信息安全工程师模拟试题上午卷 01

（1）"需要时，授权实体可以访问和使用的特性"指的是信息安全的（ ）。

A．保密性

B．完整性

C．可用性

D．可靠性

参考答案：C

（2）下面关于防火墙的说法，正确的是 （ ） 。

A、防火墙一般由软件以及支持该软件运行的硬件系统构成

B、防火墙只能防止未经授权的信息发送到内网

C、防火墙能准确地检测出攻击来自哪一台计算机

D、防火墙的主要支撑技术是加密技术

参考答案：A

（3）信息就像水、电、石油一样，与所有行业、所有人都相关，成为一种基础资源。因此，信息成为当今最具活力的生产要素和最重要的战略资源，以（ ）为核心的信息系统成为国家的重要基础设施。

A、计算机硬件

B、计算机网络

C、计算机软件

D、计算机安全

参考答案：B

（4）下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（ ）。

A、能够盗取用户数据或者传播非法信息的

B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的

C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的

D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

参考答案：A

（5） 在进行网闸配置时，每个物理设备可以关联的别名设备是（ ）个。

A、256

B、255

C、254

D、253

参考答案：D

（6） 在建立堡垒主机时，（ ）。

A、在堡垒主机上应设置尽可能少的网络服务

B、在堡垒主机上应设置尽可能多的网络服务

C、对必须设置的服务给予尽可能高的权限

D、不论发生任何入侵情况，内部网始终信任堡垒主机

参考答案：A

（7） 发送消息和用发送方私钥加密哈希加密信息将确保消息的：（ ）。

A、真实性和完整性

B、真实性和隐私

C、隐私和不可否认性

D、隐私和不可否性

参考答案：A

（8） 以下关于 CA 认证中心说法正确的是（ ）。

A、CA 认证时使用对称密钥机制的认证方法

B、CA 认证中心支负责签名，不负责证书的产生

C、CA 认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份

D、CA 认证中心不用保持中立，可以随便找一个用户来作为 CA 认证中心

参考答案：C

（9）PGP 加密算法是混合使用（ ）算法和 IDEA 算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A、DES

B、RSA

C、IDEA

D、AES

参考答案：B

（10）对入侵检测技术描述错误的是（ ）。

A、入侵检测的信息源包括主机信息源、网络信息源

B、入侵检测的 P2DR 模型是 Policy、Protection、Detection、Regponse 的缩写

C、入侵检测系统一般分为四个组件：事件产生器、事件分析器、响应单元、事件数据库

D、不同厂商的 IDS 系统之间需要通信，通信格式是 IETF

参考答案：D

（11)防火墙一般用来隔离内部网络与外部网络,确保内部网络安全,它必须保证实现(　)。
A、代理服务器功能
B、VPN 功能
C、所有内外网间的信息都经过防火墙
D、加密功能
参考答案：C

（12） CIDF 是（　）的简称。
A、通用入侵检测框架
B、通用入侵检测数据交换
C、安全部件互动协议
D、入侵检测接口标准
参考答案：A

（13） 下面对于 CC 的“保护轮廓”(PP)的说法最准确的是：（　）
A.对系统防护强度的描述
B.对评估对象系统进行规范化的描述
C.对一类 TOE 的安全需求，进行与技术实现无关的描述
D.由一系列保证组件构成的包，可以代表预先定义的保证尺度
参考答案：C

（14） IPSEC 的两种使用模式分别是_____和_____（　）
A.传输模式、安全壳模式
B.传输模式、隧道模式
C.隧道模式 、ESP 模式
D.安全壳模式、AH 模式
参考答案：B

（15）下面关于计算机恶意代码发展趋势的说法错误的是：（　）
A.木马和病毒盗窃日益猖獗
B.利用病毒犯罪的组织性和趋利性增加
C.综合利用多种编程新技术、对抗性不断增加
D.复合型病毒减少，而自我保护功能增加
参考答案：D

（16）网络安全在多网合一时代的脆弱性体现在（　）
A、网络的脆弱性
B、软件的脆弱性
C、管理的脆弱性
D、应用的脆弱性
参考答案：C

（17）抗 DDoS 防护设备提供的基本安全防护功能不包括（　）。

A、对主机系统漏洞的补丁升级

B、检测 DDoS 攻击

C、DDoS 攻击警告

D、DDoS 攻击防护

参考答案：A

相对于 DES 算法而言，RSA 算法的（18），因此，RSA（19）。

（18）A、加密密钥和解密密钥是不相同的

B、加密密钥和解密密钥是相同的

C、加密速度比 DES 要高

D、解密速度比 DES 要高

（19）A、更适用于对文件加密

B、保密性不如 DES

C、可用于对不同长度的消息生成消息摘要

D、可以用于数字签名

参考答案：A、D

某 Web 网站向 CA 申请了数字证书。用户登录该网站时，通过验证 （20） ，来确认该数字证书的有效性，从而 （21） 。

（20）A、CA 的签名

B、网站的签名

C、会话密钥

D、DES 密码

（21）A、向网站确认自己的身份

B、获取访问网站的权限

C、和网站进行双向认证

D、验证该网站的真伪

参考答案：A、D

（22）公开网上证券交易系统实时提供的最新股票报价，这种类型的公开信息的安全分类表述为（　）。

A、{（机密性， H），（完整性， M），（可用性， M）}

B、{（机密性， NA），（完整性， H），（可用性， H）}

C、{（机密性， NA），（完整性， M），（可用性， M）}

D、{（机密性， H），（完整性， H），（可用性， H）}

参考答案：B

（23） 在基于规则的安全策略中的授权通常依赖于（ ）。

A、安全性

B、敏感性

C、目地

D、角色

参考答案：B

（24）下列哪个版本的 Windows 自带了防火墙，该防火墙能够监控和限制用户计算机的网络通信。（ ）

A、 Windows 98

B、 Windows ME

C、 Windows 2000

D、 Windows XP

参考答案：D

（25）DNA 计算具有许多现在的电子计算所无法比拟的优点，以下不属于 DNA 计算的优点的是（ ）。

A、具有高度的并行性

B、极高的存储密度

C、极低的能量消耗

D、极快的存储速度

参考答案：D

（26） 拒绝服务不包括以下哪一项？（ ）。

A、DDoS

B、畸形报文攻击

C、Land 攻击

D、ARP 攻击

参考答案：D

（27） 以下哪种数据加密技术可以在基础架构层面进行？（ ）

A、IPSec

B、Secure Sockets Layer

C、Transport Layer Securit

D、RSA

参考答案：A

（28）RSA 是一种具有代表性的公钥加密算法。用户 A 利用 RSA 实施数字签名后不能抵赖的原因是( )
A.是 A 而不是第三方实施的签名
B.A 公布了自己的公钥，且不可伪造
C.RSA 签名需要使用接收方的公钥
D.只有 A 知道自己的私钥
参考答案：D

（29）甲向乙发送其数据签名，要验证该签名，乙可使用（ ）对该签名进行解密。
A. 甲的私钥　　B.甲的公钥　　C. 乙的私钥　　D. 乙的公钥
参考答案：B

（30）依据（2007）43 号《信息安全等级保护管理办法》，我国对信息系统的安全保护等级分为（ ）级
A、三
B、五
C、四
D、二
参考答案：B

（31） 卫星通讯中用到的加密模式是（ ）。
A、ECB
B、CBC
C、OFB
D、CFB
参考答案：C

（32） Outlook Express 中实现的邮件安全协议是（ ）。
A、PGP
B、S/MIME
C、POP3
D、SMTP
参考答案：B

（33） 王晓芸成功攻击了 MD5、SHA1 的什么性质？（ ）
A、定长输出
B、单向性
C、强抗碰撞性
D、弱抗碰撞性
参考答案：C

（34）一个审计评估系统，有对潜在的（ ）起到震慑或警告作用。

A、攻击者
B、不明身份者
C、异常动作者
D、外来者
参考答案：A

（35）下面安全套接字层协议（SSL）的说法错误的是？（　）
A、它是一种基于 Web 应用的安全协议
B、由于 SSL 是内嵌的浏览器中的，无需安全客户端软件，所以相对于 IPSEC 更简
C、SSL 与 IPSec 一样都工作在网络层
D、SSL 可以提供身份认证、加密和完整性校验的功能
参考答案：C

（36） 下列措施不能增强 DNS 安全的是（　）。
A、使用最新的 BIND 工具
B、双反向查找
C、更改 DNS 的端口号
D、不要让 HINFO 记录被外界看到
参考答案：C

（37） BOTNET 是（　）。
A、普通病毒
B、木马程序
C、僵尸网络
D、蠕虫病毒
参考答案：C

（38）比较先进的电子政务网站提供基于（ ）的用户认证机制用于保障网上办公的信息安全和不可抵赖性。
A．数字证书
B．用户名和密码
C．电子邮件地址
D．SSL
参考答案：A

（39）支持安全 WEB 服务的协议是( )。
A、HTTPS
B、WINS
C、SOAP
D、HTTP

参考答案：A

（40） NMAP 能收集目标主机的哪些信息？（ ）
A、目标主机用户信息和端口信息
B、目标主机的操作系统类型
C、目标主机的端口服务信息
D、目标主机的操作系统类型和端口服务信息
参考答案：D

