2021 年下半年信息安全工程师《综合知识》真题答案及解析

本资料由信管网(www.cnitpm.com)整理发布，供信管网学员使用！

信管网是专业软考中高级与 PMP 考试培训服务网站。提供了考试资讯、考试报名、成绩查询、资料下载、在线答题、考试培训、项目管理人才交流、企业内训等服务。

信管网资料库提供了备考软考的精品学习资料；信管网案例分析频道和论文频道拥有丰富的案例范例和论文范例，信管网考试中心拥有软考中高级历年真题和超过 5000 多道试题免费在线测试；信管网每年指导考生超 100000+人。

信管网——专业、专注、专心，成就你的项目管理师梦想！

信管网：www.cnitpm.com

信管网考试中心：www.cnitpm.com/exam/

信管网培训中心：www.cnitpm.com/wx/

信管网微信公众号

信管网客服微信号

1、常见的信息安全基本属性有：机密性、完整性、可用性、抗抵赖性和可控性等。其中合法许可的用户能够及时获取网络信息或服务的特性，是指信息安全的（）。

A. 机密性

B. 完整性

C. 可用性

D. 可控性

信管网参考答案：C

查看解析：www.cnitpm.com/st/5222218596.html

2、2010 年，首次发现针对工控系统实施破坏的恶意代码 Stuxnet（简称“震网”病毒），“震网”病毒攻击的是伊朗核电站西门子公司的（ ）系统。

A. Microsoft WinXP

B. Microsoft Win7

C. Google Android

D. SIMATIC WinCC

信管网参考答案：D

查看解析：www.cnitpm.com/st/522233348.html

3、要实现网络信息安全基本目标，网络应具备 （)等基本功能。

A. 预警、认证、控制、响应

B. 防御、监测、应急、恢复

C. 延缓、阻止、检测、限制

D. 可靠、可用、可控、可信

信管网参考答案：B

查看解析：www.cnitpm.com/st/5222416362.html

4、为防范国家数据安全风险，维护国家安全，保护公共利益，2021 年 7 月，中国网络安全审查办公室发布公告，对“滴滴出行”“运满满”“货车帮”和“BOSS 直聘”开展网络安全审查。此次审查依据的国家相关法律法规是（ ）。

A. 《中华人民共和国网络安全法》和《中华人民共和国国家安全法》

B. 《中华人民共和国网络安全法》和《中华人民共和国密码法》

C. 《中华人民共和国数据安全法》和《中华人民共和国网络安全法》

D. 《中华人民共和国数据安全法》和《中华人民共和国国家安全法》

信管网参考答案：A

查看解析：www.cnitpm.com/st/5222512951.html

5、2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议表决通过了《中华人民共和国数据安全法》，该法律自 （ ） 起施行。

A. 2021 年 9 月 1 日

B. 2021 年 10 月 1 日

C. 2021 年 11 月 1 日

D. 2021 年 12 月 1 日

信管网参考答案：A

查看解析：www.cnitpm.com/st/522263541.html

6、根据网络安全等级保护 2.0 的要求，对云计算实施安全分级保护。围绕“一个中心，三重防护”的原则，构建云计算安全等级保护框架。其中一个中心是指安全管理中心，三重防护包括：计算环境安全、区域边界安全和通信网络安全。以下安全机制属于安全管理中心的是（ ）。

A. 应用安全

B. 安全审计

C. Web 服务

D. 网络访问

信管网参考答案：B

查看解析：www.cnitpm.com/st/5222715531.html

7、《中华人民共和国密码法》由中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议于 2019 年 10 月 26 日通过，已于 2020 年 1 月 1 日起施行。《中华人民共和国密码法》规定国家对密码实分类管理，密码分为（ ）。

