2022 年下半年信息安全工程师《综合知识》真题答案及解析

1、网络信息不泄露给非授权的用户、实体或程序，能够防止非授权者获取信息的属性是指网络信息安全的(　　)。

A．完整性

B．机密性

C．抗抵赖性

D．隐私性

信管网参考答案：B

查看解析：www.cnitpm.com/st/57347644.html

2、网络信息系统的整个生命周期包括网络信息系统规划、网络信息系统设计、网络信息系统集成实现、网络信息系统运行和维护、网络信息系统废弃 5 个阶段。网络信息安全管理重在过程，其中网络信息安全风险评估属于(　　)阶段。

A．网络信息系统规划

B．网络信息系统设计

C．网络信息系统集成与实现

D．网络信息系统运行和维护

信管网参考答案：A

查看解析：www.cnitpm.com/st/5734824578.html

3、近些年国密算法和标准体系受到越来越多的关注，基于国密算法的应用也得到了快速发展。以下国密算法中，属于分组密码算法的是(　　)。

A．SM2

B．SM3

C．SM4

D．SM9

信管网参考答案：C

查看解析：www.cnitpm.com/st/5734923337.html

4、域名服务是网络服务的基础，该服务主要是指从事域名根服务器运行和管理、顶级域名运行

和管理、域名注册、域名解析等活动。《互联网域名管理办法》规定，域名系统出现网络与信息安全事件时，应当在(　　)内向电信管理机构报告。

A．6 小时

B．12 小时

C．24 小时

D．3 天

信管网参考答案：C

查看解析：www.cnitpm.com/st/5735019367.html

5、《中华人民共和国密码法》对全面提升密码工作法治化水平起到了关键性作用，密码法规定国家对密码实行分类管理。依据《中华人民共和国密码法》的规定，以下密码分类正确的是(　)。

A．核心密码、普通密码和商用密码

B．对称密码和非对称密码

C．分组密码、序列密码和公钥密码

D．散列函数、对称密码和公钥密码

信管网参考答案：A

查看解析：www.cnitpm.com/st/5735112507.html

6、攻击树方法起源于故障树分析方法，可以用来进行渗透测试，也可以用来研究防御机制。以下关于攻击树方法的表述，错误的是(　)

A．能够采取专家头脑风暴法，并且将这些意见融合到攻击树中去

B．能够进行费效分析或者概率分析

C．不能用来建模多重尝试攻击、时间依赖及访问控制等场景

D．能够用来建模循环事件

信管网参考答案：D

查看解析：www.cnitpm.com/st/573527306.html

7、一般攻击者在攻击成功后退出系统之前，会在系统制造一些后门，方便自己下次入侵。以下设计后门的方法，错误的是(　)。

A．放宽文件许可权

B．安装嗅探器

C．修改管理员口令

D．建立隐蔽信道

信管网参考答案：C

查看解析：www.cnitpm.com/st/5735327795.html

8、从对信息的破坏性上看，网络攻击可以分为被动攻击和主动攻击，以下属于被动攻击的是（　）。

A．拒绝服务

B．窃听

C．伪造

D．中间人攻击

信管网参考答案：B

查看解析：www.cnitpm.com/st/5735411369.html

9、端口扫描的目的是找出目标系统上提供的服务列表。根据扫描利用的技术不同，端口扫描可以分为完全连接扫描、半连接扫描、SYN 扫描、FIN 扫描、隐蔽扫描、ACK 扫描、NULL 扫描等类型。其中，在源主机和目的主机的三次握手连接过程中，只完成前两次，不建立一次完整连接的扫描属于(　)

