tb：软考项目教育店

2023下半年信息安全工程师选择题真题

一、单项选择

1、如下有关信息安全管理员职责的论述，不对的的是()

A、信息安全管理员应当对网络的总体安全布局进行规划

B、信息安全管理员应当对信息系统安全事件进行处理

C、信息安全管理员应当负责为顾客编写安全应用程序

D、信息安全管理员应当对安全设备进行优化配置

2、国家密码管理局于 2023 年公布了“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（）

A、DH

B、ECDSA

C、ECDH

D、CPK

3、如下网络袭击中，（）属于被动袭击

A、拒绝服务袭击

B、重放

C、假冒

D、流量分析

4、（）不属于对称加密算法

A、 IDEA

B、DES

C、RCS

D、RSA

5、面向身份信息旳认证应用中,最常用旳认证措施是（）

A、基于数据库旳认证

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

6、假如发送方使用旳加密密钥和接受方使用旳解密密钥不相似,从其中一种密钥难以推出另一种密钥，这样旳系统称为()

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

7、 S / Ke y 口令是一种一次性口令生产方案，它可以对抗()

A、恶意代码木马袭击

B、拒绝服务袭击

C、协议分析袭击

D、重放袭击

8、防火墙作为一种被广泛使用的网络安全防御技术，其自身有某些限制，它不能制止()

A、内部威胁和病毒威胁

B、外部袭击

C、外部袭击、外部威胁和病毒威胁

D、外部袭击和外部威胁

9、如下行为中，不属于威胁计算机网络安全的原因是（）

A、操作员安全配置不妥而导致的安全漏洞

B、在不影响网络正常工作的状况下,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

10、电子商务系统除了面临一般的信息系统所波及的安全威胁之外,更轻易成为黑客分子的袭击目的,其安全性需求普遍高于一般的信息系统,电子商务系统中的信息安全需求不包括()

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

11、如下有关认证技术的论述中，错误的是()

A、指纹识别技术的运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措施

D、消息认证可以确定接受方收到的消息与否被篡改正

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

tb：软考项目教育店

13、在如下网络威胁中,()不属于信息泄露

A、数据窃听

B、流量分析

C、盗窃顾客账户

D、暴力破解

14、未授权的实体得到了数据的访问权，这属于对安全的()

A、机密性

B、完整性

C、合法性

D、可用性

15、按照密码系统对明文的处理措施,密码系统可以分为（）

A、置换密码系统和易位密码

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、分级密码系统和序列密码系统

16、数字签名最常见的实现措施是建立在()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

17、如下选项中,不属于生物识别措施旳是()

A、指纹识别

B、声音识别

C、虹膜识别

D、个人标识号识别

18、计算机取证是将计算机调查和分析技术应用于对潜在旳、有法律效应确实定和提取。如下有关计算机取证旳描述中,错误旳是()

A、计算机取证包括对以磁介质编码信息方式存储旳计算机证据旳提取和归档

B、计算机取证围绕电子证据进行，电子证据具有高科技性等特点

C、计算机取证包括保护目旳计算机系统， 确定搜集和保留电子证据， 必须在开计算机旳状态下进行

D、计算机取证是一门在犯罪进行过程中或之后 证据

19、注入语句: ：//xxx. xxx. xxx/abc. asp?p=YYandu s er>0 不仅可以判断服务器旳后台数据库与否为 SQL-SERVER,还可以得到()

A、目前连接数据库旳顾客数据

B、目前连接数据库旳顾客名

C、目前连接数据库的顾客口令

D、目前连接的数据库名

20、数字水印技术通过在数字化的多媒体数据中嵌入隐蔽的水印标识， 可以有效地对数字多媒体数据的版权保护等功能。如下各项工， 不属于数字水印在数字版权保护必须满足的基本应用需求的是()

A、安全性

B、隐蔽性

C、鲁棒性

D、可见性

21、有一种袭击是不停对网络服务系统进行干扰,变化其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪。这种袭击叫做()