A．核心密码、普通密码和商用密码

B．对称密码、公钥密码和哈希算法

C．国际密码、国产密码和商用密码

D．普通密码，涉密密码和商用密码

信管网参考答案：A

查看解析：www.cnitpm.com/st/5222815111.html

8、现代操作系统提供的金丝雀（Canary）漏洞缓解技术属于 （ ）

A．数据执行阻止

B．SEHOP

C．堆栈保护

D．地址空间随机化技术

信管网参考答案：C

查看解析：www.cnitpm.com/st/5222926832.html

9、2021 年 7 月 30 日，国务院总理李克强签署第 745 号国务院令，公布《关键信息基础设施安全保护条例》。该条例在法律责任部分细化了在安全保护全过程中，各个环节违反相应条例的具体处罚措施。以下说法错误的是（ ）

A．在安全事故发生之前，运营者应当对关键信息基础设施的安全保护措施进行规划建设。在安全事故发生后，运营者未报告相关部门的，也会处以相应的罚金

B．对于受到治安管理处罚的人员，3 年内不得从事网络安全管理和网络安全运营关键岗位的工作

C．对于受到刑事处罚的人员，终身不得从事网络安全管理和网络安全运营关键岗位的工作

D．网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行相关职责或者玩忽职守、滥用职权、徇私舞弊的，或者发生重大责任事故的，会对相关监管、保护和服务人员给予处分，严重者追究法律责任

信管网参考答案：B

查看解析：www.cnitpm.com/st/522308845.html

10、网络攻击行为分为主动攻击和被动攻击，主动攻击一般是指攻击者对被攻击信息的修改，而

被动攻击主要是收集信息而不进行修改等操作，被动攻击更具有隐蔽性。以下网络攻击中，属于被动攻击的是（ ）。

A．重放攻击

B．假冒攻击

C．拒绝服务攻击

D．窃听

信管网参考答案：D

查看解析：www.cnitpm.com/st/5223127924.html

11、SYN 扫描首先向目标主机发送连接请求，当目标主机返回响应后，立即切断连接过程， 并查看响应情况。如果目标主机返回（ ），表示目标主机的该端口开放。

A．ACK 信息

B．RESET 信息

C．RST 信息

D．ID 头信息

信管网参考答案：A

查看解析：www.cnitpm.com/st/5223223655.html

12、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。以下给出的攻击方式中，不属于拒绝服务攻击的是（ ）

A．SYN Flood

B．DNS 放大攻击

C．SQL 注入

D．泪滴攻击

信管网参考答案：C

查看解析：www.cnitpm.com/st/5223312431.html

13、网络攻击者经常采用的工具主要包括：扫描器、远程监控、密码破解、网络嗅探器、安全渗透工具箱等。以下属于网络嗅探器工具的是（ ）。

A. Super Scan

B. LOphtCrack

C. Metasploit

D. WireShark

信管网参考答案：D

查看解析：www.cnitpm.com/st/5223417677.html

14、为保护移动应用 App 的安全性，通常采用防反编译、防调试、防篡改和防窃取等多种安全保护措施，在移动应用 App 程序插入无关代码属于(　　)技术。

A. 防反编译

B. 防调试

C. 防篡改

D. 防窃取

信管网参考答案：A

查看解析：www.cnitpm.com/st/5223518367.html

15、密码算法可以根据密钥属性的特点进行分类，其中发送方使用的加密密钥和接收方使用的解密密钥不相同，并且从其中一个密钥难以推导出另一个密钥，这样的加密算法称为(　　)。

A. 非对称密码

B. 单密钥密码

C. 对称密码

D. 序列密码

信管网参考答案：A

查看解析：www.cnitpm.com/st/5223614108.html

16、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 010001，其二进制输出为（ ）

A．0110

B．1001

C．0100

D．0101

信管网参考答案：C

查看解析：www.cnitpm.com/st/522374736.html

17、国产密码算法是指由国家密码研究相关机构自主研发，具有相关知识产权的商用密码算法。以下国产密码算法中，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/522386616.html

18、Hash 算法是指产生哈希值或杂凑值的计算方法。MD5 算法是由 Rivest 设计的 Hash 算法，该算法以 512 比特数据块为单位处理输入，产生（ ）的哈希值。