A．FIN 扫描

B．半连接扫描

C．SYN 扫描

D．完全连接扫描

信管网参考答案：B

查看解析：www.cnitpm.com/st/5735525469.html

10、通过假冒可信方提供网上服务，以欺骗手段获取敏感个人信息的攻击方式，被称为(　)。

A．网络钓鱼

B．拒绝服务

C．网络窃听

D．会话劫持

信管网参考答案：A

查看解析：www.cnitpm.com/st/5735617764.html

11、拒绝服务攻击是指攻击者利用系统的缺陷，执行一些恶意的操作，使得合法的系统用户不能及时得到应得的服务或系统资源。常见的拒绝服务攻击有：同步包风暴、UDP 洪水、垃圾邮件、泪滴攻击、Smurf 攻击、分布式拒绝服务攻击等类型。其中，能够通过在 IP 数据包中加入过多或不必要的偏移量字段，使计算机系统重组错乱的是(　　)。

A．同步包风暴

B．UDP 洪水

C．垃圾邮件

D．泪滴攻击

信管网参考答案：D

查看解析：www.cnitpm.com/st/5735713833.html

12、1997 年 NIST 发布了征集 AES 算法的活动，确定选择 Rijndael 作为 AES 算法，该算法支持的密钥长度不包括(　　)。

A．128 比特

B．192 比特

C．256 比特

D．512 比特

信管网参考答案：D

查看解析：www.cnitpm.com/st/5735821294.html

13、为了增强 DES 算法的安全性，NIST 于 1999 年发布了三重 DES 算法--TDEA。设 DES Ek()和 DES Dk()分别表示以 k 为密钥的 DES 算法的加密和解密过程，P 和 O 分别表示明文和密文消息，则 TDEA 算法的加密过程正确的是(　　)。

A. P → DES EK1 → DES EK2 → DES EK3 →O

B. P → DES DK1 → DES DK2 → DES DK3 →O

C. P → DES EK1 → DES DK2 → DES EK3 →O

D. P → DES DK1 → DES EK2 → DES DK3 →O

信管网参考答案：C

查看解析：www.cnitpm.com/st/5735929779.html

14、以下关于数字证书的叙述中，错误的是(　　)。

A. 数字证书由 RA 签发

B. 数字证书包含持有者的签名算法标识

C. 数字证书的有效性可以通过验证持有者的签名验证

D. 数字证书包含公开密钥拥有者信息

信管网参考答案：A

查看解析：www.cnitpm.com/st/5736019616.html

15、SSH 是基于公钥的安全应用协议，可以实现加密、认证、完整性检验等多种网络安全服务。SSH 由(　　)3 个子协议组成。

A. SSH 传输层协议、SSH 用户认证协议和 SSH 连接协议

B. SSH 网络层协议、SSH 用户认证协议和 SSH 连接协议

C. SSH 传输层协议、SSH 密钥交换协议和 SSH 用户认证协议

D. SSH 网络层协议、SSH 密钥交换协议和 SSH 用户认证协议

信管网参考答案：A

查看解析：www.cnitpm.com/st/573616271.html

16、针对电子邮件的安全问题，人们利用 PGP(Pretty Good Privacy)来保护电子邮件的安全。以下有关 PGP 的表述，错误的是(　　)。

A. PGP 的密钥管理采用 RSA

B. PGP 的完整性检测采用 MD5

C. PGP 的数字签名采用 RSA

D. PGP 的数据加密采用 DES

信管网参考答案：D

查看解析：www.cnitpm.com/st/5736221460.html

17、PDRR 信息模型改进了传统的只有保护的单一安全防御思想，强调信息安全保障的四个重要环节:保护(Protection)、检测(Detection)、恢复(Recovery)、响应(Response)。其中，信息隐藏是属于()的内容。