（41） 信息分类是信息安全管理工作的重要环节，下面哪一项不是对信息进行分类时需要重点考虑的？（ ）
A. 信息的价值
B. 信息的时效性
C. 信息的存储
D. 法律法规的规定
参考答案：C

（42） 以下哪项不属于防止口令猜测的措施？（ ）
A、严格限定从一个给定的终端进行非法认证的次数;
B、确保口令不在终端上再现;
C、防止用户使用太短的口令;
D、使用机器产生的口令
参考答案：B

（43） 下列哪些不是广泛使用 http 服务器？（ ）
A、W3C
B、Apache
C、IIS
D、IE
参考答案：D

（44）（ ）增加明文冗余度。
A、混淆
B、扩散
C、混淆与扩散
D、都不是
参考答案：B

（45） 如果消息接受方要确定发送方身份，则要使用（ ）原则。
A、保密性
B、鉴别
C、完整性
D、访问控制
参考答案：B

（46） 下列哪项说法是错误的？（ ）
A、脆弱性分析系统仅仅是一种工具
B、脆弱性扫描主要是基于特征的
C、脆弱性分析系统本身的安全也是安全管理的任务之一
D、脆弱性扫描能支持异常分析
参考答案：D

（47） 目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门,《计算机信息系统国际联网保密管理规定》是由下列哪个部门所指定的规章制度？（ ）
A、公安部
B、国家保密局
C、信息产业部
D、国家密码管理委员会办公室
参考答案：B

（48） Unix 中，默认的共享文件系统在哪个位置？（ ）
A、/sbin/
B、/usr/local/
C、/export/
D、/usr/
参考答案：C

（49）网络钓鱼是指（）
A、通过大量发送声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。
B、网上进行钓鱼活动
C、通过网络组织钓鱼活动，从而获得利益
D、以上都不是
参考答案：A

（50）在传输模式 IPSec 应用情况中，以下哪个区域数据报文可受到加密安全保护？（ ）
A、整个数据报文
B、原 IP 头
C、新 IP 头
D、传输层及上层数据报文
参考答案：D

（51） 从安全的角度来看，运行哪一项起到第一道防线的作用？（ ）
A、远端服务器
B、WEB 服务器
C、防火墙
D、使用安全 shell 程序

参考答案：C

（52）对于 IIS 日志文件的访问权限，下列哪些设置是正确的？（　）
A、SYSTEM（完全控制）Administrator（完全控制）Users（修改）
B、SYSTEM（完全控制）Administrator（完全控制）Everyone（读取和运行）
C、SYSTEM（完全控制）Administrator（完全控制）Inernet 来宾账户（读取和运行）
D、SYSTEM（完全控制）Administrator（完全控制）
参考答案：D

（53）电气安全主要包括人身安全、（　）安全。
A、照明
B、设备
C、电器
D、空调
参考答案：B

（54）数字签名的功能不包括 （ ） 。
A、防止发送方和接收方的抵赖行为
B、发送方身份确认
C、接收方身份确认
D、保证数据的完整性
参考答案：C

（55）下列安全协议中，（ ）能保证交易双方无法抵赖。
A、SET
B、HTTPS
C、PGP
D、MOSS
参考答案：A

（56）按照 RSA 算法，若选两奇数 p=5，q=3，公钥 e=7，则私钥 d 为 （ ） 。
A、6
B、7
C、8
D、9
参考答案：B

（57） WEB 服务的安全通信的主要方式是什么？（　）
A、IPSEC
B、SSL
C、L2TP
D、SET
参考答案：B

（58） 以下哪种安全模型未使用针对主客体的访问控制机制？（ ）
A、基于角色模型
B、自主访问控制模型
C、信息流模型
D、强制访问控制模型
参考答案：C

（59）（ ）指对主体访问和使用客体的情况进行记录和审查，以保证安全规则被正确执行，并帮助分析安全事故产生的原因。
A.安全授权
B.安全管理
C.安全服务
D. 安全审计

参考答案：D

（60）小张的U盘中存储有企业的核心数据。针对该U盘，以下有关信息安全风险评估的描述中，不正确的是（ ）。
A．风险评估首先要确定资产的重要性，由于该U盘中存储有核心数据，安全性要求高，因此该U盘重要性赋值就高
B．如果公司制定了U盘的安全使用制度，小张的U盘就不具有脆弱性
C．如果小张的计算机在接入U盘时没断网线，木马病毒就构成对该U盘的威胁
D．风险分析要同时考虑资产的重要性、威胁概率和脆弱性严重程度
参考答案：B

（61）在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的？（ ）
A、自下而上
B、自上而下
C、上下同时开展
D、以上都不正确
参考答案：B

（62） 在许多组织机构中，产生总体安全性问题的主要原因是（ ）。
A、缺少安全性管理
B、缺少故障管理
C、缺少风险分析
D、缺少技术控制机制
参考答案：A

（63）信息安全是信息网络的硬件、软件及系统中的（　　）受到保护，不因偶然或恶意的原因而受到破坏、更改或泄露。

A．数据

B．管理制度

C．用户

D．设备

参考答案：A

（64）数字签名技术，在接收端，采用（　　）进行签名验证。

A．接收者的公钥

B．发送者的私钥

C．发送者的公钥

D．接收者的私钥

参考答案：C

（65） 在数据库中，下列哪些数据不能加密？（　）

A、索引字段

B、存放日期字段

C、存放密码的

D、存放名称字段

参考答案：A

（66）以下不属于防火墙的优点的是（　）。

A、防止非授权用户进入内部网络

B、可以限制网络服务

C、方便地监视网络的安全情况并报警

D、利用 NAT 技术缓解地址空间的短缺

参考答案：B

（67）签名过程中需要第三方参与的数字签名技术称为（　）。

A、代理签名

B、直接签名

C、仲裁签名

D、群签名

参考答案：C

（68）哪一个不是与终端服务器建立远程连接的客户端？（　）

A、telnet

B、通过 MS 安装程序软件安装包的独立的 16 位或 32 位可执行文件

C、MMC 管理单元

D、终端服务器高级客户端

参考答案：A

（69）2005 年 4 月，《中华人民共和国电子签名法》正式施行。（　）主要规定了关于数据电文、电子签名与认证及相关的法律责任。

A、《电子政务法》

B、《中华人民共和国著作权法》

C、《中华人民共和国网络安全法》

D、《电子签名法》

参考答案：D

（70）数字证书不包括（　）。

A、签名算法

B、证书拥有者的信用等级（信用等级并非由数字证书决定）

C、数字证书的序列号

D、颁发数字证书单位的数字签名

参考答案：B

The Data Encryption Standard (71) and the Advanced Encryption Standard (72) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted). Despite its deprecation as an officia1 standard, DES (especially its sti1l-approved and much more secure trip1e-DES variant) remains quite popu1ar it is used across a wide range of applications，from ATM encryption to e-mail privacy and secure remote access .Many other block ciphers have been designed and re1eased, with considerable variation in qua1ity.Many have been thorough1y broken. See Category：（ 73 ）.

（ 74 ）, in contrast to the ‘block’ type, create an arbitrari1y 1ong stream of key materia1, which is combined with the p1aintext（75）or character-by-character,.somewhat 1ike the one-time pad. In a stream cipher, the output stream is created based on an interna1 state which changes as the cipher operates. That state change is controlled by the key, and, in some stream ciphers, by the p1aintext stream as well. RC4 is an examp1e of a well -known, and wide1y used, stream cipher; see Category：Stream ciphers.

（71）A. DES　B. AES　C. RC4　D. ATM

（72）A. DES　B.AES　C. RC4　D. ATM

（73）A. Stream ciphers　B. Sequence ciphers　C. Symmetric ciphers　D. Block ciphers

（74）A. Stream ciphers　B. Sequence ciphers　C. Symmetric ciphers　D. Block ciphers

（75）A. word-by-word　B. sentence-by-sentence C. bit-by-bit　D. group-by-group

参考答案：A B D A C

信息安全工程师上午卷 02

（1）DES 是一种 （ ） 算法。

A、共享密钥

B、公开密钥

C、报文摘要

D、访问控制

参考答案：A

（2） 在信息安全的服务中，访问控制的作用是什么？（ ）

A、如何确定自己的身份，如利用一个带有密码的用户帐号登录

B、赋予用户对文件和目录的权限

C、保护系统或主机上的数据不被非认证的用户访问

D、提供类似网络中“劫持”这种手段的攻击的保护措施

参考答案：B

（3）我国居民二代身份证正在使用 256 位的（ ），国内外的许多电子商务系统正在使用 1024 位的 RSA 密码。

A、椭圆曲线密码

B、Elgamal 密码

C、MD5 密码

D、SHA 密码

参考答案：A

（4） 信息安全的基本属性是（ ）。

A. 机密性

B. 可用性

C. 完整性

D. 上面 3 项都是

参考答案：D

（5）网络安全最终是一个折衷的方案，即安全强度和安全操作代价的折衷，除增加安全设施投资外，还应考虑（ ）。

A. 用户的方便性

B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持

D. 上面 3 项都是

参考答案：D

（6） 以下哪种符号在 SQL 注入攻击中经常用到？（ ）

A、$_

B、1

C、@
D、;
参考答案：D

（7）下列关于口令持有人保证口令保密性的正确做法是：（　）
A. 将口令记录在笔记本中
B. 将口令贴在计算机机箱或终端屏幕上
C. 将计算机系统用户口令借给他人使用
D. 一旦发现或怀疑计算机系统用户口令泄露，立即更换
参考答案：D