A．64 比特

B．128 比特

C．256 比特

D．512 比特

信管网参考答案：B

查看解析：www.cnitpm.com/st/5223923806.html

19、数字签名是对以数字形式存储的消息进行某种处理，产生一种类似传统手书签名功效的信息处理过程。数字签名最常见的实现方式是基于 （ ）

A．对称密码体制和哈希算法

B．公钥密码体制和单向安全哈希算法

C．序列密码体制和哈希算法

D．公钥密码体制和对称密码体制

信管网参考答案：B

查看解析：www.cnitpm.com/st/5224026082.html

20、Diffie-Hellman 密钥交换协议是一种共享秘密的方案，该协议是基于(　　)的困难性。

A．大素数分解问题

B．离散对数问题

C．椭圆离散对数问题

D．背包问题

信管网参考答案：B

查看解析：www.cnitpm.com/st/522412431.html

21、计算机网络为了实现资源共享，采用协议分层设计思想，每层网络协议都有地址信息，如网卡（MAC）地址、IP 地址、端口地址和域名地址，以下有关上述地址转换的描述错误的是　（　　）。

A．DHCP 协议可以完成 IP 地址和端口地址的转换

B．DNS 协议可以实现域名地址和 IP 地址之间的转换

C．ARP 协议可以实现 MAC 地址和 IP 地址之间的转换

D．域名地址和端口地址无法转换

信管网参考答案：A

查看解析：www.cnitpm.com/st/522428592.html

22、BLP 机密性模型中，安全级的顺序一般规定为：公开＜秘密＜机密＜绝密。两个范畴集之间的关系是包含、被包含或无关。如果一个 BLP 机密性模型系统访问类下：

文件 E 访问类：｛机密：财务处，科技处｝；

文件 F 访问类：｛机密：人事处，财务处｝；

用户 A 访问类：｛绝密：人事处｝；

用户 B 访问类：｛绝密：人事处，财务处，科技处｝。

则以下表述中，正确的是（ ）

A．用户 A 不能读文件 F

B．用户 B 不能读文件 F

C．用户 A 能读文件 E

D．用户 B 不能读文件 E

信管网参考答案：A

查看解析：www.cnitpm.com/st/522436218.html

23、BiBa 模型主要用于防止非授权修改系统信息，以保护系统的信息完整性，该模型提出的“主体不能向上写”指的是（ ）

A．简单安全特性

B．保密特性

C．调用特性

D．＊特性

信管网参考答案：D

查看解析：www.cnitpm.com/st/522448086.html

24、PDRR 模型由防护（Protection），检测（Detection）、恢复（Recovery）、响应（Response）四个重要环节组成。数据备份对应的环节是（ ）

A．防护

B．检测

C．恢复

D．响应

信管网参考答案：C

查看解析：www.cnitpm.com/st/522459811.html

25、能力成熟度模型（CMM）是对一个组织机构的能力进行成熟度评估的模型，成熟度级别一般分为五级：1 级-非正式执行，2 级-计划跟踪，3 级-充分定义，4 级-量化控制，5 级-持续优化。在软件安全能力成熟度模型中，漏洞评估过程属于（ ）

A．CMM1 级

B．CMM2 级

C．CMM3 级

D．CMM4 级

信管网参考答案：C

查看解析：www.cnitpm.com/st/5224622759.html

26、等级保护制度是中国网络安全保障的特色和基石，等级保护 2.0 新标准强化了可信计算技术使用的要求。其中安全保护等级（　　）　要求对应用程序的所有执行环节进行动态可信验证。

A．第一级

B．第二级

C．第三级

D．第四级

信管网参考答案：D

查看解析：www.cnitpm.com/st/5224717103.html

27、按照《计算机场地通用规范（GB / T2887-2011）》的规定，计算机机房分为四类：主要工作房间、第一类辅助房间、第二类辅助房间和第三类辅助房间。以下属于第一类辅助房间的是（　　）。

A．终端室

B．监控室

C．资料室

D．储藏室

信管网参考答案：B

查看解析：www.cnitpm.com/st/522489182.html

28、认证一般由标识和鉴别两部分组成。标识是用来代表实体对象的身份标志，确保实体的唯一性和可辨识性，同时与实体存在强关联。以下不适合作为实体对象身份标识的是（　　）。