A、重放袭击

B、拒绝服务袭击

C、反射袭击

D、服务袭击

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,可以采用的防备措施是()

A、将要访问的 Web 站点按其可信度分派到浏览器的不一样安全区域

B、在浏览器中安装数字证书

C、运用 IP安全协议访问 Web 站点

D、运用 SSL 访问 Web 站点

23、下列说法中,错误旳是()

A、服务袭击是针对某种特定袭击旳网络应用旳袭击

B、重要旳渗透威胁有特洛伊木马和陷阱

C、非服务袭击是针对网络层协议而进行旳

D、对于在线业务系统旳安全风险评估，应采用最小影响原则

24、根据国家信息安全等级保护有关原则,军用不对外公开旳信息系统至少应当属于（)

A、二级及二级以上

B、三级及三级以上

C、四级及四级以上

D、无极

25、电子邮件是传播恶意代码旳重要途径,为了防止电子邮件中旳恶意代码旳袭击,用(）方式阅读电子邮件

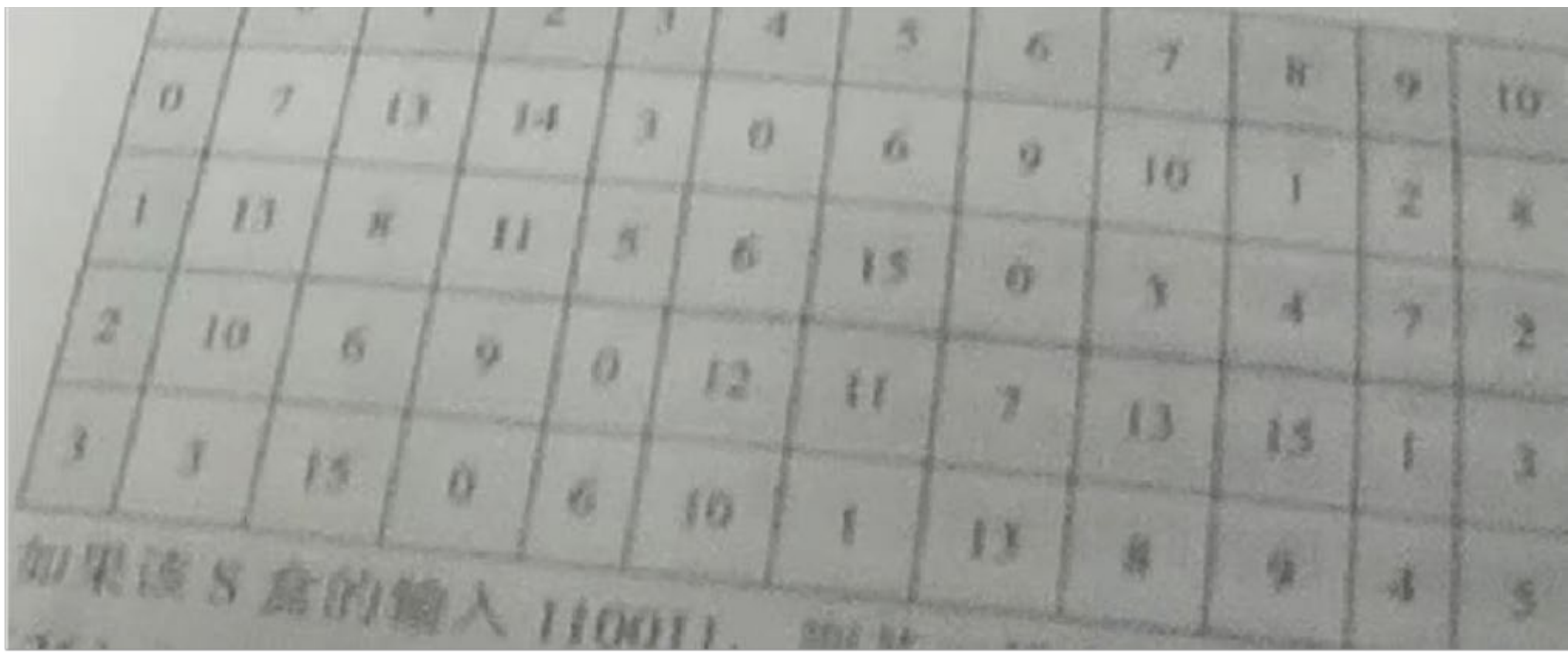
A、网页

B、 纯文本

C、程序

D、会话

26、已知 DES 算法旳 S 盒如下:



假如该 S 盒旳输入 110011,则其二进制输出为()

A、0110

B、1001

C、 0100

D、 0101

27、在 IPv4 旳数据报格式中，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

tb：软考项目教育店

28、Kerb er os 是一种常用旳身份认证协议，它采用旳加密算法是（）

A、Elgamal

B、DES

C、 MD5

D、RSA

29、如下有关加密技术旳论述中，错误旳是()

A、对称密码体制旳加密密钥和解密密钥是相似旳

B、密码分析旳目旳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旳

D、所有旳密钥均有生存周期

30、移动顾客有些属性信息需要受到保护,这些信息一旦泄露,会对公众顾客旳生命财产安全构成威胁。如下各项中,不需要被保护旳属性是()

A、顾客身份（ID)

B、顾客位置信息

C、终端设备信息

D、公众运行商信息

31、如下有关数字证书旳论述中,错误旳是()

A、证书一般有 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

D、证书一般携带 CA的公开密钥