（8）以下关于网络物理隔离技术的描述中，错误的是( )。
A.内网与外网(或内网与专网)永不连接
B.内网与外网(或内网与专网)的数据交换采用渡船策略
C.每一次数据交换，都需要经历数据写入和数据读出两个过程
D.内网和外网(或内网与专网)在同一时刻最多只有一个物理隔离设备建立 TCP/IP 数据连接
参考答案：D

（9）信息安全策略的设计与实施步骤是( )。
A.定义活动目录角色、确定组策略管理安全性、身份验证、访问控制和管理委派
B.确定标准性、规范性、可控性、整体性、最小影响、保密性原则，确定公钥基本结构
C.确定安全需求、制订可实现的安全目标、制订安全规划、制订系统的日常维护计划
D.确定安全需求、确定安全需求的范围、制订安全规划、制订系统的日常维护计划
参考答案：C

（10）以下关于 WLAN 安全机制的叙述中，（　）是正确的
A、WPA 是为建立无线网络安全环境提供的第一个安全机制
B、WEP 和 IPSec 协议一样，其目标都是通过加密无线电波来提供安全保护
C、WEP2 的初始化向量（IV）空间 64 位
D、WPA 提供了比 WEP 更为安全的无线局域网接入方案
参考答案：D

（11） 以下哪两个安全模型分别是多级完整性模型和多边保密模型？（　）
A.Biba 模型和 Bell 一 Lapadula 模型
B.Bell 一 Lapaduia 模型和 Biba 模型
C.Chinese Wall 模型和 Bell 一 Lapadula 模型
D.Biba 模型和 Chinese Wall 模型
参考答案：D

（12）在层的方式当中，哪种参考模型描述了计算机通信服务和协议？（　）
A、IETF 因特网工程工作小组
B、ISO 国际标准组织
C、IANA 因特网地址指派机构

D、OSI 开放系统互联
参考答案：D

（13）网络空间安全的核心内涵是（　）
A、硬件安全
B、信息安全
C、平台安全
D、数据安全
参考答案：B

（14）在应用层协议中，（　）既可使用传输层的 TCP 协议，又可用 UDP 协议。
A.SNMP
B.DNS
C.HTTP
D.FTP
参考答案：B

（15）某企业应用系统为保证运行安全，只允许操作人员在规定的工作时间段内登录该系统进行业务操作，这种安全策略属于（ ）层次。
A. 数据域安全
B. 功能性安全
C. 资源访问安全
D. 系统级安全

参考答案：D

（16）以下关于信息安全管理的描述中，错误的是( )。
A.安全管理贯穿于计算机网络系统规划、设计、实施、运维等各个阶段，既包括行政手段，又包括技术措施
B.一级安全管理制度的控制点有两个，二级、三级、四级安全管理制度的控制点有 3 个
C.信息安全的 3 条基本管理原则是:单独工作原则、限制使用期限原则和责任分散原则
D.在安全管理中，最活跃的因素是人，对人的管理基于完备安全管理政策和制度这一前提

参考答案：C

（17）以下关于校验码的叙述中，正确的是 （ ） 。
A、海明码利用多组数位的奇偶性来检错和纠错
B、海明码的码距必须大于等于 1
C、循环冗余校验码具有很强的检错和纠错能力
D、循环冗余校验码的码距必定为 1

参考答案：A

（18）关于网络安全措施，以下说法错误的是（　　）。
A.加强口令管理
B.从著名网站上下载资料
C.安装防火墙
D.不限制浏览内容
参考答案：D

（19）一般而言，网络安全审计从审计级别上可分为（　　）、应用级设计和用户级审计三种级别
A、组织级审计
B、物理审计
C、系统级审计
D、单元级审计
参考答案：C

（20）目前 Word 加密时，使用的对称加密算法是（　）。
A、DES
B、RC4
C、AES
D、RSA
参考答案：B

（21）单项散列函数的安全性来自于他的（　）。
A、单向性
B、算法复杂性
C、算法的保密性
D、离散性
参考答案：A

（22）对明文字母重新排列，并不隐藏他们的加密方法属于（　）。
A、代替密码
B、分组密码
C、置换密码
D、序列密码
参考答案：C

（23)驻留在多个网络设备上的程序在短时间内同时产生大量的请求信息冲击某个 Web 服务器，导致该服务器不堪重负，无法正常响应其它合法用户的请求，这属于 （ ） 。
A、网上冲浪
B、中间人攻击
C、DDoS 攻击
D、MAC 攻击

参考答案：C

（24）所谓网络安全漏洞是指（　）。
A.用户的误操作引起的系统故障
B.网络节点的系统软件或应用软件在逻辑设计上的缺陷
C.网络硬件性能下降产生的缺陷
D.网络协议运行中出现的错误
参考答案：B

（25）文件型病毒传染的对象主要是（　　）类文件。
A．.EXE 和.WPS
B．COM 和.EXE
C．.WPS
D．.DBF
参考答案：B

（26） DES 是一种 block（块）密文的加密算法，是把数据加密成多大的块？（　）
A、32 位
B、64 位
C、128 位
D、256 位
参考答案：B

（27） 以下哪项是数据库加密方法中的库外加密的缺点？（　）
A、即使访问一条数据也要对整个数据库解密
B、密钥管理比较复杂
C、加密之后不能完整的查询数据
D、密钥过于简单，容易被破解
参考答案：A

（28）在（ ）中，①代表的技术通过对网络数据的封包和加密传输，在公网上传输私有数据、达到私有网络的安全级别；②代表的技术把所有传输的数据进行加密，可以代替 telnet，可以为 ftp 提供一个安全的“通道”；③代表的协议让持有证书的 Internet 浏览器软件和 WWW 服务器之间构造安全通道传输数据，该协议运行在 TCP/IP 层之上，应用层之下。
A. ①SSH　②VPN　③SSL
B. ①VPN　②SSH　③SSL
C. ①VPN　②SSL　③SSH
D. ①SSL　②VPN　③SSH
参考答案：B

（29）修改已签订的合同文件，对原合同的什么属性造成了危害（　）。
A、完整性
B、不可否认性
C、可用性

D、机密性
参考答案：A

（30）PDR 模型中 Dt 是从入侵者开始发动入侵开始，系统能够检测到（　）所花费的时间。
A、系统异常
B、系统保护建立
C、入侵行为
D、灾难恢复启动
参考答案：C

（31） 不属于计算机病毒防治的策略的是（　）
A.确认您手头常备一张真正“干净”的引导盘
B.及时、可靠升级反病毒产品
C.新购置的计算机软件也要进行病毒检测
D.整理磁盘
参考答案：D

（32）下列哪一个说法是正确的？（　）
A、风险越大，越不需要保护
B、风险越小，越需要保护
C、风险越大，越需要保护
D、越是中等风险，越需要保护
参考答案：C

（33） 信息安全风险缺口是指（　）。
A、IT 的发展与安全投入，安全意识和安全手段的不平衡
B、信息化中，信息不足产生的漏洞
C、计算机网络运行，维护的漏洞
D、计算中心的火灾隐患
参考答案：A

（34）下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求？（　）
A、国家秘密和其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关规定
B、各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级
C、对是否属于国家和属于何种密级不明确的事项，可有各单位自行参考国家要求确定和定级，然后国家保密工作部门备案
D、对是否属于国家和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。
参考答案：C

（35） 一般证书采用哪个标准？（　）

A、ISO/IEC 15408
B、ISO/IEC 17799
C、BS 7799
D、X.509 V3
参考答案：D

（36）网络病毒防范的三个阶段主要是预防范阶段、病毒爆发阶段和哪个阶段？（　）
A、残余风险评估阶段
B、检查阶段
C、入侵检测系统监控阶段
D、网络异常流量临控阶段
参考答案：A

（37）要成功实施信息系统安全管理并进行维护，应首先对系统（ ）进行评估鉴定。
A.风险
B.资产
C.威胁
D.脆弱性

参考答案：D

（38）下面病毒中，属于蠕虫病毒的是　（　　。
A、Wom.Sasser 病毒
B、Trojan.QQPSW 病毒
C、Backdoor.IRCBot 病毒
D、Macro.Melissa 病毒
参考答案：A

（39）下列叙述中错误的是(　)。
A：数字签名可以保证信息在传输过程中的完整性
B：数字签名可以保证数据在传输过程中的安全性
C：数字签名可以对发送者的身份进行认证
D：数字签名可以防止交易中的抵赖法则
参考答案：B

（40）下面对于标识和鉴别的解释最准确的是：（　）
A.标识用于区别不同的用户，而鉴别用于验证用户身份的真实性
B.标识用于区别不同的用户，而鉴别用于赋予用户权限
C.标识用于保证用户信息的完整性，而鉴别用于验证用户身份的真实性
D.标识用于保证用户信息的完整性，而鉴别用于赋予用户权限
参考答案：A