A. 保护

B. 检测

C. 恢复

D. 响应

信管网参考答案：A

查看解析：www.cnitpm.com/st/573631022.html

18、BLP 机密性模型用于防止非授权信息的扩散，从而保证系统的安全。其中主体只能向下读，不能向上读的特性被称为( )。

A. *特性

B. 调用特性

C. 简单安全特性

D. 单向性

信管网参考答案：C

查看解析：www.cnitpm.com/st/5736413368.html

19、依据《信息安全技术网络安全等级保护测评要求》的规定，定级对象的安全保护分为五个等级，其中第三级称为（）

A. 系统保护审计级

B. 安全标记保护级

C. 结构化保护级

D. 访问验证保护级

信管网参考答案：B

查看解析：www.cnitpm.com/st/5736517832.html

20、美国国家标准与技术研究院 NIST 发布了《提升关键基础设施网络安全的框架》，该框架定义了五种核心功能:识别(ldentify)、保护(Protect)、检测(Detect)、响应(Respond)、恢复(Recover)，每个功能对应具体的子类。其中，访问控制子类属于( )功能。

A．识别

B．保护

C．检测

D．响应

信管网参考答案：B

查看解析：www.cnitpm.com/st/573669963.html

21、物理安全是网络信息系统安全运行、可信控制的基础。物理安全威胁一般分为自然安全威胁和人为安全威胁。以下属于人为安全威胁的是( )。

A．地震

B．火灾

C．盗窃

D．雷电

信管网参考答案：C

查看解析：www.cnitpm.com/st/5736711800.html

22、互联网数据中心(IDC)是一类向用户提供资源出租基本业务和有关附加业务、在线提供 IT 应用平台能力租用服务和应用软件租用服务的数据中心。《互联网数据中心工程技术规范 GB51195-2016)》规定 IDC 机房分为 R1、R2、R3 三个级别。其中，R2 级 IDC 机房的机房基础设施和网络系统应具备冗余能力，机房基础设施和网络系统可支撑的 IDC 业务的可用性不应小于( )。

A．95%

B．99%

C．99.5%

D．99.9%

信管网参考答案：D

查看解析：www.cnitpm.com/st/5736826195.html

23、目前，计算机及网络系统中常用的身份认证技术主要有:口令认证技术、智能卡技术、基于生物特征的认证技术等。其中不属于生物特征的是( )。

A．数字证书

B．指纹

C．虹膜

D．DNA

信管网参考答案：A

查看解析：www.cnitpm.com/st/5736921545.html

24、Kerberos 是一个网络认证协议,其目标是使用密钥加密为客户端/服务器应用程序提供强身份认证。以下关于 Kerberos 的说法中，错误的是( )。

A．通常将认证服务器 AS 和票据发放服务器 TGS 统称为 KDC

B．票据(Ticket)主要包括客户和目的服务方 Principal、客户方 IP 地址、时间戳、Ticket 生存期和会话密钥

C．Kerberos 利用对称密码技术，使用可信第三方为应用服务器提供认证服务

D．认证服务器 AS 为申请服务的用户授予票据

信管网参考答案：D

查看解析：www.cnitpm.com/st/5737026640.html

25、一个 Kerberos 系统涉及四个基本实体: Kerberos 客户机、认证服务器 AS、票据发放服务器 TGS、应用服务器。其中，实现识别用户身份和分配会话秘钥功能的是(

A．Kerberos 客户机

B．认证服务器 AS

C．票据发放服务器 TGS

D．应用服务器

信管网参考答案：B

查看解析：www.cnitpm.com/st/5737150.html

26、访问控制机制是由一组安全机制构成，可以抽象为一个简单模型，以下不属于访问控制模型要素的是()。

A．主体

B．客体

C．审计库

D．协议

信管网参考答案：D

查看解析：www.cnitpm.com/st/5737211115.html

27、自主访问控制是指客体的所有者按照自己的安全策略授予系统中的其他用户对其的访问权。自主访问控制的实现方法包括基于行的自主访问控制和基于列的自主访问控制两大类，以下属于基于列的自主访问控制实现方法的是()。

A．访问控制表

B．能力表

C．前缀表

D．口令

信管网参考答案：A

查看解析：www.cnitpm.com/st/5737319918.html

28、访问控制规则是访问约束条件集，是访问控制策略的具体实现和表现形式。目前常见的访问控制规则有：基于角色的访问控制规则、基于时间的访问控制规则、基于异常事件的访问控制规则、基于地址的访问控制规则等。当系统中的用户登录出现三次失败后，系统在一段时间内冻结账户的规则属于( )。