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、截获密文并获得密钥

C、截获密文,理解加密算法和解密算法

D、截获密文,获得密钥并理解解密算法

33、运用公开密钥算法进行数据加密时，采用的措施是()

A、发送方用公开密钥加密，接受方用公开密钥解密

B、发送方用私有密钥加密，接受方用私有密钥解密

C、发送方用公开密钥加密，接受方用私有密钥解密

D、发送方用私有密钥加密,接受方用公开密钥解密

34、数字信封技术可以()

A、对发送者和接受者的身份进行认证

B、保证数据在传播过程中的安全性

C、防止交易中的抵赖发送

D、隐藏发送者的身份

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

36、甲不仅怀疑乙发给他的被造人篡改，并且怀疑乙的公钥也是被人冒充的,为了消除甲的疑虑,甲和乙决定找一种双方都信任的第三方来签发数字证书，这个第三方为()

A、国际电信联盟电信原则分部(ITU-T)

B、国家安全局（NSA)

C、认证中心（CA)

D、国标化组织（ISO)

37、WI－FI 网络安全接入是一种保护无线网络安全的系统， WPA 加密模式不包括()

A、WPA 和 WPA2

B、WPA-PSK

C、 WEP

D、WPA2-PSK

38、特洛伊木马袭击旳威胁类型属于()

A、授权侵犯威胁

B、渗透威胁

C、植入威胁

D、旁路控制威胁

39、信息通过网络进行传播旳过程中， 存在着被篡改旳风险,为了处理这一安全问题， 一般采用旳安全防护技术是()

A、加密技术

B、匿名技术

C、消息认证技术

D、数据备份技术

40、甲收到一份来自乙旳电子订单后，将订单中旳货品送到达乙时，乙否认自己曾经发送过这份订单，为理解除这种纷争，采用旳安全技术是()

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

tb：软考项目教育店

41、目前使用的防杀病毒软件的作用是()

A、检查计算机与否感染病毒,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、检查计算机与否感染病毒,清除部分已感染病毒

42、IP 地址分为全球地址和专用地址，如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

43、下列汇报中，不属于信息安全风险评估识别阶段的是()

