全国计算机技术与软件专业技术资格（水平）考试

2018 年上半年 信息安全工程师 上午试卷与解析

（考试时间 9：00～11：30 共 150 分钟）

请按下述要求正确填写答题卡

1. 在答题卡的指定位置上正确写入你的姓名和准考证号，并用正规 2B 铅笔在你写入的准考证号下填涂准考证号。 2. 本试卷的试题中共有 75 个空格，需要全部解答，每个空格 1 分，满分 75 分。 3. 每个空格对应一个序号，有 A、B、C、D 四个选项，请选择一个最恰当的选项作为解答，在答题卡相应序号下填涂该选项。 4. 解答前务必阅读例题和答题卡上的例题填涂样式及填涂注意事项。解答时用正规 2B 铅笔正确填涂选项，如需修改，请用橡皮擦干净，否则会导致不能正确评分。

http://www.cnitpm.com/exam/

1、2016 年 11 月 7 日,十二届全国人大常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

信管网参考答案：B

试题解析：

《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。

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

信管网参考答案：D

试题解析：

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)。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：A

试题解析：
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。

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
信管网参考答案：C
试题解析：
《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。

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
信管网参考答案：B
试题解析：
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。

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
信管网参考答案：C
试题解析：
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。

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

信管网参考答案：A

试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

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

信管网参考答案：C

试题解析：

安卓平台中恶意软件最常见的恶意行为是疯狂的给你推送各种弹窗、通知广告诱导你下载软件，然后捆绑其他应用，通过恶意扣费、窃取个人隐私信息、偷跑流量，直接或间接造成经济损失或隐私泄漏。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：B

试题解析：

“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。

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

信管网参考答案：A

试题解析：

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，它通过模拟一个 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。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：A

试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

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

信管网参考答案：C

试题解析：

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。

21、（　）是一种通过不断对网络服务系统进行扰,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

信管网参考答案：B

试题解析：

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。

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Wb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

信管网参考答案：A

试题解析：

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。

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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：A

试题解析：

Linux 系统所有的日志文件都在/var/log 目录下。

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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：A

试题解析：

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。

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

信管网参考答案：C

试题解析：

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。

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
信管网参考答案：B
试题解析：
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。

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
信管网参考答案：A
试题解析：
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。

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
信管网参考答案：D
试题解析：
公众运营商是公开信息，比如移动公司，不需要被保护。

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
信管网参考答案：A
试题解析：
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。

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
信管网参考答案：D
试题解析：
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。

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
信管网参考答案：C
试题解析：
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；而置乱是指将图像的信息次序打乱，使其变换成杂乱无章难以辨认的图像。

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
信管网参考答案：B
试题解析：
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。

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
信管网参考答案：A
试题解析：
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。

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
信管网参考答案：C
试题解析：
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。

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
信管网参考答案：B
试题解析：
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。

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
信管网参考答案：C
试题解析：
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。

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.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
信管网参考答案：C
试题解析：
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。

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
信管网参考答案：A
试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：C

试题解析：

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。

47、攻击者通过对目标主机进行端口扫可以直接获得（　）。

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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

49、文件型病毒不能感染的文件类型是（　）。

A.SYS 型

B.EXE 类型

C.COM 型

D.HTML 型

信管网参考答案：D

试题解析：

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。

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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：C

试题解析：

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。

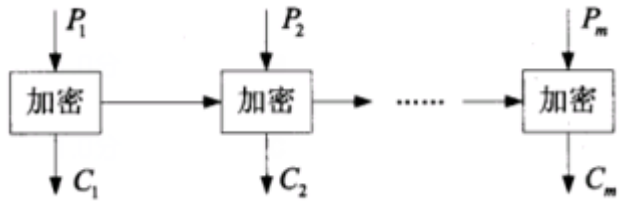
52、无线局域网鉴别和保密体系 WAPI 是我国无线局域网安全强制性标准,以下关于 WAP 的描述,正确的是（　）。

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 WAl 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
信管网参考答案：D
试题解析：
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。

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 Pi 表示明文分组,Ci 表示密文分组）



A.ECB 模式
B.CFB 模式
C.CBC 模式
D.OFB 模式
信管网参考答案：B
试题解析：
在 CFB 模式中，前一个密文分组会被送回到密码算法的输入端。

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
信管网参考答案：B
试题解析：
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。

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

信管网参考答案：A

试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：A

试题解析：

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 计算机多级安全模望，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。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：D

试题解析：

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)。

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露

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 不能同时实现信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,不具数据加密功能

信管网参考答案：A

试题解析：

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。

62、对于定义在 GF(p)上的椭圆曲线,取素数 P=11,椭圆曲线 y2=x3+x+6mod11,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

信管网参考答案：B

试题解析：

取 p=11， 椭圆曲线 y^2=x^3 +x+6。由于 p 较小，使 GF(p)也较小，故可以利用穷举的方法求出所有解点。穷举过程如下表所示。

x	x^3+x+6 mod 11	是否模 11 平方剩余	y
0	6	No	
1	8	No	
2	5	Yes	4,7
3	3	Yes	5,6
4	8	No	
5	4	Yes	2,9
6	8	No	
7	4	Yes	2,9
8	9	Yes	3,8
9	7	No	
10	4	Yes	2,9

其中模 11 平方剩余，其 x 的值可为 2、3、5、7、8、10 等。

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

信管网参考答案：B

试题解析：

当防火墙在网络层实现信息过滤与控制时，主要是针对 TCPIIP 协议中的 E 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。

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

信管网参考答案：C

试题解析：

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。

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

信管网参考答案：D

试题解析：

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。

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密来确定解密密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

信管网参考答案：B

试题解析：

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。

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

信管网参考答案：A

试题解析：

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 Merkle-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 64 比特。

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

信管网参考答案：A

试题解析：

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。

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

信管网参考答案：B

试题解析：

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。

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
信管网参考答案：C
试题解析：
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。

71-75、Trust is typically interpreted as a subjective belief in the reliability, honesty and security of an entity on which we depend （ ）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（ ）fails , then the sytems and applications that depend on it can（ ）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

信管网参考答案：B、A、B、B、A

试题解析：