（41）窃听是一种（　）攻击，攻击者（　）将自己的系统插入到发送站和接收站之间。截获是一种（　　）攻击，攻击者（　　）将自己的系统插入到发送站和接受站之间。

A.　被动,无须,主动,必须

B.　主动,必须,被动,无须

C.　主动,无须,被动,必须

D.　被动,必须,主动,无须

参考答案：A

（42）为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？（　）

A、人际关系技能

B、项目管理技能

C、技术技能

D、沟通技能

参考答案：D

（43） 攻击者截获并记录了从 A 到 B 的数据，然后又从早些时候所截获的数据中提取出信息重新发往 B 称为（　　）。

A.中间人攻击

B.口令猜测器和字典攻击

C.强力攻击

D.重放攻击

参考答案：D

（44）在 IPSec 中，（　）是两个通信实体经过协调建立起来的一种协定，觉得用来保护数据包安全的 IPSec 协议、密码算法、密钥等信息。

A、ESP

B、SPI

C、SA

D、SP

参考答案：C

关于 kerberos 和 PKI 两种认证协议的叙述中正确的是（45），在使用 kerberos 认证时，首先向密钥分发中心发送初始票据（46）来请求会话票据，以便获取服务器提供的服务。

（45）A．kerberos 和 PKI 都是对称密钥

B．kerberos 和 PKI 都是非对称密钥

C．kerberos 是对称密钥，而 PKI 是非对称密钥

D．kerberos 是非对称密钥，而 PKI 是对称密钥

（46）A．RSA

B．TGT

C．DES

D．LSA

参考答案：C、B

（47）入侵是指没有经过授权就非法获得系统的访问权限或相关授权的行为，其中攻击者利用默认密码进入系统内部属于（　）入侵方式
A、旁路控制
B、假冒
C、口令破译
D、合法用户的非授权访问
参考答案：C

（48） 对称加密体制中，不公开的信息是（ ）。
A、密钥
B、算法
C、密文空间
D、明文空间
参考答案：A

（49） 为了防止电子邮件中的恶意代码，应该由（ ）方式阅读电子邮件。
A、纯文本
B、网页
C、程序
D、会话
参考答案：A

（50）链路加密要求必须先对链路两端的加密设备进行（　）。
A、异步
B、重传
C、同步
D、备份
参考答案：C

（51） 在以下隧道协议中，属于三层隧道协议的是（　）。
A、L2F
B、PPTP
C、L2TP
D、IPSec
参考答案：D

（52）下面有关加密技术的叙述中，（ ）是错误的。
A、IDEA 是一种对称加密算法
B、公钥加密技术和单向陷门函数密不可分
C、IKE 是一种消息摘要算法
D、公钥加密的一个重要应用是数字签名

参考答案：C

（53）网络隔离技术的目标是确保把有害的攻击隔离，在保证可信网络内部信息部不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是　（ ）　。
A、多重安全网关
B、防火墙
C、VLAN 隔离
D、物理隔离
参考答案：D

（54）采用 CRC 进行差错校验，生成多项式为 G(X)=X4+X+1，信息码字为 10111，则计算出的 CRC 校验码是　（ ）　。
A、0000
B、0100
C、0010
D、1100
参考答案：D

（55）发生（ ）后，磁盘上的物理数据和日志文件被破坏，这是最严重的一种故障，恢复方法是重装数据库，然后重做已完成的事务。
A、系统故障
B、事故故障
C、介质故障
D、软件故障
参考答案：C

（56） 那类 TCP 扫描不带任何标志位？（ ）
A、SYN 扫描
B、ACK 扫描
C、FIN 扫描
D、NULL 扫描
参考答案：D

（57） 以下哪一种是入侵检测系统所通常采用的：（ ）
A、基于网络的入侵检测系统
B、基于 IP 的入侵检测系统
C、基于服务的入侵检测系统
D、基于域名的入侵检测系统
参考答案：A

（58） 对于信息安全发展历史描述正确的是：（ ）
A.信息安全的概念是随着计算机技术的广泛应用而诞生的
B.目前信息安全已经发展到计算机安全的阶段
C.目前信息安全不仅仅关注信息技术，人们意识到组织、管理、工程过程和人员同样是促进

系统安全性的重要因素
D.我们可以将信息安全的发展阶段概括为，由“计算机安全”到“通信安全”，再到“信息安全”，直至现在的“信息安全保障”
参考答案：C

（59）交换机转发以太网的数据基于：（ ）。
A、交换机端口号
B、MAC 地址
C、IP 地址
D、数据类别
参考答案：B

（60）WindowsNT 和 Windows2000 系统能设置为在若干次无效登录后锁定账号，此技术可以防止（ ）。
A、暴力攻击
B、木马病毒
C、缓存溢出攻击
D、IP 欺骗

参考答案：A

某网站向 CA 申请了数字证书。用户通过 （61） 来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过 （62） 进行加密和验证，该网站通过 （63） 进行解密和签名。
（61）A、CA 的签名
B、证书中的公钥
C、网站的私钥
D、用户的公钥
（62）A、CA 的签名
B、证书中的公钥
C、网站的私钥
D、用户的公钥
（63）A、CA 的签名
B、证书中的公钥
C、网站的私钥
D、用户的公钥
参考答案：A、B、C

（64）以下关于加密算法的叙述中，正确的是 （ ） 。
A、DES 算法采用 128 位的密钥进行加密
B、DES 算法采用两个不同的密钥进行加密
C、三重 DES 算法采用 3 个不同的密钥进行加密
D、三重 DES 算法采用 2 个不同的密钥进行加密

参考答案：D

（65） 病毒在感染计算机系统时，一般（ ）感染系统的。
A、病毒程序都会在屏幕上提示，待操作者确认（允许）后
B、是在操作者不觉察的情况下
C、病毒程序会要求操作者制定存储的磁盘和文件夹后
D、在操作者为病毒制定存储的文件名以后
参考答案：B

（66）下列措施中，（ ）不是减少病毒的传染
和造成的损失的好办法。
A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态
B、外来的文件要经过病毒检测才能使用，不要使用盗版软件
C、不与外界进行任何交流，所有软件都自行开发
D、定期用抗病毒软件对系统进行查毒、杀毒
参考答案：C

（67）下面关于漏洞扫描系统的叙述，错误的是（ ）。
A、漏洞扫描系统是一种自动检测目标主机安全弱点的程序
B、黑客利用漏洞扫描系统可以发现目标主机的安全漏洞
C、漏洞扫描系统可以用于发现网络入侵者
D、漏洞扫描系统的实现依赖于系统漏洞库的完善
参考答案：C

（68）CA 在数字签名当中扮演的主要角色是（ ）。
A、签名者
B、仲裁
C、验证者
D、攻击者
参考答案：B

（69）目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（ ）
A、GB/T 18336-2001 信息技术安全性评估准则
B、GB 17859-1999 计算机信息系统安全保护等级划分准则
C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构
D、GA/T 391-2002 计算机信息系统安全等级保护管理要求
参考答案：B

（70） 非对称密钥的密码技术具有很多优点，其中不包括：（ ）。
A、可提供数字签名、零知识证明等额外服务
B、加密/解密速度快，不需占用较多资源
C、通信双方事先不需要通过保密信道交换密钥
D、密钥持有量大大减少

参考答案：B

Much of the theoretical work in cryptography concerns cryptographic primitives algorithms with basic cryptographic properties - and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. Complex functionality in an application must be built in using combinations of these algorithms and assorted protocols. Such combinations are called（ 71 ） and it is they which users actually encounter. Examples include PGP and its variants, ssh, SSL/TLS, all PKIs, （ 72 ）, etc For example, a （ 73 ） is function intended to be easy to compute but hard to invert.

But note that, in a very general sense, for any cryptographic application to be secure (if based on computational feasibility assumptions) one-way functions must exist. However, if one-way functions exist, this implies that （ 74 ）≠NP. Since the P versus NP problem is currently unsolved, it is not known if one-way functions really do exist. For instance, if one way functions exist, then secure pseudorandom generators and secure pseudorandom functions exist.

Other （ 75 ）include the encryption algorithms themselves, one-way permutations, trapdoor permutations, etc.

（71）A. Password base B. cryptosystems C. Principles of cryptography D. Equipment system

（72）A. Certification B. Digest Summary C. digital signatures D. Identification

（73）A. Hash function B. one-way function C. Bidirectional function D. Power function

（74）A. NPC B. N C. NP D. P

（75）A. cryptographic primitives B. Principles of cryptography

C. cryptosystems D. Password base

参考答案：B C B D A

信息安全工程师上午卷 03

（1）在信息系统安全技术体系中，环境安全只要指中心机房的安全保护。以下不属于该体系环境安全内容的是（ ）。

A．设备防盗器

B．接地和防雷击

C．机房控制

D．防电磁泄漏

参考答案：A

（2）根据统计显示，80%的网络攻击源于内部网络，因此，必须加强对内部网络的安全控制和防范。下面的措施中，无助于提高同一局域网内安全性的措施是( )。

A.使用防病毒软件

B.使用日志审计系统
C.使用入侵检测系统
D.使用防火墙防止内部攻击
参考答案：D

（3）关于 RSA 算法的说法不正确的是（ ） 。
A、RSA 算法是一种对称加密算法
B、RSA 算法的运算速度比 DES 慢
C、RSA 算法可用于某种数字签名方案
D、RSA 的安全性主要基于素因子分解的难度
参考答案：A

公钥体系中，私钥用于 （4） ，公钥用于 （5） 。
（4）A、解密和签名
B、加密和签名
C、解密和认证
D、加密和认证
（5）A、解密和签名
B、加密和签名
C、解密和认证
D、加密和认证
参考答案：A、D