A、资产价值分析汇报

B、风险评估汇报

C、威胁分析汇报

D、已经有安全威胁分析汇报

44、计算机犯罪是指运用信息科学技术且以计算机跟踪对象的犯罪行为， 与其他类型的犯罪相比,具有明显的特性，下列说法中错误的是（）

A、计算机犯罪具有隐蔽性

B、计算机犯罪具有高智能性,罪犯也许掌握某些其他高科技手段

C、计算机犯罪具有很强旳破坏性

D、计算机犯罪没有犯罪现场

45、如下对 OSI（开放系统互联）参照模型中数据链路层旳功能论述中,描述最贴切是()

A、保证数据对旳旳次序、无差错和完整

B、控制报文通过网络旳路由选择

C、提供顾客与网络旳接口

D、处理信号通过介质旳传播

46、深度流检测技术就是以流为基本研究对象，判断网络流与否异常旳一种网络安全技术，其重要构成部分一般不包括()

A、流特性选择

B、流特性提供

C 、分类器

D、 响应

47、一种全局旳安全框架必须包括旳安全构造原因是()

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

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

48、如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

C、入侵检测技术

D、差错控制

49、病毒的引导过程不包括()

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

50、网络系统中针对海量数据的加密，　一般不采用()

A、链路加密

B、会话加密

C、公钥加密

D、端对端加密

51、安全备份的方略不包括()

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、定期验证备份文献的对的性和完整性

52、如下有关安全套接层协议（SSL)的论述中,错误的是（）

A、是一种应用层安全协议

B、 为TCP/IP 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

53、入侵检测系统放置在防火墙内部所带来的好处是()

A、减少对防火墙的袭击

B、减少入侵检测

C、增长对低层次袭击的检测

D、增长检测能力和检测范围

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塑胶，智能卡的片内操作系统(COS)是智能卡芯片内的一种监控软件,如下不属于COS构成部分的是()

A、通讯管理模块

B、数据管理模块

C、安全管理模块

D、文献管理模块

55、如下有关IPSec协议的论述中，对的的是()

A、IPSec 协议是处理IP 协议安全问题的一

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

56、不属于物理安全威胁的是()

A、自然灾害

B、物理袭击

C、硬件故障

D、系统安全管理人员培训不够

57、如下有关网络钓鱼的说法中，不对的的是()

A、网络钓鱼融合了伪装、欺骗等多种袭击方式

B、网络钓鱼与 Web 服务没有关系

C、经典的网络钓鱼袭击都将被袭击者引诱到一种通过精心设计的钓鱼网站上

D、网络钓鱼是“社会工程袭击”是一种形式

tb：软考项目教育店

58、如下有关隧道技术说法不对的的是()

A、隧道技术可以用来处理 TCP / IP 协议的某种安全威胁问题

B、隧道技术的本质是用一种协议来传播此外一种协议

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

59、安全电子交易协议 SET 是有 VISA 和 MasterCard 两大信用卡组织联合开发的电子商务安全协议。如下有关 SET 的论述中，对的的是()

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 要实现的重要目的包括保障付款安全,确定应用的互通性和到达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

60、在 PKI中,不属于CA 的任务是()

A、证书的措施

B、证书的审改

C、证书的备份

D、证书的加密

tb：软考项目教育店

61、如下有关 VPN的论述中,对的的是()

A、VPN 指的是顾客通过公用网络建立的临时的、安全的连接

B、VPN 指的是顾客自己租用线路，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

62、扫描技术（）

A、只能作为袭击工具

B、只能作为防御工具

C、只能作为检查系统漏洞的工具

D、既可以作为工具，也可以作为防御工具

63、包过滤技术防火墙在过滤数据包时，　一般不关怀()

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

64、如下有关网络流量监控的论述中，不对的的是()

A、流量检测中所检测的流量一般采集自主机节点、 服务器、 路由器接口和途径等

B、数据采集探针是专门用于获取网络链路流量的硬件设备

C、流量监控可以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

65、两个密钥三重 DES 加密：C=CK1[DK2[EK1[P]]]，K1≠K2,其中有效的密钥为()

