内 容 简 介

信息安全工程师考试是计算机技术与软件专业技术资格（水平）考试的中级职称考试，是历年各级考试报名中的热点之一。本书汇集了从 2016 年到 2020 年的所有试题和权威的解析，参加考试的考生，认真读懂本书的内容后，将会更加了解考题的思路，对提升自己考试通过率的信心会有很大的帮助。

图书在版编目（CIP）数据

信息安全工程师 2016 至 2020 年试题分析与解答 / 计算机技术与软件专业技术资格考试研究部主编. —北京：清华大学出版社，2021.12
全国计算机技术与软件专业技术资格（水平）考试指定用书
ISBN 978-7-302-58925-9

Ⅰ. ①信… Ⅱ. ①计… Ⅲ. ①信息安全－安全技术－资格考试－题解 Ⅳ. ①TP309-44

中国版本图书馆 CIP 数据核字（2021）第 171774 号

责任编辑：杨如林
封面设计：杨玉兰
责任校对：徐俊伟
责任印制：宋 林

出版发行：清华大学出版社
网 址：http://www.tup.com.cn, http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 邮 编：100084
社 总 机：010-62770175 邮 购：010-83470235
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：大厂回族自治县彩虹印刷有限公司
经 销：全国新华书店
开 本：185mm×230mm 印 张：11.5 防伪页：1 字 数：276 千字
版 次：2021 年 12 月第 1 版 印 次：2021 年 12 月第 1 次印刷
定 价：49.00 元

产品编号：093772-01

前　言

根据国家有关的政策性文件，全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）已经成为计算机软件、计算机网络、计算机应用、信息系统、信息服务领域高级工程师、工程师、助理工程师（技术员）国家职称资格考试。而且，根据信息技术人才年轻化的特点和要求，报考这种资格考试不限学历与资历条件，以不拘一格选拔人才。现在，软件设计师、程序员、网络工程师、数据库系统工程师、系统分析师、系统架构设计师和信息系统项目管理师等资格的考试标准已经实现了中国与日本互认，程序员和软件设计师等资格的考试标准已经实现了中国与韩国互认。

计算机软件考试规模发展很快，至今累计报考人数超过 600 万人。

计算机软件考试已经成为我国著名的 IT 考试品牌，其证书的含金量之高已得到社会的公认。计算机软件考试的有关信息见网站www.ruankao.org.cn中的资格考试栏目。

对考生来说，学习历年试题分析与解答是理解考试大纲的最有效、最具体的途径。

为帮助考生复习备考，计算机技术与软件专业技术资格考试研究部组织编写了信息安全工程师 2016 至 2020 年的试题分析与解答，以便于考生测试自己的水平，发现自己的弱点，更有针对性、更系统地学习。

计算机软件考试的试题质量高，包括了职业岗位所需的各个方面的知识和技术，不但包括技术知识，还包括法律法规、标准、专业英语、管理等方面的知识；不但注重广度，而且还有一定的深度；不但要求考生具有扎实的基础知识，还要具有丰富的实践经验。

这些试题中，包含了一些富有创意的试题，一些与实践结合得很好的试题，一些富有启发性的试题，具有较高的社会引用率，对学校教师、培训指导者、研究工作者都是很有帮助的。

由于编者水平有限，时间仓促，书中难免有错误和疏漏之处，诚恳地期望各位专家和读者批评指正，对此，我们将深表感激。

编者

2021 年 8 月

目　　录

第 1 章　2016 下半年信息安全工程师

上午试题分析与解答

试题（1）

以下有关信息安全管理员职责的叙述，不正确的是__（1）__。

（1）A．信息安全管理员应该对网络的总体安全布局进行规划

B．信息安全管理员应该对信息系统安全事件进行处理

C．信息安全管理员应该负责为用户编写安全应用程序

D．信息安全管理员应该对安全设备进行优化配置

试题（1）分析

本题考查考生对于信息安全管理员职责的认识。

信息安全管理员是保障信息系统安全的主要管理者和安全技术的实施者，应该有明确的职责，具体包括：对网络的总体安全布局进行规划；对信息系统安全事件进行处理；对安全设备进行优化配置。信息安全管理员的职责中没有为用户编写安全应用程序这一项。