（6）下列算法中，明文分组最长的是（ ）。
A、3DES
B、DES
C、IDEA
D、AES
参考答案：D

（7） 著名的橘皮书指的是（ ）。
A、可信计算机系统评估标准(TCSEC)
B、信息安全技术评估标准（ITSEC）
C、美国联邦标准（FC）
D、通用准则（CC）
参考答案：A

（8）关于 WEB 应用软件系统安全，说法正确的是（ ）？
A、Web 应用软件的安全性仅仅与 WEB 应用软件本身的开发有关
B、系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴
C、黑客的攻击主要是利用黑客本身发现的新漏洞
D、以任何违反安全规定的方式使用系统都属于入侵
参考答案：D

（9）目前在网络上流行的“熊猫烧香”病毒属于 （ ） 类型的病毒。
A、目录
B、引导区
C、蠕虫
D、DOS
参考答案：C

杀毒软件报告发现病毒 Macro.Melissa，由该病毒名称可以推断出病毒类型是 （10） ，这类病毒主要感染目标是 （11） 。
（10）A、文件型
B、引导型
C、目录型
D、宏病毒
（11）A、EXE 或 COM 可执行文件
B、WORD 或 EXCEL 文件
C、DLL 系统文件
D、磁盘引导区
参考答案：D、B

（12） 在入侵检测系统中，事件分析器接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其常用的三种分析方法中不包括（ ）。
A. 模式匹配
B. 密文分析
C. 数据完整性分析
D. 统计分析
参考答案：B

（13） 在我国的 GB/T 18794.7-2003/ISO/IEC10181-7:1996 中将安全审计的整个执行流程分为多个阶段，并且加以描述。其中错误的为（ ）。
A、检测阶段：检测安全相关事件
B、辨别阶段：决定是否记录该事件，或是否需要产生报警
C、报警处理阶段：可能发出一个安全审计报警或安全审计消息
D、归档阶段：将分布式安全审计跟踪记录汇集成单个安全审计跟踪记录。
参考答案：D

（14）对于现存的安全策略有两个方面, 它们都是建立在（ ）这一概念之上。
A、策略制定
B、授权行为
C、安全要素
D、安全标记
参考答案：B

（15） 灾难恢复与数据恢复的关系是（ ）。
A、两者意义相同

B、前者包含后者
C、后者包含前者
D、两者没有关系
参考答案：B

（16）组成 IPSEC 的主要安全协议不包括以下哪一项：（　）
A、 ESP
B、 DSS
C、 IKE
D、 AH
参考答案：B

（17） 信息系统和网络系统安全的基本策略不包括（　）
A、保护
B、检测
C、嗅探
D、响应
参考答案：C
保护、检测、响应（PDR) 策略是确保信息系统和网络系统安全的基本策略。

（18）DNS 系统对于网络的正常运行是至关重要的，以下措施中不能增强 DNS 安全的是（ ）。
A、使用防火墙控制对 DNS 的访问
B、避免 DNS 的 HINFO 记录被窃取
C、更改 DNS 的端口号
D、限制区域传输
参考答案：C

下图所示 PKI 系统结构中，负责生成和签署数字证书的是（19），负责验证用户身份的是（20）。
（19）A. 证书机构 CA　　B. 注册机构 RA
　　C. 证书发布系统　　D. PKI 策略
（20）A. 证书机构 CA　　B. 注册机构 RA
　　C. 证书发布系统　　D. PKI 策略
参考答案：A、B

（21） 以下属于网络空间安全学科所特有的理论基础的是（　）
A、信息理论
B、计算理论
C、数学
D、密码学理论
参考答案：D
数学、信息理论(信息论、系统论、控制论)、计算理论(可计算性理论、计算复杂性理论)是网络空间安全学科的理论基础，而博弈论、访问控制理论和密码学理论是网络空间安全学科所特有的理论基础。

（22）数字签名要预先使用单向 Hash 函数进行处理的原因是（　）。
A、多一道加密工序使密文更难破译
B、 提高密文的计算速度
C、缩小签名密文的长度，加快数字签名和验证签名的运算速度
D、保证密文能正确还原成明文
参考答案：C

（23）计算机系统应选用（　）电缆。
A、铜芯
B、铅芯
C、铁芯
D、没有要求
参考答案：A

（24）计算机信息系统防护，简单概括起来就是：均压、分流、屏蔽和良好接地。所以防雷保安器必须有合理的（　）。
A、屏蔽配置
B、接地配置
C、分流配置
D、均压配置
参考答案：B

（25）Code Red 爆发于 2001 年 7 月，利用微软的 IIS 漏洞在 Web 服务器之间传播。针对这一漏洞，微软早在 2001 年三月就发布了相关的补丁。如果今天服务器仍然感染 Code Red，那么属于哪个阶段的问题？（　）
A、系统管理员维护阶段的失误
B、微软公司软件的设计阶段的失误
C、最终用户使用阶段的失误
D、微软公司软件的实现阶段的失误
参考答案：A

（26）以下有关防火墙的说法中，错误的是（ ）。
A、防火墙可以提供对系统的访问控制
B、防火墙可以实现对企业内部网的集中安全管理
C、防火墙可以隐藏企业网的内部 IP 地址
D、防火墙可以防止病毒感染程序（或文件）的传播
参考答案：D

（27）（ ） 不属于 PKI　CA（认证中心）的功能。
A、接受并验证最终用户数字证书的申请
B、向申请者颁发或拒绝颁发数字证书
C、产生和发布证书废止列表（CRL），验证证书状态
D、业务受理点 LRA 的全面管理

参考答案：D

（28）关于网络安全，以下说法正确的是 （ ） 。
A、使用无线传输可以防御网络监听
B、木马是一种蠕虫病毒
C、使用防火墙可以有效地防御病毒
D、冲击波病毒利用 Windows 的 RPC 漏洞进行传播
参考答案：D

（29）漏洞扫描器有哪几类？（ ）
A、基于协议端口的漏洞扫描器和基于操作系统指纹的扫描器
B、基于网络的漏洞扫描器和基于主机的漏洞扫描器
C、基于漏洞库的扫描器和基于插件技术的扫描器
D、基于协议分析的漏洞扫描器和基于网络行为的漏洞扫描器
参考答案：B

（30）下列算法中，出现最早的公钥算法是（ ）。
A、DES
B、RSA
C、Elgamal
D、ECC
参考答案：B

（31） 不属于数据库加密方式的是（ ）。
A、库外加密
B、库内加密
C、硬件/软件加密
D、专用加密中间件
参考答案：D

（32）数字签名技术是公开密钥算法的一个典型的应用，在发送端，它是采用（ ）对要发送的的信息进行数字签名。
A．发送者的公钥
B．接收者的公钥
C．发送者的私钥
D．接收者的私钥
参考答案：C

（33） 不管网络工程规模如何，都存在一个可扩展的总体安全体系框架。（ ）是整个安全架构的基础。
A、以安全技术为核心的技术措施
B、安全运维服务体系
C、数据容灾与恢复体系
D、安全管理体系

参考答案：D

（34）在审核信息系统设计时，重点审查系统的（　）设计，防止对信息的篡改，越权获取和蓄意破坏以及预防自然灾害。
A、容错
B、结构化
C、可靠性
D、安全性
参考答案：D

（35）为了防止物理上取走数据库而采取的加强数据库安全的方法是（　）。
A、数据加密
B、数据库加密
C、口令保护
D、数据审计
参考答案：B

（36）漏洞扫描的主要功能是什么？（　）
A、扫描目标主机的服务端口
B、扫描目标主机的操作系统
C、扫描目标主机的漏洞
D、扫描目标主机的 IP 地址
参考答案：C

（37）使用 TCP 79 端口的服务是：（　）。
A、telnet
B、SSH
C、Web
D、Finger
参考答案：D

（38）（　）指对主体访问和使用客体的情况进行记录和审查，以保证安全规则被正确执行，并帮助分析安全事故产生的原因。
A.安全授权
B.安全管理
C.安全服务
D.安全审计
参考答案：D

（39）身份认证是安全服务中的重要一环，以下关于身份认证叙述不正确的是（　）。
A. 身份认证是授权控制的基础
B. 身份认证一般不用提供双向的认证
C. 目前一般采用基于对称密钥加密或公开密钥加密的方法
D. 数字签名机制是实现身份认证的重要机制

参考答案：B

（40）(　)的主要任务是指对数据库系统应用程序或用户使用资源的情况进行记录和审计，用以保证数据的安全。
A、数据库备份
B、数据库恢复
C、数据库审计
D、数据库转储
参考答案：C

（41）偷看私人电子邮件，攻击了电子邮件的什么属性（　）。
A、完整性
B、不可否认性
C、可用性
D、机密性
参考答案：D

（42） 在本机的特定存储介质上进行的备份称为（　）。
A、异地备份
B、本地备份
C、可更新备份
D、动态备份
参考答案：B

（43） 以下哪一项不是跨站脚本攻击？（　）
A.给网站挂马
B.盗取 COOKIE
C.伪造页面信息
D.暴力破解密码
参考答案：D

（44）不属于常见的危险密码是（　）
A、跟用户名相同的密码
B、使用生日作为密码
C、只有 4 位数的密码
D、10 位的综合型密码
参考答案：D

（45） 根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？（　）
A、威胁、脆弱性
B、系统价值、风险
C、信息安全、系统服务安全
D、受侵害的客体、对客体造成侵害的程度业务