A．基于角色的访问控制规则

B．基于时间的访问控制规划

C．基于异常事件的访问控制规则

D．基于地址的访问控制规则

信管网参考答案：C

查看解析：www.cnitpm.com/st/573746559.html

29、UNIX 系统中超级用户的特权会分解为若干组特权子集，分别赋给不同的管理员，使管理员只能具有完成其任务所需的权限，该访问控制的安全管理被称为()。

A．最小特权管理

B．最小泄漏管理

C．职责分离管理

D．多级安全管理

信管网参考答案：A

查看解析：www.cnitpm.com/st/57375838.html

30、防火墙是由一些软件、硬件组合而成的网络访问控制器，它根据一定的安全规则来控制流过防火墙的数据包，起到网络安全屏障的作用。以下关于防火墙的叙述中错误的是( )。

A．防火墙能够屏蔽被保护网络内部的信息、拓扑结构和运行状况

B．白名单策略禁止与安全规则相冲突的数据包通过防火墙，其他数据包都允许

C．防火墙可以控制网络带宽的分配使用

D．防火墙无法有效防范内部威胁

信管网参考答案：B

查看解析：www.cnitpm.com/st/5737625506.html

31、 Cisco IOS 的包过滤防火墙有两种访问规则形式: 标准 IP 访问表和扩展 IP 访问表。

标准 IP 访问控制规则的格式如下：

access-list list-number{deny/permit}source[source - wildcard][log]

扩展 IP 访问控制规则的格式如下:

access-list list-number {deny/permit}protocol

source source-wildcard source-qualifiers

destination destination-wildcard destination-qualifiers [log|log-input]

针对标准 IP 访问表和扩展 IP 访问表，以下叙述中，错误的是( )。

A. 标准 IP 访问控制规则的 list-number 规定为 1~99

B. permit 表示若经过 Cisco IOS 过滤器的包条件匹配，则允许该包通过

C. source 表示来源的 IP 地址

D. source-wildcard 表示发送数据包的主机地址的通配符掩码，其中 0 表示“忽略”

信管网参考答案：D

查看解析：www.cnitpm.com/st/5737729793.html

32、网络地址转换简称 NAT，NAT 技术主要是为了解决网络公开地址不足而出现的。网络地址转换的实现方式中，把内部地址映射到外部网络的一个 IP 地址的不同端口的实现方式被称为( )。

A. 静态 NAT

B. NAT 池

C. 端口 NAT

D. 应用服务代理

信管网参考答案：C

查看解析：www.cnitpm.com/st/573787319.html

33、用户在实际应用中通常将入侵检测系统放置在防火墙内部，这样可以( )。

A. 增强防火墙的安全性

B. 扩大检测范围

C. 提升检测效率

D. 降低入侵检测系统的误报率

信管网参考答案：D

查看解析：www.cnitpm.com/st/57379669.html

34、虚拟专用网 VPN 技术把需要经过公共网络传递的报文加密处理后由公共网络发送到目的地。以下不属于 VPN 安全服务的是()。

A. 合规性服务

B．完整性服务

C．保密性服务

D．认证服务

信管网参考答案：A

查看解析：www.cnitpm.com/st/573806186.html

35、按照 VPN 在 TCP/IP 协议层的实现方式，可以将其分为链路层 VPN、网络层 VPN、传输层 VPN。以下 VPN 实现方式中，属于网络层 VPN 的是()。

