的 socket 网络通信套接字。

```
void process_heartbeat(unsigned char *p, SOCKET s)
{
```

```
unsigned short hbtype;
unsigned int payload;
 hbtype=*p++;                    //心跳包类型
 n2s(p, payload);               //心跳包数据长度
pl=p;                     //pl 指向心跳包数据
if（hbtype=HB_REQUEST）{
     unsigned char *buffer, *bp;
     buffer=malloc(1+2+payload);
    *bp++=HB_RESPONSE;   //填充 1 byte 的心跳包类型
     s2n(payload, bp);     //填充 2 bytes 的数据长度
   memcpy(bp,pl,payload);
/*将构造好的心跳响应包通过 socket s 返回客户端  */
   r=write_bytes(s, buffer,3+payload);
 }
}
```

【问题 1】（4 分）

（1）心跳包数据长度字段的最大取值是多少?

（2）心跳包中的数据长度字段给出的长度值是否必须和后续的数据字段的实际长度一致?

【问题 2】（5 分）

（1）上述接收代码存在什么样的安全漏洞?

（2）该漏洞的危害是什么?

【问题 3】（2 分）

模糊测试(Fuzzing)是一种非常重要的信息系统安全测评方法,它是一种基于缺陷注入的自动化测试技术。请问模糊测试属于黑盒测试还是白盒测试?其测试结果是否存在误报?

【问题 4】（4 分）

模糊测试技术能否测试出上述代码存在的安全漏洞?为什么?

我能过软考分析

【问题 1】

已知表示心跳包的数据长度值为 2 字节，则其最大长度为 2^16-1=65535。

心跳包中的数据长度字段给出的长度值必须与后续的数据字段的实际长度一致； 如果不一致会产生“心脏出血”漏洞，造成有用数据泄露。

【问题 2】

心脏出血漏洞主要通过攻击者模拟向服务器端发送自己编写的 Heartbeat 心跳数据包，主要是 HeartbeatMessage 的长度与 payload 的 length 进行匹配，若 payload_lenght 长度大于 HeartbeatMessage 的 length，则会在服务器返回的 response 响应包中产生数据溢出，造成有用数据泄露。

题中每条心跳包记录中包含一个类型域(type)、一个长度域(length)和一个指向记录数据的指针(data)。心跳包的第一个字节标明了心跳包的类型。宏 n2s 从指针 p 指向的数组中取出前两个字节，并把它们存入变量 payload 中—

—这实际上是心跳包载荷的长度域(length)。注意程序并没有检查这条心跳包记录的实际长度。变量 pl 则指向由访问者提供的心跳包数据。

buffer=malloc(1+2+payload)；程序将分配一段由访问者指定大小的内存区域，这段内存区域最大为(65535 +1+2)个字节。变量 bp 是用来访问这段内存区域的指针。

代码中宏 s2n 与宏 n2s 干的事情正好相反：s2n 读入一个 16bit 长的值，然后将它存成双字节值，所以 s2n 会将与请求的心跳包载荷长度相同的长度值存入变量 payload。然后程序从 pl 处开始复制 payload 个字节到新分配的 bp 数组中——pl 指向了用户提供的心跳包数据。最后，程序将所有数据发回给用户。如果用户并没有在心跳包中提供足够多的数据，比如 pl 指向的数据实际上只有一个字节，那么 memcpy 会把这条心跳包记录之后的数据（无论那些数据是什么）都复制出来。

【问题 3】

模糊测试是一种黑盒测试技术，它将大量的畸形数据输入到目标程序中，通过监测程序的异常来发现被崩程序中可能存在的安全漏洞。模糊测试是一种基于缺陷注入的自动化测试技术，没有具体的执行规则，旨在预测软件中可能存在的错误以及什么样的输入能够触发错误。其通过模糊器向目标应用发送大量的畸形数据并监视程序运行异常以发现软件故障，通过记录触发异常的输入数据来进一步定位异常位置。与基于源代码的自盒测试相比，模糊测试的测试对象是二进制目标文件，因而具有更好的适用性:模糊测试是一种自动化的动态漏洞挖据技术，不存在误报，也不需要人工进行大量的逆向分析工作。

【问题 4】

网络协议的模糊测试的原理是通过特定的 Socket 形式将变异或者生成的含有错误信息的数据包发送给目标程序。根据协议的格式、定义，准备大量的测试数据，从客户端发送给服务器端，从而试图找到一些安全漏洞。