A．常用 IP 地址

B．网卡地址

C．通信运营商信息

D．用户名和口令

信管网参考答案：C

查看解析：www.cnitpm.com/st/5224914397.html

29、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。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，为用户提供服务的设备或系统被称为（　　）

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：D

查看解析：www.cnitpm.com/st/5225018038.html

30、公钥基础设施 PKI 是有关创建、管理、存储、分发和撤销公钥证书所需要的硬件、软件、人员、策略和过程的安全服务设施。公钥基础设施中，实现证书废止和更新功能的是(　　)

A．CA

B．终端实体

C．RA

D．客户端

信管网参考答案：A

查看解析：www.cnitpm.com/st/5225119631.html

31、访问控制是对信息系统资源进行保护的重要措施，适当的访问控制能够阻止未经授权的用户有意或者无意地获取资源。如果按照访问控制的对象进行分类，对文件读写进行访问控制属于（　　）。

A．网络访问控制

B．操作系统访问控制

C．数据库 / 数据访问控制

D．应用系统访问控制

信管网参考答案：B

查看解析：www.cnitpm.com/st/5225229602.html

32、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。以下形式属于基于列的自主访问控制的是（　　）

A．能力表

B．前缀表

C．保护位

D．口令

信管网参考答案：C

查看解析：www.cnitpm.com/st/5225321719.html

33、访问控制规则实际上就是访问约束条件集，是访问控制策略的具体实现和表现形式。常见的访问控制规则有基于用户身份、基于时间、基于地址、基于服务数量等多种情况。其中，根据用户完成某项任务所需要的权限进行控制的访问控制规则属于（　　）。

A．基于角色的访问控制规则

B．基于地址的访问控制规则

C．基于时间的访问控制规则

D．基于异常事件的访问控制规则

信管网参考答案：A

查看解析：www.cnitpm.com/st/5225421270.html

34、IIS 是 Microsoft 公司提供的 Web 服务器软件，主要提供 Web 服务。IIS 的访问控制主要包括：请求过滤、URL 授权控制、IP 地址限制、文件授权等安全措施，其中对文件夹的 NTFS 许可权限管理属于（　　）。

A．请求过滤

B．URL 授权控制

C．IP 地址限制

D．文件授权

信管网参考答案：D

查看解析：www.cnitpm.com/st/5225521667.html

35、防火墙是由一些软件、硬件组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网络数据包，从而起到网络安全屏障的作用，防火墙不能实现的功能是（　　）。

A．限制网络访问

B．网络带宽控制

C．网络访问审计

D．网络物理隔离

信管网参考答案：D

查看解析：www.cnitpm.com/st/5225622197.html

36、包过滤是在 IP 层实现的防火墙技术，根据包的源 IP 地址、目的 IP 地址、源端口、目的端口及包传递方向等包头信息判断是否允许包通过。包过滤型防火墙扩展 IP 访问控制规则的格式如下：

access-list list-number {demy|permit}protocol

source source-wildcard source-qualifiers

destination destination-wildcard

destination-qualifiers[log|log-input]