A．ATM

B．隧道技术

C．SSL

D．多协议标签交换 MPLS

信管网参考答案：B

查看解析：www.cnitpm.com/st/5738125095.html

36、IPSec 是 Internet Protocol Security 的缩写,以下关于 IPSec 协议的叙述中,错误的是()。

A．IP AH 的作用是保证 IP 包的完整性和提供数据源认证

B．IP AH 提供数据包的机密性服务

C．IP ESP 的作用是保证 IP 包的保密性

D．IP Sec 协议提完整性验证机制

信管网参考答案：B

查看解析：www.cnitpm.com/st/5738225093.html

37、SSL 是一种用于构建客户端和服务器端之间安全通道的安全协议，包含:握手协议、密码规格变更协议、记录层协议和报警协议。其中用于传输数据的分段、压缩及解压缩、加密及解密、完整性校验的是( )。

A．握手协议

B．密码规格变更协议

C．记录层协议

D．报警协议

信管网参考答案：C

查看解析：www.cnitpm.com/st/573835294.html

38、IPSec VPN 的功能不包括( )。

A．数据包过滤

B．密钥协商

C．安全报文封装

D．身份鉴别

信管网参考答案：A

查看解析：www.cnitpm.com/st/5738426888.html

39、入侵检测模型 CIDF 认为入侵检测系统由事件产生器、事件分析器、响应单元和事件数据库 4 个部分构成，其中分析所得到的数据，并产生分析结果的是()。

A．事件产生器

B．事件分析器

C．响应单元

D．事件数据库

信管网参考答案：B

查看解析：www.cnitpm.com/st/5738514533.html

40、误用入侵检测通常称为基于特征的入侵检测方法，是指根据已知的入侵模式检测入侵行为。常见的误用检测方法包括：基于条件概率的误用检测方法、基于状态迁移的误用检测方法、基于键盘监控的误用检测方法、基于规则的误用检测方法。其中 Snort 入侵检测系统属于( )。

A．基于条件概率的误用检测方法

B．基于状态迁移的误用检测方法

C．基于键盘监控的误用检测方法

D．基于规则的误用检测方法

信管网参考答案：D

查看解析：www.cnitpm.com/st/5738625539.html

41、根据入侵检测系统的检测数据来源和它的安全作用范围，可以将其分为基于主机的入侵检测系统 HIDS、基于网络的入侵检测系统 NIDS 和分布式入侵检测系统 DIDS 三种。以下软件不属于基于主机的入侵检测系统 HIDS 的是()。

A. Cisco Secure ID

B. SWATCH

C. Tripwire

D. 网页防篡改系统

信管网参考答案：A

查看解析：www.cnitpm.com/st/5738725871.html

42、根据入侵检测应用对象，常见的产品类型有 Web IDS、数据库 IDS、工控 IDS 等。以下攻击中，不宜采用数据库 IDS 检测的是( )。

A. SQL 注入攻击

B. 数据库系统口令攻击

C. 跨站点脚本攻击

D. 数据库漏洞利用政击

信管网参考答案：C

查看解析：www.cnitpm.com/st/5738820369.html

43、Snort 是典型的网络入侵检测系统，通过获取网络数据包，进行入侵检测形成报警信息。Snort 规则由规则头和规则选项两部分组成。以下内容不属于规则头的是( )。

A. 源地址

B. 目的端口号

C. 协议

D. 报警信息

信管网参考答案：D

查看解析：www.cnitpm.com/st/5738924053.html

44、网络物理隔离系统是指通过物理隔离技术，在不同的网络安全区域之间建立一个能够实现物理隔离、信息交换和可信控制的系统，以满足不同安全区域的信息或数据交换。以下有关网络物理隔离系统的叙述中，错误的是()。

A．使用网闸的两个独立主机不存在通信物理连接，主机对网闸只有“读”操作

B．双硬盘隔离系统在使用时必须不断重新启动切换，且不易于统一管理

C．单向传输部件可以构成可信的单向信道，该信道无任何反馈信息

D．单点隔离系统主要保护单独的计算机，防止外部直接攻击和干扰

信管网参考答案：A

查看解析：www.cnitpm.com/st/5739022339.html

45、网络物理隔离机制中，使用一个具有控制功能的开关读写存储安全设备，通过开关的设置来连接或者切断两个独立主机系统的数据交换,使两个或者两个以上的网络在不连通的情况下，实现它们之间的安全数据交换与共享，该技术被称为()。