模糊测试有许多优点。

第一，模糊测试不需要程序的源代码即可发现问题。

第二，模糊测试不受限于被测系统的内部实现细节和复杂程度。例如，使用模糊测试可以不用关心被测对象的实现语言等细节。

第三， 使用模糊测试的可复用性较好，一个测试用例可适用于多种产品。

参考答案

【问题 1】

（1）心跳包数据长度的最大取值为 65535

（2）必须是一致的。

【问题 2】“心脏出血”漏洞；会造成有用数据的泄露。

【问题 3】属于黑盒测试；不存在误报。

【问题 4】

模糊测试技术能够测试出上述存在的安全漏洞；

网络协议的模糊测试是通过特定的 Socket 形式将变异或者生成的含有错误信息的数据包发送给目标程序。根据协议的格式、定义，准备大量的测试数据，从客户端发送给服务器端，从而试图找到一些安全漏洞，不需要程序的源代码即可发现问题。

4. 2017 年上半年试题 1

阅读下列说明，回答问题 1 至问题 3，将解答写在答题纸的对应栏内。

【说明】

安全目标的关键是实现安全的三大要素:机密性、完整性和可用性。对于一般性的信息类型的安全分类有以下表达形式:

{ (机密性，影响等级)， (完整性，影响等级)， (可用性，影响等级) }

在上述表达式中，"影响等级"的值可以取为低 (L)、中(M)、高(H) 三级以及不适用 (NA)。

【问题 1】。 (6 分)

请简要说明机密性、完整性和可用性的含义。

【问题 2】(2 分)

对于影响等级"不适用"通常只针对哪个安全要素?

【问题 3 】(3 分)

如果一个普通人在它的个人 Web 服务器上管理其公开信息。请问这种公开信息的安全分类是什么?

我能过软考分析

本题是在考查信息安全的基本属性，题目比较基础，在书中能够直接获得答案。问题三中的这样的考法需要我们注意。

【问题一】

（1）机密性：维护对信息访问和公开经授权的限制，包括保护个人隐私和私有的信息，机密性的缺失是指信息的非经授权的公开。

（2）完整性：防止信息不适当的修改和毁坏，包括保证信患的不可抵赖性和真实性。完整性的缺失是指信息未经授权的修改和毁坏。

（3）可用性：保证信息及时且可靠的访问和使用。可用性的缺失是指信息或信息系统的访问或使用被中断。

【问题二】

对于公开信息类型，机密性的缺失并没有什么潜在的影响，因为公开的信息没有保密的需求，所以机密性在公开信息类型中并不适用。

【问题三】

一个普通人在它的个人 Web 服务器上管理其公开信息。

首先机密性在公开信息类型中并不适用，比如在个人微博上发表了一篇博文，显然这是公开信息，机密性的缺失不受影响；

其次，对于完整性的缺失是一个 Moderate 的影响；

再次，对可用性的缺失也是一个 Moderate 的影响。这种类型的公开信息的安全分类表述如下:

{ (机密性， NA) , (完整性， M) , (可用性， M) }

参考答案

【问题一】

（1）机密性：维护对信息访问和公开经授权的限制，包括保护个人隐私和私有的信息。

（2）完整性：防止信息不适当的修改和毁坏，包括保证信患的不可抵赖性和真实性。

（3）可用性：保证信息及时且可靠的访问和使用。

【问题二】“不适用”通常针对机密性。

【问题三】

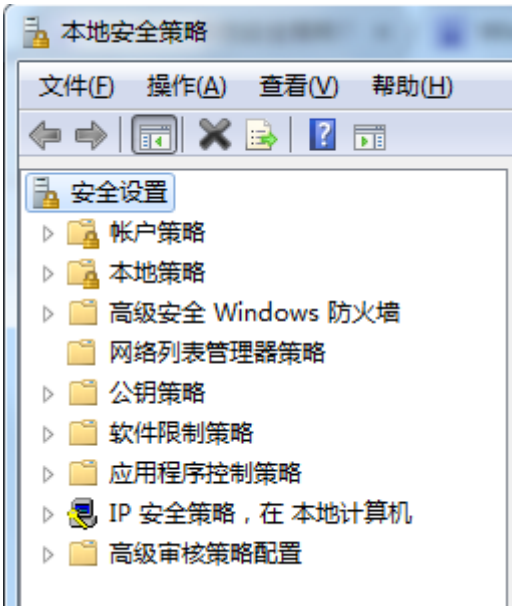
{（机密性，NA），（完整性，M），（可用性，M）}

5. 2017 年上半年试题 2

阅读下列说明，回答问题 1 和问题 2，将解答写在答题纸的对应栏内。

【说明】

Windows 系统的用户管理配置中，有多项安全设置，如图 2-1 所示。



【问题 1】(3 分)

请问密码和帐户锁定安全选项设置属于图中安全设置的哪一项?

【问题 2】(3 分)

Windows 的密码策略有一项安全策略就是要求密码必须符合复杂性要求，如果启用此策略，那么请问:用户 Administrator 拟选取的以下六个密码中的哪些符合此策略?