参考答案

（1）C

试题（2）

国家密码管理局于 2006 年发布了“无线局域网产品须使用的系列密码算法”，其中规定密钥协商算法应使用的是__（2）__。

（2）A．DH　　B．ECDSA　　C．ECDH　　D．CPK

试题（2）分析

本题考查考生对于密钥协商协议的了解。

2006 年，国家密码管理局规定的无线局域网产品须使用的系列密码算法中，密钥协商算法应使用 ECDH。

参考答案

（2）C

试题（3）

以下网络攻击中，__（3）__属于被动攻击。

（3）A．拒绝服务攻击　B．重放　　C．假冒　　D．流量分析

试题（3）分析

本题考查考生对于网络攻击方式的分类。

网络攻击行为分为主动攻击和被动攻击。主动攻击一般是指攻击者对被攻击信息的修改，而被动攻击主要是收集信息而不进行修改等操作，被动攻击更具有隐蔽性。主动攻击包

括拒绝服务攻击、重放攻击、假冒攻击等，被动攻击包括流量分析、窃听等。

参考答案

（3）D

试题（4）

（4）不属于对称加密算法。

（4）A．IDEA　　B．DES　　C．RC5　　D．RSA

试题（4）分析

本题考查考生对于密码算法分类的掌握情况。

根据密钥的属性，密码算法可以分为对称密码和非对称密码（公钥密码）。对称加密是指加密和解密使用相同密钥的加密算法，非对称加密算法则需要两个密钥：公钥和私钥。常见的对称密码包括：IDEA、DES、RC5、AES 等，常见的非对称密码包括：RSA、椭圆曲线密码算法等。

参考答案

（4）D

试题（5）

面向身份信息的认证应用中，最常用的认证方式是（5）。

（5）A．基于数据库认证　　B．基于摘要算法认证

C．基于 PKI 认证　　D．基于账户名/口令认证

试题（5）分析

本题考查考生对于身份认证方式的掌握情况。

身份认证是指在计算机及计算机网络系统中确认操作者身份的过程。通过身份认证可以确定用户是否具有对某种资源的访问和使用权限，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。面向身份信息的认证应用中最常用的认证方式是基于账户名/口令认证。

参考答案

（5）D

试题（6）

如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的系统称为（6）。

（6）A．公钥加密系统　　B．单密钥加密系统

C．对称加密系统　　D．常规加密系统

试题（6）分析

本题考查考生对于公钥密码特点的掌握情况。

根据密钥的属性，密码算法可以分为对称密码和非对称密码（公钥密码）。对称加密是指加密和解密使用相同密钥的加密算法，非对称加密算法则需要两个密钥：公钥和私钥。所以，如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥的加密系统是公钥加密系统。

参考答案

（6）A

试题（7）

S/Key 口令是一种一次性口令生成方案，它可以对抗__（7）__。

（7）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

试题（7）分析

本题考查考生 S/Key 口令性能的掌握情况。

S/Key 口令协议是一种一次性口令生成方案。客户向身份认证服务器提出连接请求，服务器应答并返回参数，客户输入口令，系统通过 Hash 计算产生一次性口令，传给服务器，服务器收到用户传过来的一次性口令，通过协议进行验证。该一次性口令生成方案具有较好的安全性，可以对抗重放攻击。

参考答案

（7）D

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__（8）__。

（8）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

试题（8）分析

本题考查考生对于防火墙功能的理解。

防火墙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。它的主要功能是保护内网安全，可以有效阻止外部攻击、外部威胁和病毒威胁等安全威胁。

参考答案

（8）A

试题（9）

以下行为中，不属于威胁计算机网络安全的因素是__（9）__。

（9）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

试题（9）分析

本题考查考生对于网络安全常识的了解。

网络安全防护是一项系统性工程。目前，威胁计算机网络安全的因素有很多，包括：操作员安全配置不当而造成的安全漏洞；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；安装非正版软件等。但是安装蜜罐系统并不会影响计算机网络系统的安全性能。