参考答案：D

（46）对 SQL 数据库来说，以下哪个用户输入符号对系统的安全威胁最大， 需要在数据输入时进行数据过滤？（ ）
A、--
B、-
C、-=
D、-+
参考答案：B

（47）属于被动攻击的恶意网络行为是（ ）。
A、缓冲区溢出
B、网络监听
C、端口扫描
D、IP 欺骗
参考答案：B

（48）在 IPSec 中，IKE 提供（ ）方法供两台计算机建立。
A、解释域
B、安全关联
C、安全关系
D、选择关系
参考答案：B

（49） 除了在代码设计开发阶段预防 SQL 注入外，对数据库进行加固也能够把攻击者所能造成的损失控制在一定范围内，下列哪项不是数据库加固范围？（ ）
A、禁止将任何高权限账号（例如 sa,dba 等等）用于应用程序数据库访问。更安全的方法是单独为应用创建有限访问账户
B、拒绝用户访问敏感的系统存储过程
C、禁止用户访问的数据库表
D、限制用户所能够访问的数据库表
参考答案：C

（50）审计管理指：（ ）。
A．保证数据接收方收到的信息与发送方发送的信息完全一致
B．防止因数据被截获而造成的泄密
C．对用户和程序使用资源的情况进行记录和审查
D．保证信息使用者都可有得到相应授权的全部服务
参考答案：C

（51）以下不属于物理访问控制要点的是 （ ） 。
A、硬件设施在合理范围内是否能防止强制入侵
B、计算机设备的钥匙是否具有良好的控制
C、计算机设备电源供应是否能适当控制在合理的规格范围内

D、计算机设备在搬动时是否需要设备授权通行的证明
参考答案：C

（52）域名服务系统（DNS）的功能是（　）。
A、完成域名和 IP 地址之间的转换
B、完成域名和网卡地址之间的转换
C、完成主机名和 IP 地址之间的转换
D、完成域名和电子邮件地址之间的转换
参考答案：A

（53）PKI 无法实现（　）。
A、身份认证
B、数据的完整性
C、数据的机密性
D、权限分配
参考答案：D

（54） RSA 算法建立的理论基础是（　）。
A、DES
B、替代想组合
C、大数分解和素数检测
D、哈希函数
参考答案：C

（55）某商业银行决定开发网络安全审计系统，希望该系统是在应用系统内部嵌入一个与应用服务同步运行专用的审计服务应用进程，用于全程跟踪应用服务进程的运行。该商业银行的安全审计系统最适合采用（　）。
A．基于网络旁路监控的审计
B．基于应用系统独立程序的审计
C．基于网络安全入侵检测的预警系统
D．基于应用系统代理的审计

参考答案：B

（56）计算机感染特洛伊木马后的典型现象是 （ ） 。
A、程序异常退出
B、有未知程序试图建立网络连接
C、邮箱被垃圾邮件填满
D、Windows 系统黑屏
参考答案：B

（57） 异常入侵检测以（　）作为比较的参考基准。
A、异常的行为特征轮廓
B、正常的行为特征轮廓

C、日志记录
D、审计记录
参考答案：B

（58）下面哪个功能属于操作系统中的日志记录功能（　）
A、控制用户的作业排序和运行
B、以合理的方式处理错误事件，而不至于影响其他程序的正常运行
C、保护系统程序和作业，禁止不合要求的对程序和数据的访问
D、对计算机用户访问系统和资源的情况进行记录
参考答案：D

（59） 一般来说，通过 WEB 运行 http 服务的子进程时，我们会选择（　）的用户权限方式，这样可以保证系统的安全。
A、root
B、httpd
C、guest
D、nobody
参考答案：D

（60）通过收集和分析计算机系统或网络的关键节点信息，以发现网络或系统中是否有违反安全策略的行为和被攻击的迹象的技术被称为（　）
A、系统检测
B、系统分析
C、系统审计
D、入侵检测
参考答案：D

（61） “在遇到应急事件后所采取的措施和行动”被称为（　）。
A、灾难恢复
B、数据恢复
C、应急响应
D、计算机取证
参考答案：C

（62）向有限的空间输入超长的字符串是哪一种攻击手段？（　）
A、缓冲区溢出
B、网络监听
C、拒绝服务
D、IP 欺骗
参考答案：A

（63） （　）是一个对称 DES 加密系统，它使用一个集中式的专钥密码功能，系统的核心是 KDC。
A.　TACACS

B. RADIUS
C. Kerberos
D. PKI
参考答案：C

（64）计算机网络系统中，入侵检测一般分为3个步骤，依次为（ ）。
①数据分析 ②响应 ③信息收集
A. ③①②
B. ②③①
C. ③②①
D. ②①③
参考答案：A

（65） 有关L2TP（Layer 2 Tunneling Protocol）协议说法有误的是（ ）。
A、L2TP是由PPTV协议和Cisco公司的L2F组合而成
B、L2TP可用于基于Internet的远程拨号访问
C、为PPP协议的客户建立拨号连接的VPN连接
D、L2TP只能通过TCP/IP连接
参考答案：D

（66） 黑客进行攻击的最后一个步骤是：（ ）
A.侦查与信息收集
B.漏洞分析与目标选定
C.获取系统权限
D.打扫战场、清除证据
参考答案：D

（67）银河大学是一所拥有6万多名师生的综合性大学。规划师对于该大学数据中心网络防火墙的访问控制问题，最可能采取的方案是( )。
A.基于角色的访问控制(RBAC)方案
B.自主型访问控制(DAC)方案
C.基于任务的访问控制(TBAC)方案
D.强制型访问控制(MAC)方案
参考答案：A

（68）以下不是安全审计系统作用的是（ ）。
A、记录和跟踪各种系统状态的变化
B、对审计日志进行智能分析
C、实现对各种安全事故的定位
D、对攻击者的犯罪行为进行处罚
参考答案：D

（69）在信息系统的用户管理中，( )身份认证方式是一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的

矛盾。
A.用户名/密码
B.动态密码
C.IC卡
D.USB Key
参考答案：D

（70） 物理安全技术包括机房安全和（ ）。
A、数据安全
B、系统安全
C、通信安全
D、设施安全
参考答案：D

Securing network infrastructure is like（ 71 ）possible en points of attacks on a country by deploying appropriate defense. Computer security is more like providing means to（ 72 ）a single PC against outside intrusion. The former is better and practical to protect the civilians from getting exposed to the attacks. （ 73 ）empt to secure the access to individual computers…the network itself-thereby protecting the computers and other shared resources such as printers, network-attached storage connected by the network. Attacks could be stopped at their en points before they spread. As opposed to this, in computer security the measures taken are focused on securing individual computer hosts. A computer host whose security is compromised is likely to infect other hosts connected to a potentially（ 74 ）. A computer host's security is vulnerable to users with higher （ 75 ）to those hosts.
（71）A. assuring B. guarantee C. securing D. proving
（72）A. ensure B. keep C. support D. protect
（73）A. The attack means B. The attack target C.The cyber securityD.The preventive measures
（74）A. Secure network B. unsecured network C. Botnet D. Vulnerability Network
（75）A. access mechanism B. Secure access C. access privileges D. access means
参考答案：C D D B C

信息安全工程师上午卷 04

（1）我国强制性国家标准《计算机信息安全保护等级划分准则》将计算机信息系统分为5个安全保护等级，其中适用于地方各级国家机关、金融机构、邮电通信、能源与水源供给部门的信息系统适用（ ）。
A. 安全标记保护级 B. 结构化保护级 C.访问验证保护级 D.系统审计保护级
参考答案：A

（2)信息系统安全风险评估是通过数字化的资产评估准则完成的,它通常会覆盖人员安全、人员信息、公共秩序等方面的各个要素，以下不会被覆盖的要素是（　）
A、立法及规章未确定的义务
B、金融损失或对业务活动的干扰
C、信誉的损失
D、商业及经济的利益
参考答案：A

（3）下列哪个不是常见的网络应用服务？（　）
A、WEB
B、MAIL
C、DNS
D、ARP
参考答案：D

（4） 主要用于加密机制的协议是（　）
A、HTTP
B、FTP
C、TELNET
D、SSL
参考答案：D

（5） 在网络安全风险评估中，将风险的资产、威胁、脆弱性等要素的属性进行量化赋值，然后选用相乘法、矩阵法等计算方法进行风险值计算。这种计算方法被称作（）：
A、定性计算
B、定量计算
C、定性计算与定量计算相结合
D、都不是
参考答案：A

（6） 以下哪一项不是流氓软件的特征？（　）
A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装
B、通常添加驱动保护使用户难以卸载
C、通常会启动无用的程序浪费计算机的资源
D、通常会显示下流的言论
参考答案：D

（7）在 PKI 体系中_____负责管理 PKI 结构下的所有用户(包括各种应用程序)的证书，把 用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份.
A、RADIUS server
B、ISP
C、CA
D、IE
参考答案：C

（8）下列哪一条与操作系统安全配置的原则不符合?（　）
A、关闭没必要的服务
B、不安装多余的组件
C、安装最新的补丁程序
D、开放更多的服务
参考答案：D

（9）目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（　）?
A、数据库系统庞大会提供管理成本
B、数据库系统庞大会降低管理效率
C、数据的集中会降低风险的可控性
D、数据的集中会造成风险的集中
参考答案：D