123456　　Admin123　　Abcd321

Admin@　　test123！　　123@host

我能过软考分析

本题考查 windows 操作系统安全的内容。第一题的内容在教材中 758 页，是一个比较容易忽略的点，第二题在书中给出了密码安全的要求，了解即可。

【问题一】

账户策略主要包括密码策略和账户锁定策略两种安全设置。

【问题二】

密码必须符合复杂性要求：启用此策略，用户账户使用的密码必须符合复杂性的要求。

- 密码复杂性必须符合下列最低要求：
- 不能包含用户的账户名；
- 不能包含用户姓名中超过两个连续字符的部分；
- 至少有六个字符长；
- 密码组成必须包含一下 4 类字符中的三类字符：

1、英文大写字母（A-Z）

2、英文小写字母(a-z)

3、10 个基本数字（0-9）

4、特殊符号（！@#￥%等)

参考答案

【问题一】

属于账号策略。

【问题二】

Abcd321　　test123!　　123@host

考点 6：信息系统安全工程

1. 2019 年上半年下午真题试题 5

阅读下列说明和图，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

[说明]

信息系统安全开发生命周期(Security Development Life Cycle (SDLC))是微软提出的从安全角度指导软件开发过程的管理模式，它将安全纳入信息系统开发生命周期的所有阶段，各阶段的安全措施与步骤如下图 5.1 所示。

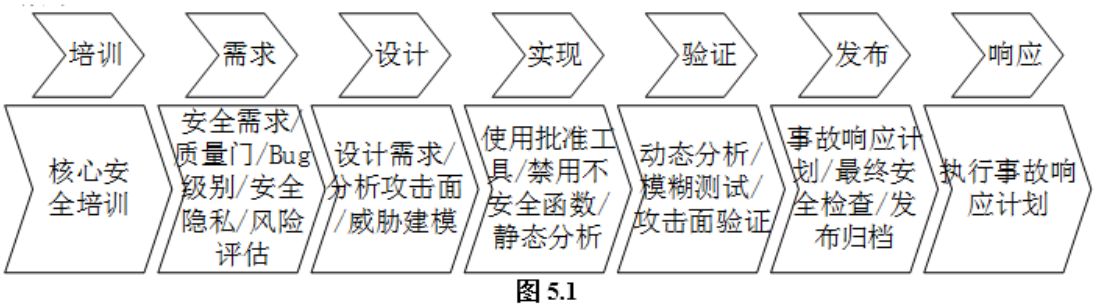


图 5.1

[问题 1] (4 分)

在培训阶段，需要对员工进行安全意识培训，要求员工向弱口令说不!针对弱口令最有效的攻击方式是什么?以下口令中，密码强度最高的是( )。

A. security2019

B.2019Security

C. Security@2019

D. Security2019

[问题 2] (6 分)

在大数据时代，个人数据正被动地被企业搜集并利用。在需求分析阶段，需要考虑采用隐私保护技术防止隐私泄露。从数据挖掘的角度，隐私保护技术主要有:基于数据失真的隐私保护技术、基于数据加密的隐私保护技术、基于数据匿名隐私保护技术。

请问以下隐私保护技术分别属于上述三种隐私保护技术的哪一种?

(1)随机化过程修改敏感数据

(2)基于泛化的隐私保护技术

(3)安全多方计算隐私保护技术

[问题 3] (4 分)

有下述口令验证代码:

```
#define PASSWORD "1234567"
int verify_ password (char *password)
{
int authenticated;
char buffer[8];
authenticated=strcmp(password ,PASSWORD);
strcpy(buffer ,password);
return authenticated;
```

```
}
int main(int argc , char* argv[ ])
{
int valid_ flag=0;
char password[1024];
while(1)
{
    printf("please input password: ");
    scanf("%s" ,password);
    valid_flag=verity_password(password),验证口令
    if( valid_flag)//口令无效
    {
        printf(  “incorrect password !n\n");
    }
    else //口令有效
    {
        print("Congratulation! You have passed the verification!\n");
        break;
}
}
```

其中 main 函数在调用 verify_password 函数进行口令验证时，堆栈的布局如图 5.2 所示。

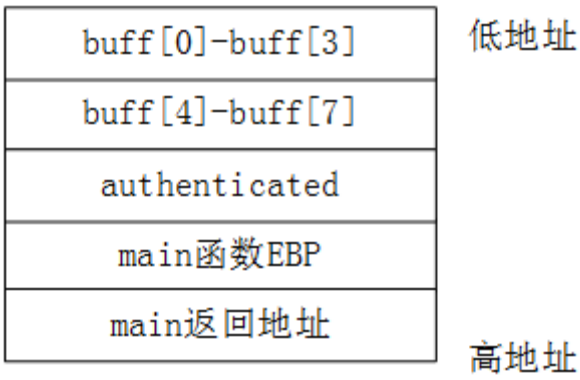


图 5.2

请问调用 verify_password 函数的参数满足什么条件，就可以在不知道真实口令的情况下绕过口令验证功能?