A、56

B、128

C、168

D、112

66、设在 RSA 的公钥密码体制中，公钥为（c,n)＝（13,35）,则私钥为()

A、11

B、13

C、15

D、17

67、杂凑函数SHAI 的输入分组长度为（)比特

A、128

B、258

C、512

D、1024

68、 AES 构造由如下 4 个不一样旳模块构成,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

69、67mod119 旳逆元是()

A、52

B、 67

C、16

D、19

70、在 DES 算法中，需要进行 16 轮加密,每一轮旳子密钥长度为()

A、16

B、32

C、48

D、64

71-75(1）isthe s cienceofhidinginformation.Whereasthegoal ofcryptographyistomakedataunreadablebyathirdparty. thegoal

tb：软考项目教育店

ofsteganographyistohidethedatafromathirdparty.Inthisart
icle, Iwilldi scusswhatsteganographyis,whatp ur posesits er
ves, an dwillprovideanexampleusingavailablesoftware.
Therearealargenumberofsteganographic(2) thatmostof usar efam
iliarwith (especiallyifyouwatchalotofsp y movies), ra ngin
gfrominvisibleinkandmicrodotstosecretingahiddenmessagein
thesecondletterofeachwordofalargebodyoftextandspreadsp
ectrumradiocommunication. Withcomputersandnetworks, the
rear emanyotherwaysofhidinginf orma tions,suchas :
Covertchannels (c,g,Lokiandsomedistributeddenial
-of-servicetoolsusetheInternetControl (3) Protocol , orIC
MP,asthecommunicationchannelbetweenthe“badguy”andacompro
micyedsystem)
HiddentextwithinWebpages
Hidingfilesin“plainsight”(c,g.whatbetterplaceto“hide”
afilethanwithanimportantsoundingnameinthec: \winntsyst
em32directory)
Nullciphers(c, g, u singthefirstletterofeach wor dtoformahi
ddenmessageinanotherwisein nocu oustext)

tb：软考项目教育店

steganographytoday,however,issignificantlymore (4) thanthee xampleaboutsuggest, allowingausertohidelargeamountsofi nformationwithinimageanda u dio.Theseformsofsteg ano gr aphyoften are usedi nco njunctionwithcryptographysothei nformationisdoubleprotected;firstitisencryptedandt henhiddensothatanadvertisem en tfirst. findtheinformatio n(anoftendifficulttaskinandofitself)andthedecryptedit.

Thesimplestapproachtohidingdatawithinanimagefileiscalled （5）signaturei nse r tion.Inthismethod,wecantakethebinaryre pre sen tationofthehiddendat aan dthebitofeachbytewithinthe covertimage. Ifweareusing24-bitcolortheamountandwillbemini muma ndindiscriminatetothehumane y e .

(1)A、Cryptography

B、Geography

C、Stenography

D、Steganograph y

(2)A、 methods

B、softwa re

C、tool s

D、services

（3）A、Member

B、Management

C、Message

D、Mail

(4)A、powerful

B、sophistication

C、advanced

D、easy

（5）A、 least

B、mo st

C、much

D、l ess

一、单项选择

1:C 2:C 3:D 4:D 5:D 6:A 7:D 8:A 9:D 10:C 11:B 12:D 13:D

14:A 15:A

16:C 17:D 18:C 19:B 20:D 21:B 22:A 23:B 24:B 25:B 26:C 27:D 28:C 29：C

30:D

31:D 32:D 33:C 34:B 35:A 36:C 37:C 38:C 39:C 40:A 41:D 42:B 43:B

44:D 45:A

46:D 47:B 48:D 49:D 50:C 51:C 52:A 53:B 54:B 55:A 56:D 57:B 58:C

tb：软考项目教育店

59:C 60:D

61:A 62:D 63:D 64:C 65:D 66:B 67:C 68:A 69:C 70:C 71:A 72:A 73:C

74:B 75:A