A．双硬盘

B．信息摆渡

C．单向传输

D．网闸

信管网参考答案：D

查看解析：www.cnitpm.com/st/573913865.html

46、网络安全审计是指对网络信息系统的安全相关活动信息进行获取、记录存储、分析和利用的工作。在《计算机信息系统安全保护等级划分准则》(GB17859)中，不要求对删除客体操作具备安全审计功能的计算机信息系统的安全保护等级属于()。

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：A

查看解析：www.cnitpm.com/st/5739212614.html

47、操作系统审计一般是对操作系统用户和系统服务进行记录，主要包括用户登录和注销、系统服务启动和关闭、安全事件等。Windows 操作系统记录系统事件的日志中，只允许系统管理员访问的是()。

A．系统日志

B．应用程序日志

C．安全日志

D．性能日志

信管网参考答案：C

查看解析：www.cnitpm.com/st/5739317185.html

48、网络审计数据涉及系统整体的安全性和用户隐私性，以下安全技术措施不属于保护审计数据安全的是( )。

A．系统用户分权管理

B．审计数据加密

C．审计数据强制访问

D．审计数据压缩

信管网参考答案：D

查看解析：www.cnitpm.com/st/573944460.html

49、以下网络入侵检测不能检测发现的安全威胁是( )。

A．黑客入侵

B．网络蠕虫

C．非法访问

D．系统漏洞

信管网参考答案：D

查看解析：www.cnitpm.com/st/573957167.html

50、网络信息系统漏洞的存在是网络攻击成功的必要条件之一。以下有关安全事件与漏洞对应关系的叙述中，错误的是( )。

A. Internet 蠕虫，利用 Sendmail 及 finger 漏洞

B. 冲击波蠕虫，利用 TCP/IP 协议漏洞

C. Wannacry 勒索病毒，利用 Windows 系统的 SMB 漏洞

D. Slammer 蠕虫，利用微软 MS SQL 数据库系统漏洞

信管网参考答案：B

查看解析：www.cnitpm.com/st/5739624568.html

51、网络信息系统的漏洞主要来自两个方面：非技术性安全漏洞和技术性安全漏洞。以下属于非技术性安全漏洞来源的是( )。

A. 网络安全策略不完备

B. 设计错误

C. 缓冲区溢出

D. 配置错误

信管网参考答案：A

查看解析：www.cnitpm.com/st/573973134.html

52、以下网络安全漏洞发现工具中，具备网络数据包分析功能的是( )。

A. Flawfinder

B. Wireshark

C. MOPS

D. Splint

信管网参考答案：B

查看解析：www.cnitpm.com/st/5739812451.html

53、恶意代码能够经过存储介质或网络进行传播，未经授权认证访问或破坏计算机系统。恶意代码的传播方式分为主动传播和被动传播。()属于主动传播的恶意代码。

A. 逻辑炸弹

B. 特洛伊木马

C. 网络蠕虫

D. 计算机病毒

信管网参考答案：C

查看解析：www.cnitpm.com/st/573991850.html

54、文件型病毒不能感染的文件类型是( )。

A. HTML 型

B. COM 型

C. SYS 型

D. EXE 类型

信管网参考答案：A

查看解析：www.cnitpm.com/st/5740011619.html

55、网络蠕虫利用系统漏洞进行传播。根据网络蠕虫发现易感主机的方式，可将网络蠕虫的传播方法分成三类:随机扫描、顺序扫描、选择性扫描。以下网络蠕虫中，支持顺序扫描传播策略的是()。