参考答案

（9）D

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__（10）__。

（10）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（10）分析

本题考查考生电子商务安全需求的理解。

电子商务是以信息网络技术为手段，以商品交换为中心的商务活动。由于网络的复杂性和脆弱性，以因特网为主要平台的电子商务的发展面临着严峻的安全问题。仅涉及交易的安全需求就包括：交易的真实性、交易的保密性和完整性、交易的不可抵赖性。电子商务本身具有商业交易的特点，交易应该具备可撤销性。

参考答案

（10）C

试题（11）

以下关于认证技术的叙述中，错误的是__（11）__。

（11）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

试题（11）分析

本题考查考生身份认证相关技术的理解。

身份认证是指在计算机及计算机网络系统中确认操作者身份的过程。通过身份认证可以确定用户是否具有对某种资源的访问和使用权限，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。数字签名是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生，其签名结果并非是十六进制的字符串。

参考答案

（11）B

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__（12）__。

（12）A．动态化原则　　B．木桶原则

C．等级性原则　　D．整体原则

试题（12）分析

本题考查考生对信息安全木桶原则的掌握情况。

由于攻击者往往会在系统中最薄弱的地方进行攻击，因此，需要对系统的安全漏洞和安全威胁进行分析、评估和检测，防止最常用的攻击手段，提高整个系统的“安全最低点”的安全性能，这就是木桶原则，即要求对信息进行均衡、全面地保护。

参考答案

（12）B

试题（13）

在以下网络威胁中，__（13）__不属于信息泄露。

（13）A．数据窃听　　B．流量分析

C．偷窃用户账号　　D．暴力破解

试题（13）分析

本题考查考生信息泄露这类安全威胁的理解。

对于网络用户来说，信息泄漏是一种常见的安全威胁，尤其是用户个人敏感信息的泄露，往往会造成很大的安全隐患。常见的信息泄露方式包括：数据窃听、网络流量分析、偷窃用户账号，这些属于被动攻击，而暴力破解属于主动攻击。

参考答案

（13）D

试题（14）

未授权的实体得到了数据的访问权，这属于对安全的__（14）__的破坏。

（14）A．保密性　　B．完整性

C．合法性　　D．可用性

试题（14）分析

本题考查考生对于信息安全基本属性的理解。

信息安全的基本属性包括：保密性、完整性、不可否认性、可用性和可控性。这也是信息安全技术需要实现的基本安全目标，未授权的实体得到了数据的访问权属于对信息保密性的破坏。

参考答案

（14）A

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__（15）__。

（15）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

试题（15）分析

本题考查考生对密码系统加密方式的掌握情况。

第 10 章　2020 下半年信息安全工程师

下午试题分析与解答

试题一（共 14 分）

阅读下列说明，回答问题 1 至问题 6，将解答填入答题纸的对应栏内。

【说明】

Linux 系统通常将用户名相关信息存放在/etc/passwd 文件中，假如有/etc/passwd 文件的部分内容如下，请回答相关问题。

security@ubuntu:~$ cat /etc/passwd

user1:x:0:0:user:/home/user1:/bin/bash

user2:x:1000:1000:ubuntu64:/home/user2:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

【问题 1】（2 分）

口令字文件/etc/passwd 是否允许任何用户访问？

【问题 2】（2 分）

根据上述/etc/passwd 显示的内容，给出系统权限最低的用户名字。

【问题 3】（2 分）

在 Linux 中，/etc/passwd 文件中每一行代表一个用户，每行记录又用冒号（:）分隔为 7 个字段，请问 Linux 操作系统是根据哪个字段来判断用户的？

【问题 4】（3 分）

根据上述/etc/passwd 显示的内容，请指出该系统中允许远程登录的用户名。

【问题 5】（2 分）

Linux 系统把用户密码保存在影子文件中，请给出影子文件的完整路径及其名字。

【问题 6】（3 分）

如果使用 ls-al 命令查看影子文件的详细信息，请给出数字形式表示的影子文件访问权限。

试题一分析

本题考查 Linux 系统身份认证和权限控制相关的知识点。

此类题目要求考生对常用的操作系统安全机制有清晰的理解，并对安全机制在操作系统中的具体实现及其使用能熟练掌握。题目围绕 Linux 系统的口令字文件/etc/passwd 设置相关