（10）网络攻击的有效载体是什么？（　　）
A．黑客
B．网络
C．病毒
D．蠕虫
参考答案：C

（11）关于使用电脑有以下行为规范：（　　）
①及时安装系统补丁
②及时修改登录密码
③使用建行分配的 IP 地址
④保证杀毒软件病毒库为最新
在脱离建行网络环境下使用电脑时，应该注意什么？
A、①②
B、①④
C、②③
D、①②④
参考答案：D

（12）下列行为不属于网络攻击的是 （ ） 。
A、连续不停 Ping 某台主机
B、发送带病毒和木马的电子邮件
C、向多个邮箱群发一封电子邮件
D、暴力破解服务器密码

参考答案：C

（13） “冲击波”病毒运行时会将自身复制到 Windows 目录下，并命名为（ ）
A、Gsrss.exe
B、msbast.exe
C、msblast.exe
D、lsass.exe
参考答案：C

（14）一个密码系统，通常简称为密码体制。可由五元组（M,C,K,E,D）构成密码体制模型，以下有关叙述中，（ ）是不正确的。
A. M 代表明文空间；C 代表密文空间；K 代表密钥空间；E 代表加密算法；D 代表解密算法
B. 密钥空间是全体密钥的集合，每一个密钥 K 均由加密密钥 Ke 和解密密钥 Kd 组成，即有 K=
C. 加密算法是一簇由 M 到 C 的加密变换，即有 C=（M, Kd）
D. 解密算法是一簇由 C 到 M 的加密变换，即有 M=（C, Kd）
参考答案：C

（15）下面有关安全审计的说法错误的是（ ）
A、安全审计需要用到数据挖掘和数据仓库技术
B、安全审计产品指包括主机类、网络类及数据库类
C、安全审计的作用包括帮助分析案情事故发生的原因
D、安全审计是主体对客体进行访问和使用情况进行记录和审查
参考答案：B

（16）根据《信息安全等级保护管理办法》中的规定，信息系统的安全保护等级应当根据信息系统的国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危险程度等因素确定。其中安全标记保护级处于（ ）
A、第二级
B、第三级
C、第四级
D、第五级
参考答案：B

（17）下列哪些属于 WEB 脚本程序编写不当造成的（ ）？
A、IIS5.0 Webdav Ntdll.dll 远程缓冲区一处漏洞
B、apache 可以通过../../../../../../../etc/passwd 方位系统文件
C、登陆页面可以用 password=’a’or’a’=’a’绕过
D、数据库中的口令信息明文存放
参考答案：C

（18） AES 密钥长度不能是（ ）。

A、128 位
B、192 位
C、256 位
D、512 位
参考答案：D

（19）信息安全管理体系是指（ ）。
A. 网络维护人员的组织体系
B. 信息系统的安全设施体系
C. 防火墙等设备、设施构建的安全体系
D. 组织建立信息安全方针和目标并实现这些目标的体系

参考答案：D

（20）网吧管理员小李发现局域网中有若干台电脑有感染病毒的迹象，这时应首先（ ），以避免病毒的进一步扩散。
A．关闭服务器
B．启动反病毒软件查杀
C．断开有嫌疑计算机的物理网络连接
D．关闭网络交换机
参考答案：C

（21）PH 软件开发公司承接了 ZF 企业基于因特网的 B2C 业务系统的研发任务。ZF 企业提出的业务系统安全性要求之一是防止授权侵犯和保留用户痕迹。针对这一要求，PH 公司架构师给出的解决方案最可能是（ ）。
A.完整性(Integrity)框架方案
B.访问控制(Access Control)框架方案
C.身份鉴别(Authentication)框架方案
D.抗抵赖(Non-repudiation)框架方案
参考答案：D

（22）网络空间安全学科的方法论与数学或计算机科学等学科的方法论既有联系又有区别。其内容不包括（ ）
A．理论分析
B．数理分析
C．实验验证
D．技术实现
参考答案：B

网络空间安全学科的方法论与数学或计算机科学等学科的方法论既有联系又有区别。具体概括为理论分析、逆向分析、实验验证、技术实现四个核心内容。这四者既可以独立运用，也可以相互结合，指导解决网络空间安全问题，推动网络空间安全学科发展。在运用网络空间安全的方法论分析和解决网络空间安全问题时，特别强调底层性和系统性。即，根据网络空间安全学科方法论的指导，从信息系统的软硬件底层和系统角度来分析信息安全问题，从

信息系统的软硬件底层和系统层综合采取措施来解决信息安全问题。

（23）计算机病毒主要造成（　）。
A、磁盘损坏
B、计算机用户的伤害
C、CPU 的损坏
D、程序和数据的破坏
参考答案：D

（24） 信息安全风险应该是以下哪些因素的函数？（　）
A、信息资产的价值、面临的威胁以及自身存在的脆弱性等
B、病毒、黑客、漏洞等
C、保密信息如国家密码、商业秘密等
D、网络、系统、应用的复杂的程度
参考答案：A

（25）以下哪个不属于信息安全的三要素之一？（　）
A、机密性
B、完整性
C、抗抵赖性
D、可用性
参考答案：C

（26） 应用网关防火墙的逻辑位置处在 OSI 中的哪一层？（　）
A、传输层
B、链路层
C、应用层
D、物理层
参考答案：C

公钥体系中，私钥用于　（27）　，公钥用于　（28）　。
（27）A、解密和签名
　　B、加密和签名
　　C、解密和认证
　　D、加密和认证
（28）A、解密和签名
　　B、加密和签名
　　C、解密和认证
　　D、加密和认证
参考答案：A、D

（29）下列攻击方式中，（　）不是利用 TCP/IP 漏洞发起的攻击。
A．SQL 注入攻击
B．Land 攻击

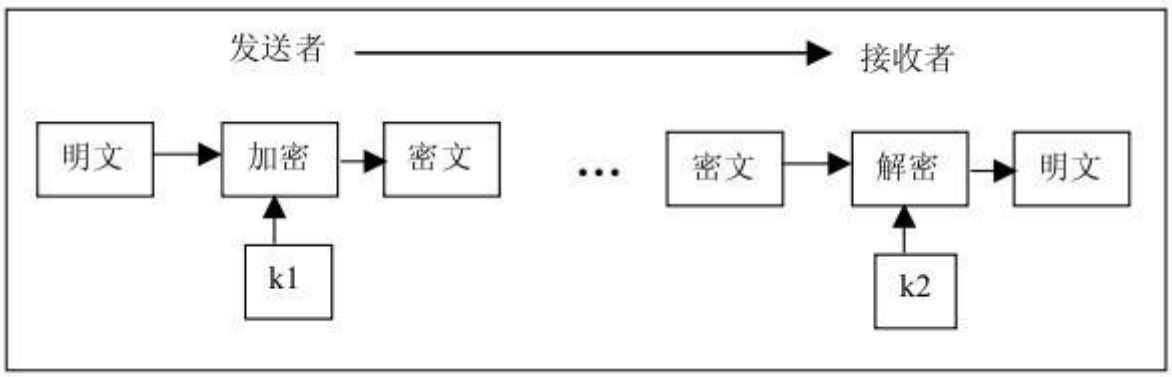
C. Ping of Death
D. Teardrop 攻击
参考答案：A

（30）传统的安全方案要取得成功依赖于系统正确的设置和完善的（　）。
A、防御手段
B、安全体系
C、安全标准
D、信息保护
参考答案：A

（31）下列哪种方法不能有效的防范 SQL 进入攻击（　）？
A、对来自客户端的输入进行完备的输入检查
B、把 SQL 语句替换为存储过程、预编译语句或者使用 ADO 命令对象
C、使用 SiteKey 技术
D、关掉数据库服务器或者不使用数据库
参考答案：C

（32）数字签名可以解决（　）。
A、数据被泄露
B、数据被篡改
C、未经授权擅自访问
D、冒名发送数据或发送后抵赖
参考答案：D

（33）下图是发送者利用不对称加密算法向接收者传送信息的过程，图中 k1 是（ ）。



A. 接收者的公钥
B. 接收者的私钥
C. 发送者的公钥
D. 发送者的私钥

参考答案：A

（34）访问控制是为了限制访问主体对访问客体的访问权限，从而使计算机系统在合法范围内使用的安全措施，以下关于访问控制的叙述中，（　）是不正确的
A、访问控制包括 2 个重要的过程：鉴别和授权
B、访问控制机制分为 2 种：强制访问控制(MAC)和自主访问控制（DAC）
C、RBAC 基于角色的访问控制对比 DAC 的先进之处在于用户可以自主的将访问的权限授给其它用户
D、RBAC 不是基于多级安全需求的，因为基于 RBAC 的系统中主要关心的是保护信息的完整性，即”谁可以对什么信息执行何种动作”
参考答案：C

（35） 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（　）不属于信息运行安全技术的范畴。
A、风险分析
B、审计跟踪技术
C、应急技术
D、防火墙技术
参考答案：B

（36） 以下关于宏病毒说法正确的是：（　）
A.宏病毒主要感染可执行文件
B.宏病毒仅向办公自动化程序编制的文档进行传染
C.宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区
D.CIH 病毒属于宏病毒
参考答案：B