A. Slammer

B. Nimda

C. Lion Worm

D. Blaster

信管网参考答案：D

查看解析：www.cnitpm.com/st/5740111345.html

56、()是指攻击者利用入侵手段，将恶意代码植入目标计算机，进而操纵受害机执行恶意活动

A. ARP 欺骗

B. 网络钓鱼

C. 僵尸网络

D. 特洛伊木马

信管网参考答案：C

查看解析：www.cnitpm.com/st/5740212962.html

57、拒绝服务攻击是指攻击者利用系统的缺陷，执行一些恶意操作，使得合法用户不能及时得到应得的服务或者系统资源。常见的拒绝服务攻击包括：UDP 风暴、SYN Food、ICMP 风暴、Smurf 攻击等。其中，利用 TCP 协议中的三次握手过程，通过攻击使大量第三次握手过程无法完成而实施拒绝服务攻击的是()。

A．UDP 风暴

B．SYN Flood

C．ICMP 风暴

D．Smurf 攻击

信管网参考答案：B

查看解析：www.cnitpm.com/st/5740316181.html

58、假如某数据库中数据记录的规范为<姓名，出生日期，性别，电话>，其中一条数据记录为:<张三，1965 年 4 月 15 日，男，12345678>。为了保护用户隐私，对其进行隐私保护处理，处理后的数据记录为:<张*，1960-1970 年生，男，1234****>这种隐私保护措施被称为()。

A．泛化

B．抑制

C．扰动

D．置换

信管网参考答案：A

查看解析：www.cnitpm.com/st/5740428925.html

59、信息安全风险评估是指确定在计算机系统和网络中每一种资源缺失或遭到破坏对整个系统造成的预计损失数量，是对威胁、脆弱点以及由此带来的风险大小的评估。一般将信息安全风险评估实施划分为评估准备、风险要素识别、风险分析和风险处置 4 个阶段。其中对评估活动中的各类关键要素资产、威胁、脆弱性、安全措施进行识别和赋值的过程属于( )阶段

A．评估准备

B．风险要素识别

C．风险分析

D．风险处置

信管网参考答案：B

查看解析：www.cnitpm.com/st/5740511702.html

60、计算机取证主要围绕电子证据进行，电子证据必须是可信、准确、完整、符合法律法规的。电子证据肉眼不能够直接可见，必须借助适当的工具的性质，是指电子证据的( )。

A．高科技性

B．易破坏性

C．无形性

D．机密性

信管网参考答案：C

查看解析：www.cnitpm.com/st/5740613690.html

61、按照网络安全测评的实施方式，测评主要包括安全管理检测、安全功能检测、代码安全审计、安全渗透、信息系统攻击测试等。其中《信息安全技术 信息系统等级保护安全设计技术要求》(GB/T25070-2019)等国家标准是( )的主要依据