的考查点。

【问题 1】

因为操作系统通常都允许每个用户修改自己的身份信息包括口令，如果用户无法访问/etc/passwd 文件，则无法满足上述要求，因此任何用户都可以访问该文件。

【问题 2】

Linux 系统用户是根据用户 ID 来识别的，用户 ID 与用户名是一一对应的。用户 ID 取值范围是 0～65535。0 表示超级用户 root，1～499 表示系统用户，普通用户从 500 开始。用户 ID 由/etc/passwd 文件每一行用冒号隔开的第三列表示，由此得知本题的 user2 的用户 ID 值为 1000，属于普通用户，其权限最低。

【问题 3】

Linux 系统用户是根据用户 ID（UserID，简称 UID）来识别的。

【问题 4】

在/etc/passwd 的最后一列，可以看到有/usr/sbin/nologin 或者为空，通常意味着该用户无法登录系统。因此，user1/usre2/sync 用户可以登录。

【问题 5】

为了安全起见，用户口令通常保存在另外一个文件中，文件路径和名字为：/etc/shadow。

【问题 6】

上述影子文件不像 etc/passwd 文件，不是每个用户都可以访问的，否则每个人都能看到其他用户加密存储的口令字。该文件通常只能由 root 查看和修改，其他用户是没有任何访问权的。具体到不同的 Linux 类系统稍微有些不同，主要的访问权限有 640 或者 600 或者 400 或者 000。

参考答案

【问题 1】

允许

【问题 2】

user2

【问题 3】

第三个字段或者 UID 字段

【问题 4】

user1，user2，sync

【问题 5】

/etc/shadow

【问题 6】

640 或者 600 或者 400 或者 000

试题二（共 20 分）

阅读下列说明，回答问题 1 至问题 8，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】（3 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 C.I.A 分别表示什么？

【问题 2】（3 分）

RSA 公钥密码是一种基于大整数因子分解难题的公开密钥密码。对于 RSA 密码的参数：$p,q,n,\varphi(n),e,d$，哪些参数是可以公开的？

【问题 3】（2 分）

如有 RSA 密码算法的公钥为（55，3），请给出对小王的年龄 18 进行加密的密文结果。

【问题 4】（2 分）

对于 RSA 密码算法的公钥（55，3），请给出对应私钥。

【问题 5】（2 分）

在 RSA 公钥算法中，公钥和私钥的关系是什么？

【问题 6】（2 分）

在 RSA 密码中，消息 m 的取值有什么限制？

【问题 7】（3 分）

是否可以直接使用 RSA 密码进行数字签名？如果可以，请给出消息 m 的数字签名计算公式。如果不可以，请给出原因。

【问题 8】（3 分）

上述 RSA 签名体制可以实现【问题 **1**】所述的哪三个安全基本目标？

试题二分析

本题考查公钥密码算法 RSA 的基本原理及其加解密过程。

此类题目要求考生对常见的密码算法及其应用有清晰的了解。

【问题 1】

CIA 分别表示单词 Confidentiality、Integrity 和 Availability，也就是保密性、完整性和可用性三个安全目标的缩写。

【问题 2】

RSA 密码是基于大数分解难题，RSA 密码的参数主要有：$p,q,n,\varphi(n),e,d$，其中模数 $n=p\times q$，$\varphi(n)=(p-1)\times(q-1)$，$e\times d=1 \bmod \varphi(n)$，由这些关系，只有 n 和 e 作为公钥是可以公开的，其他的任何一个参数泄露，都会导致私钥泄露。

【问题 3】

根据 RSA 加密算法，密文 $c=18^3 \bmod 55=2$。

【问题 4】

根据 $n=55$，可知 $p=11$，$q=5$，$\varphi(n)=40$，由 e=3，可得到 $d=27$ 时满足 $e\times d=1 \bmod 40$，因