（37） 网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（　）
A、密码加密后，不会被窃听
B、Cookie 字段可以被窃听
C、报文和帧可以窃听
D、高级窃听者还可以进行 ARPSpoof，中间人攻击
参考答案：A

（38)在构建信息安全管理体系中,应建立起一套动态闭环的管理流程,这套流程指的是(　)。
A．评估—响应—防护—评估
B．检测—分析—防护—检测
C．评估—防护—响应—评估
D．检测—评估—防护—检测

参考答案：A

（39） 甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息可用 （ ）验证该消息数字签名的真伪。
A. 甲的公钥
B. 甲的私钥
C. 乙的公钥
D. 乙的私钥
参考答案：A

（40)网络隔离技术的目标是确保把有害的攻击隔离,在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（ ）。
A、多重安全网关
B、防火墙
C、Vlan 隔离
D、物理隔离
参考答案：D

（41） 电子邮件的机密性与真实性是通过下列哪一项实现的？（ ）
A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密
B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密
C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密
D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密
参考答案：A

（42）信息安全策略的设计与实施步骤是（ ）
A.定义活动目录角色、确定组策略管理安全性、身份验证、访问控制和管理委派
B.确定标准性、规范性、可控性、整体性、最小影响、保密性原则，确定公钥基本结构
C.确定安全需求、制订可实现的安全目标、制订安全规划、制订系统的日常维护计划
D.确定安全需求、确定安全需求的范围、制订安全规划、制订系统的日常维护计划
参考答案：C

（43）关于 RSA 算法的叙述不正确的是（ ） 。
A. RSA 算法是一种对称加密算法
B. RSA 算法的运算速度比 DES 慢
C. RSA 算法可用于某种数字签名方案
D. RSA 的安全性主要基于素因子分解的难度
参考答案：A

（44）《计算机信息系统安全保护等级划分准则》规定了计算机系统安全保护能力的 5 个等级。其中，按照（ ）的顺序从左到右安全能力逐渐增强
A、系统审计保护级、结构化保护级、安全标记保护级
B、用户自主保护级、访问验证保护级、安全标记保护级
C、访问验证保护级、系统审计保护级、安全标记保护级
D、用户自主保护级、系统审计保护级、安全标记保护级
参考答案：D

（45）下面哪一个情景属于授权（Authorization）（　）
A、用户依照系统提示输入用户名和口令
B、用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改
C、用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容
D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中
参考答案：B

（46）信息安全的级别划分有不同的维度，以下级别划分正确的是（ ）。
A.系统运行安全和保密有 5 个层次，包括设备级安全、系统级安全、资源访问安全、功能性安全和数据安全
B.机房分为 4 个级别：A 级、B 级、C 级、D 级
C.根据系统处理数据划分系统保密等级为绝密、机密和秘密
D.根据系统处理数据的重要性，系统可靠性分 A 级和 B 级
参考答案：C

（47）利用报文摘要算法生成报文摘要的目的是（ ）。
A．验证通信对方的身份，防止假冒
B．对传输数据进行加密，防止数据被窃听
C．防止发送方否认发送过的数据
D．防止发送的报文被篡改
参考答案：D

（48）对于提供网络服务的内部网络，通常选择下列哪种防火墙对服务效率影响最大（　）。
A、包过滤防火墙
B、双宿主机防火墙
C、屏蔽主机防火墙
D、屏蔽子网防火墙
参考答案：B

（49） 基于网络的入侵检测系统利用（　）作为数据源。
A、审计记录
B、日志记录
C、网络数据包
D、加密数据
参考答案：C

（50）攻击者通过搭线或在电磁波辐射范围内安装截收装置等方式获得机密信息，或通过对信息流量和流向、通信频率和长度等参数的分析推导出有用信息的威胁称为（ ）
A、破坏
B、抵赖

C、截取
D、窃取
参考答案：C

（51）计算机病毒为了隐蔽起见,首先依靠它的（　）实现自身与合法的系统程序连接在一起。
A、系统调用部分
B、启动部分
C、破坏部分
D、传染部分
参考答案：B

（52） 基于网络的入侵检测系统的输入信息源是（　）。
A、系统的审计日志
B、系统的行为数据
C、应用程序的事务日志文件
D、网络中的数据包
参考答案：D

（53） IDS 可以利用的信息来源不包括（　）。
A、逻辑形式的入侵信息
B、网络和系统日志文件
C、目录和文件中不期望的改变
D、物理形式的入侵信息
参考答案：A

（54）安全电子邮件协议 PGP 不支持（　）。
A、确认发送者的身份
B、确认电子邮件未被修改
C、防止非授权者阅读电子邮件
D、压缩电子邮件大小
参考答案：D

（55）防火墙的工作层次是决定防火墙效率及安全的主要因素，下面的叙述中正确的是（　）。
A. 防火墙工作层次越低，则工作效率越高，同时安全性越高
B. 防火墙工作层次越低，则工作效率越低，同时安全性越低
C. 防火墙工作层次越高，则工作效率越高，同时安全性越低
D. 防火墙工作层次越高，则工作效率越低，同时安全性越高
参考答案：D

（56）《国家保密法》对违法人员的量刑标准是（　）。
A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑
B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，

处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑
C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑
D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑
参考答案：A

（57）某单位允许其内部网络中的用户访问 Internet。由于业务发展的需要，现要求在政务网与单位内部网络之间进行数据安全交换。适合选用的隔离技术是（　）。
A.防火墙
B.多重安全网关
C.网闸
D.VPN 隔离
参考答案：C

（58）采用 Kerberos 系统进行认证时，可以在报文中加入（ ）来防止重放攻击。
A、会话密钥
B、时间戳
C、用户 ID
D、私有密钥
参考答案：B

（59）在访问控制中，对网络资源的访问是基于什么的？（ ）
A、用户
B、权限
C、访问对象
D、工作组
参考答案：B

（60） 身份认证的主要目标包括：确保交易者是交易者本人、避免与超过权限的交易者进行交易和（　）。
A、可信性
B、访问控制
C、完整性
D、保密性
参考答案：B

（61） 目前最安全的身份认证机制是（　）。
A、一次口令机制
B、双因素法
C、基于智能卡的用户身价认证
D、身价认证的单因素法
参考答案：A

（62） 以下哪种方法是防止便携式计算机机密信息泄露的最有效的方法？（ ）
A、用所有者的公钥对硬盘进行加密处理
B、激活引导口令（硬件设置口令）
C、利用生物识别设备
D、利用双因子识别技术将登录信息写入记事本
参考答案：A

（63）2005 年 12 月，ISO 正式发布了①作为 IT 服务管理的国际标准；2007 年 10 月，ITU 接纳②为 3G 标准；2005 年 10 月，ISO 正式发布了③作为信息安全管理的国际标准。①、②和③分别是（ ）。
A.①ISO27000 ②IEEE802.16 ③ISO20000
B.①ISO27000 ②ISO20000 ③IEEE802.16
C.①ISO20000 ②IEEE802.16 ③ISO27000
D.①IEEE802.16 ②ISO20000 ③ISO27000
参考答案：C

（64）（ ） 不属于将入侵检测系统部署在 DMZ 中的优点。
A、可以查到受保护区域主机被攻击的状态
B、可以检测防火墙系统的策略配置是否合理
C、可以检测 DMZ 被黑客攻击的重点
D、可以审计来自 Internet 上对受到保护网络的攻击类型
参考答案：D

（65）在以下认证方式中，最常用的认证方式是：（ ）
A、基于账户名/口令认证
B、基于摘要算法认证;
C、基于 PKI 认证;
D、基于数据库认证
参考答案：A

（66） 下列哪一种攻击方式不属于拒绝服务攻击：（ ）。
A、LOphtCrack
B、Synflood
C、Smurf
D、Ping of Death
参考答案：A

（67） 一个数据包过滤系统被设计成只允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则？（ ）
A、最小特权
B、阻塞点
C、失效保护状态
D、防御多样化
参考答案：A

（68）下面哪一个不是常见的备份类型（　　）。
A．完全备份
B．增量备份
C．差分备份
D．每周备份
参考答案：D

（69）电路网关防火墙工作在 OSI 协议的哪一层？（　）。
A、传输层
B、链路层
C、应用层
D、物理层
参考答案：A

（70） 一个电子邮件的发送者对数据摘要应用了数字签名。这能确保：（　）
A、信息的数据和时间戳
B、识别发信的计算机
C、对信息内容进行加密
D、对发送者的身份进行识别
参考答案：D

Network security starts from （ 71 ） any user, most likely a username and a password. Once authenticated, a stateful firewall enforces （ 72 ）such as what services are allowed to be accessed by network users. Though effective to prevent unauthorized access, this component fails to check potentially harm contents such as computer worms being transmitted over the network. An intrusion prevention system (IPS)helps detect and prevent such malware. （ 73 ）also monitors suspicious network affic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

（ 74 ）, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network （ 75 ） by the honeypot.

（71）A. authenticating	B. Proofreading	C. checking	D. detecting
（72）A. Control Strategy	B. access permission	C. access policies	D. security strategy
（73）A. lPS	B.IDS	C. P2DR	D. P2DR2
（74）A. Botnet	B. Honeypots	C. Phishing	D. Demilitarized zone
（75）A. being destroyed	B. being attacked	C. being damaged	D. being protected

参考答案：A C A B D