A．安全管理检测

B．信息系统攻击测试

C．代码安全审计

D．安全功能检测

信管网参考答案：D

查看解析：www.cnitpm.com/st/5740717883.html

62、网络安全渗透测试的过程可以分为委托受理、准备、实施、综合评估和结题 5 个阶段，其中确认渗透时间，执行渗透方案属于()阶段。

A．委托受理

B．准备

C．实施

D．综合评估

信管网参考答案：C

查看解析：www.cnitpm.com/st/5740814231.html

63、日志文件是纯文本文件,日志文件的每一行表示一个消息,由（）4 个域的固定格式组成

A．时间标签、主机名、生成消息的子系统名称、消息

B．主机名、生成消息的子系统名称、消息、备注

C．时间标签、主机名、消息、备注

D．时间标签、主机名、用户名、消息

信管网参考答案：A

查看解析：www.cnitpm.com/st/5740910270.html

64、在 Windows 系统中需要配置的安全策略主要有账户策略、审计策略、远程访问、文件共享等。以下不属于配置账户策略的是，（ ）。

A．密码复杂度要求

B．账户锁定阈值

C．日志审计

D．账户锁定计数器

信管网参考答案：C

查看解析：www.cnitpm.com/st/574104720.html

65、随着数据库所处的环境日益开放，所面临的安全威胁也日益增多，其中攻击者假冒用户身份获取数据库系统访问权限的威胁属于（ ）。

A．旁路控制

B．隐蔽信道

C．口令破解

D．伪装

信管网参考答案：D

查看解析：www.cnitpm.com/st/5741115212.html

66、多数数据库系统有公开的默认账号和默认密码，系统密码有些就存储在操作系统中的普通文本文件中，如：Oracle 数据库的内部密码就存储在( )文件中。

A. listener.ora

B. strXXX.cmd

C. key.ora

D. paswrD.cmd

信管网参考答案：B

查看解析：www.cnitpm.com/st/5741226131.html

67、数据库系统是一个复杂性高的基础性软件，其安全机制主要有标识与鉴别、访问控制、安全审计、数据加密、安全加固、安全管理等，其中( )可以实现安全角色配置、安全功能管理

A. 访问控制

B. 安全审计

C. 安全加固

D. 安全管理

信管网参考答案：D

查看解析：www.cnitpm.com/st/5741314592.html

68、交换机是构成网络的基础设备，主要功能是负责网络通信数据包的交换传输。其中工作于 OSI 的数据链路层，能够识别数据中的 MAC，并根据 MAC 地址选择转发端口的是()

A. 第一代交换机

B. 第二代交换机

C. 第三代交换机

D. 第四代交换机

信管网参考答案：B

查看解析：www.cnitpm.com/st/57414167.html

69、以下不属于网络设备提供的 SNMP 访问控制措施的是( )。

A. SNMP 权限分级机制

B. 限制 SNMP 访问的 IP 地址

C. SNMP 访问认证

D. 关闭 SNMP 访问

信管网参考答案：A

查看解析：www.cnitpm.com/st/5741518043.html

70、网络设备的常见漏洞包括拒绝服务漏洞、旁路、代码执行、溢出、内存破坏等。CVE-2000-0945 信息显示思科 Catalyst 3500 XL 交换机的 Web 配置接口允许远程攻击者不需要认证就执行命令，该漏洞属于( )。

A. 拒绝服务漏洞

B. 旁路

C. 代码执行

D. 内存破坏

信管网参考答案：C

查看解析：www.cnitpm.com/st/5741620645.html

71~75、Perhaps the most obvious difference between private-key and public-key encryption is that the former assumes complete secrecy of all cry to graphic keys, whereas the latter requires secrecy for only the private key.Although this may seem like a minor distinction ,the ramifications are huge: in the private-key setting the communicating parties must somehow be able to share the (71) key without allowing any third party to learn it, whereas in the public-key setting the (72) key can be sent from one party to the other over a public channel without compromising security.For parties shouting across a room or, more realistically , communicating over a public network like a phone line or then ternet, public-key encryption is the only option.

Another important distinction is that private-key encryption sch emesuse the (73) key for both encryption and decryption, whereas public key encryption schemes use (74) keys

for each operation.That is public-key encryption is inherently as ymmetri C. This asymmetry in the public-key setting means that the roles of sender and receiver are not interchangeable as they are in the private-key setting; a single key-pair allows communication in one direction only.(Bidirectional communication can be achieved in a number of ways; the point is that a single invocation of a public-key encryption scheme forces ad is tinction between one user who acts as a receiver and other users who act as senders.)。In addition, a single instance of a (75) encryption scheme enables multiple senders to communicate privately with a single receiver,in contrast to the private-key case where a secret key shared between two parties enables private communication only between those two parties.

(1) A. main

B. same

C. public

D. secret

(2) A. stream

B. different

C. public

D. secret

(3) A. different

B. same

C. public

D. private

(4) A. different

B. same

C. public

D. private

(5) A. private-key

B. public-key

C. stream

D. Hash

信管网参考答案：D、C、B、A、B

查看解析：www.cnitpm.com/st/5741716708.html