全国计算机技术与软件专业技术资格（水平）考试

2016 年下半年 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。

注：以下答案和解析仅供参考，最终答案以信管网和软题库考试系统答案为准

http://www.ruantiku.com

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

2016下半年信息安全工程师真题与查分专题（综合、案例）：http://www.cnitpm.com/zt/2016xaqcf/

1、以下有关信息安全管理员职责的叙述，不正确的是（）
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

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（）
A、DH
B、ECDSA
C、ECDH
D、CPK

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

4、（）不属于对称加密算法
A、IDEA
B、DES
C、RCS
D、RSA

5、面向身份信息的认证应用中，最常用的认证方法是（）
A、基于数据库的认证
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、如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的系统称为（）
A、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/Key 口令是一种一次性口令生产方案，它可以对抗（）
A、恶意代码木马攻击
B、拒绝服务攻击
C、协议分析攻击
D、重放攻击

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

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的情况下，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

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，更容易成为黑客分子的攻击目标，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、以下关于认证技术的叙述中，错误的是（）：做例子分析，答题技巧：很多题目都有技巧
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

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

13、在以下网络威胁中，（）不属于信息泄露
A、数据窃听
B、流量分析
C、偷窃用户账户
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方法，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、分组密码系统和序列密码系统

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（排除法）
D、公证系统和 MD4 摘要算法

17、以下选项中，不属于生物识别方法的是（）
A、指纹识别
B、声音识别
C、虹膜识别
D、个人标记号识别

18、计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效应的确定和提取。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息方式存储的计算机证据的提取和归档
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标计算机系统，确定收集和保存电子证据，必须在开计算机的状态下进行
D、计算机取证是一门在犯罪进行过程中或之后收集证据

19、注入语句：http：//xxx.xxx.xxx/abc.asp?p=YY 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据
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

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记，可以有效地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

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 站点
D、利用 SSL 访问 Web 站点

23、下列说法中，错误的是（）
A、服务攻击是针对某种特定攻击的网络应用的攻击
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

24、依据国家信息安全等级保护相关标准，军用不对外公开的信息系统至少应该属于（）
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、五级

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的攻击，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 算法的 S 盒如下：

如果该 S 盒的输入 110011，则其二进制输出为（）

	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

A、0110

B、1001

C、0100

D、0101

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

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

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

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构成威胁。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

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（CA 是签发机构）
B、证书携带持有者的公开密钥（看看）
C、证书的有效性可以通过验证持有者的签名（自己签发给自己的证书，可以这样验证）
D、证书通常携带 CA 的公开密钥（有颁发机构信息，通过信息可以查询到颁发机构的签名证书，利用签名证书验证证书）

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，了解加密算法和解密算法
D、截获密文，获得密钥并了解解密算法

33、利用公开密钥算法进行数据加密时，采用的方法是（）
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

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

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、甲不但怀疑乙发给他的被人篡改，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，这个第三方为（）
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、国家标准化组织（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

39、信息通过网络进行传输的过程中，存在着被篡改的风险，为了解决这一安全问题，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

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

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

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

43、下列报告中，不属于信息安全风险评估识别阶段的是（）
A、资产价值分析报告
B、风险评估报告
C、威胁分析报告
D、已有安全威胁分析报告

44、计算机犯罪是指利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，具有明显的特征，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，罪犯可能掌握一些其他高科技手段
C、计算机犯罪具有很强的破坏性
D、计算机犯罪没有犯罪现场（电子取证、现场勘探）

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（网络层）
C、提供用户与网络的接口
D、处理信号通过介质的传输（物理层）

46、深度流检测技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、流特征提供
C、分类器
D、响应

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
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、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
C、入侵检测技术
D、差错控制

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

50、网络系统中针对海量数据的加密，通常不采用（）

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（备份策略是为了保证服务持续性）
D、定期验证备份文件的正确性和完整性

52、以下关于安全套接层协议（SSL）的叙述中，错误的是（）
A、是一种应用层安全协议（介于传输层与应用层之间）
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、减少对防火墙的攻击
B、降低入侵检测
C、增加对低层次攻击的检测
D、增加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个监控软件，以下不属于 COS 组成部分的是（）
A、通讯管理模块（Transmission Manager）
B、数据管理模块
C、安全管理模块
D、文件管理模块（File Manager）

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（HASH 函数）
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（AH，ESP 都提供认证）

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

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都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”是一种形式

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 协议的某种安全威胁问题
B、隧道技术的本质是用一种协议来传输另外一种协议
C、IPSec 协议中不会使用隧道技术（IPsec 有隧道和传输两种模式）
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。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（公钥算法 RSA，对称密码算法是 DES）
B、SET 不需要可信的第三方认证中心的参与（第三方：支付网关）
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（数字签名、身份认证的过程）

60、在 PKI 中，不属于 CA 的任务是（）
A、证书的颁发
B、证书的审改
C、证书的备份
D、证书的加密

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

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

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

64、以下关于网络流量监控的叙述中，不正确的是（）
A、流量检测中所检测的流量通常采集自主机节点、服务器、路由器接口和路径等
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

65、两个密钥三重 DES 加密：$C=C_{K1}[D_{K2}[E_{K1}[P]]]$,K1≠K2，其中有效的密钥为（）应该是 EDE
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 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

69、67mod119 的逆元是（）乘法逆元
A、52
B、67
C、16
D、19

70、在 DES 算法中，需要进行 16 轮加密，每一轮的子密钥长度为（）
A、16
B、32
C、48
D、64

71-75（1）is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party. the goal of steganography（[ˌ stegə'nɒ grəfɪ]隐写术） is to hide the data from a third party. In this article, I will discuss what steganography is, what purposes it serves, and will provide an example using available software.

There are a large number of steganographic（2）that most of us are familiar with (especially if you watch a lot of spy movies), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding informations, such as:

Covert channels (c,g, Loki and some distributed denial-of-service tools use the Internet Control （3）Protocol, or ICMP, as the communication channel between the “bad guy” and a compromicyed system)

Hidden text within Web pages

Hiding files in “plain sight”(c,g. what better place to “hide” a file than with an important sounding name in the c:\winnt system32 directory)

Null ciphers(c,g, using the first letter of each word to form a hidden message in an otherwise innocuous text)

steganography today, however, is significantly more （4）than the example about suggest, allowing a user to hide large amounts of information within image and audio. These forms of steganography often are used in conjunction with cryptography so the information is double protected; first it is encrypted and then hidden so that an advertisement first. find the information (an often difficult task in and of itself) and the decrypted it.

The simplest approach to hiding data within an image file is called（5）signature insertion. In this method, we can take the binary representation of the hidden data and the bit of each byte within the covert image. If we are using 24-bit color the amount and will be minimum and indiscriminate to the human eye.

（1）A、Cryptography

B、Geography

C、Stenography

D、Steganography

（2）A、methods

B、software

C、tools

D、services

（3）A、Member

B、Management

C、Message

D、Mail

（4）A、powerful

B、sophistication（[səˌfɪstɪˈkeɪʃn]可理解为先进）

C、advanced

D、easy

（5）A、least（LSB：*least significant bit*）

B、most

C、much

D、less

参考答案可以到以下地址查看或下载：

http://www.cnitpm.com/zhenti/aq.html