[问题 4] (3 分)

SDLC 安全开发模型的实现阶段给出了 3 种可以采取的安全措施，请结合问题 3 的代码举例说明?

答案

[问题 1]

(1)穷举攻击 (2) C

[问题 2]

(1)基于数据失真的隐私保护技术;

(2)基于数据匿名化的隐私保护技术;

(3)基于数据加密的隐私保护技术。

[问题 3]

参数 password 的值满足: 12 个字符的字符串，前面 8 个字符为任意字符，

后面 4 个字符为空字符。

[问题 4]

使用批准的工具来编写安全正确的程序;禁用不安全的函数来防范因数组没有边界检查而导致的缓冲区溢出;通过静态分析进行程字指针完整性检查。

试题分析

[问题 1]

(1)弱口令可以通过穷举攻击方式来破解。

(2)密码必须符合复杂性要求:启用此策略，用户账户使用的密码必须符合复杂性的要求。

密码复杂性必须符合下列最低要求:

不能包含用户的账户名;

不能包含用户姓名中超过两个连续字符的部分;

至少有六个字符长;

密码总必须包含以下 4 类字符中的三类字符:

1、英文大写字母(A-Z)

2、英文小写字母(a-z)

3、10 个基本数字(0-9)

4、特殊符号(! @#￥%等)

[问题 2]

(1)基于数据失真的隐私保护技术:它是使敏感数据失真但同时保持某些关

键数据或者属性不变的隐私保护技术，例如，采用交换(swapping)、添加噪声等技术对原始数据集进行处理，并且保证经过扰动处理后的数据仍然保持统计

方面的性质，以便进行数据挖掘等操作。

(2)基于数据加密的隐私保护技术:它是采用各种加密技术在分布式环境下隐藏敏感数据的方法，如安全多方计算

(SMC)分布式匿名化、分布式关联规则挖掘和分布式聚类等。

(3)基于数据匿名化的隐私保护技术:它是根据具体情况有条件地发布数据，例如，不发布原始数据的某些值、数据泛化等。

[问题 3]

该代码按正常流程走下来，函数 verify-password ()会返回变量 authenticated 的值，而只有当其值为 0 时，会绕过口令。

再来分析 strcpy()函数这个函数,该用来复制字符串，其原型为:

char *strcpy(char *dest, const char *srC);

[参数] dest 为目标字符串指针，src 为源字符串指针。

注意: src 和 dest 所指的内存区域不能重叠，且 dest 必须有足够的空间放置 src 所包含的字符串(包含结束符

NULL)。

[返回值]成功执行后返回目标数组指针 dest.

strcpy()把 src 所指的由 NULL 结束的字符串复制到 dest 所指的数组中，返回指向 dest 字符串的起始地址。

注意:如果参数 dest 所指的内存空间不够大，可能会造成缓冲溢出。

主函数中，当 valid- flag 为 0 时，会绕过口令，而 valid- flag 是函数 verify-

password（）的返回值，在函数 verify-password（）中，其返回值是变量 authenticated 的值，在返回该值时，使用了 strcpy 函数将 password 的值复制到数组 bufer 中，buffer 数组的长度为 8 个字符，一-用户输入数据长度大于 8 个字符就会溢出，溢出部分就会覆盖其他变量的值，从上图堆栈中的数据存储方式可以看出，bufer 数组一旦溢出，溢出部分就会覆盖 authenticated 的值;根据题目意思，只要令溢出部分的值为 0 即可令 authenticated=0,最终使得 valid-flag 为 0，从而满足条件。所以可以先任意输入 8 个字符堆满 bufer 数组，再输入时就是溢出部分，可以输入空字符，因 authenticated 为整形数据， 所以将字符赋给整形变量时，会按其 ASCI 码值进行处理,空字符的 ASICC 值为 0，从而可以把 authenticated 值变成 0 满足条件。

[问题 4]

使用批准的工具来编写安全正确的程序，只要在所有拷贝数据的地方进行数据长度和有效性的检查，确保目标缓冲区中数据不越界并有效,则就可以避免缓冲区溢出，更不可能使程序跳转到恶意代码上。禁用不安全的函数来防范因数组没有边界检查而导致的缓冲区溢出，C 语言中存在缓冲区溢出攻击隐患的系统函数有很多。例如 gets（），sprintf（），strcpy（），strcat()， fscanf()， scanf( )。vsprintf( )等。可以禁用这些不安全函数。通过静态分析进行程序指针完整性检查，在每次在程序指针被引用之 前先检测该指针是否己被恶意改动过，如果发现被改动,程序就拒绝执行。