则以下说法错误的是 （　　）。

A．source 表示来源的 IP 地址

B．deny 表示若经过过滤器的包条件匹配，则允许该包通过

C．destination 表示目的 IP 地址

D．log 表示记录符合规则条件的网络包

信管网参考答案：B

查看解析：www.cnitpm.com/st/5225716273.html

37、以下有关网站攻击防护及安全监测技术的说法，错误的 （ ）

A. Web 应用防火墙针对 80、443 端口

B. 包过滤防火墙只能基于 IP 层过滤网站恶意包

C. 利用操作系统的文件调用事件来检测网页文件的完整性变化，可以发现网站被非授权修改

D. 网络流量清洗可以过滤掉针对目标网络攻击的恶意网络流量

信管网参考答案：B

查看解析：www.cnitpm.com/st/5225826897.html

38、通过 VPN 技术，企业可以在远程用户、分支部门、合作伙伴之间建立一条安全通道，实现 VPN 提供的多种安全服务。VPN 不能提供的安全服务是( )。

A. 保密性服务

B. 网络隔离服务

C. 完整性服务

D. 认证服务

信管网参考答案：B

查看解析：www.cnitpm.com/st/5225924498.html

39、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。以下属于网络层 VPN 实现方式的是（ ）。

A. 多协议标签交换 MPLS

B. ATM

C. Frame Relay

D. 隧道技术

信管网参考答案：D

查看解析：www.cnitpm.com/st/5226011434.html

40、在 IPSec 虚拟专用网当中，提供数据源认证的协议是（ ）

A. SKIP

B. IP AH

C. IP ESP

D. ISAKMP

信管网参考答案：B

查看解析：www.cnitpm.com/st/5226114857.html

41、通用入侵检测框架模型（CIDF）由事件产生器、事件分析器、响应单元和事件数据库四个部分组成。其中向系统其他部分提供事件的是（ ）

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：A

查看解析：www.cnitpm.com/st/5226223863.html

42、蜜罐技术是一种基于信息欺骗的主动防御技术，是入侵检测技术的一个重要发展方向，蜜罐为了实现一台计算机绑定多个 IP 地址，可以使用（ ） 协议来实现。

A. ICMP

B. DHCP

C. DNS

D. ARP

信管网参考答案：D

查看解析：www.cnitpm.com/st/5226326060.html

43、基于网络的入侵检测系统（NIDS）通过侦听网络系统，捕获网络数据包，并依据网络包是否包含攻击特征，或者网络通信流是否异常来识别入侵行为。以下不适合采用 NIDS 检测的入侵行为是（ ）。

A. 分布式拒绝服务攻击

B．缓冲区溢出

C．注册表修改

D．协议攻击

信管网参考答案：C

查看解析：www.cnitpm.com/st/5226416390.html

44、网络物理隔离有利于强化网络安全的保障，增强涉密网络的安全性。以下关于网络物理隔离实现技术的表述，错误的是（ ）。

A．物理断开可以实现处于不同安全域的网络之间以间接方式相连接

B．内外网线路切换器通过交换盒的开关设置控制计算机的网络物理连接

C．单硬盘内外分区技术将单台物理 PC 虚拟成逻辑上的两台 PC

D．网闸通过具有控制功能开关来连接或切断两个独立主机系统的数据交换

信管网参考答案：A

查看解析：www.cnitpm.com/st/5226516747.html

45、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。Linux 操作系统中，文件 lastlog 记录的是（ ）。

A．系统开机自检日志

B．当前用户登录日志

C．最近登录日志

D．系统消息

信管网参考答案：C

查看解析：www.cnitpm.com/st/522668877.html

46、关键信息基础设施的核心操作系统、关键数据库一般设有操作员、安全员和审计员三种角色类型。以下表述错误的是（ ）。

A．操作员只负责对系统的操作维护工作

B．安全员负责系统安全策略配置和维护

C．审计员可以查看操作员、安全员的工作过程日志

D．操作员可以修改自己的操作记录

信管网参考答案：D

查看解析：www.cnitpm.com/st/5226714399.html

47、网络流量数据挖掘分析是对采集到的网络流量数据进行挖掘，提取网络流量信息，形成网络审计记录。网络流量数据挖掘分析主要包括：邮件收发协议审计、网页浏览审计、文件共享审计、文件传输审计、远程访问审计等。其中文件传输审计主要针对（　　）协议。

A．SMTP

B．FTP

C．Telnet

D．HTTP

信管网参考答案：B

查看解析：www.cnitpm.com/st/5226824423.html

48、网络安全漏洞是网络安全管理工作的重要内容，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主要来源的是　（　　）

A．缓冲区溢出

B．输入验证错误

C．网络安全特权控制不完备

D．配置错误

信管网参考答案：C

查看解析：www.cnitpm.com/st/522697983.html

49、在 Linux 系统中，可用（　　）工具检查进程使用的文件、TCP／UDP 端口、用户等相关信息。

A．ps

B．lsof

C．top

D．pwck

信管网参考答案：B

查看解析：www.cnitpm.com/st/5227024855.html

50、计算机病毒是一组具有自我复制、传播能力的程序代码。常见的计算机病毒类型包括引导型病毒、宏病毒、多态病毒、隐蔽病毒等。磁盘杀手病毒属于（　　）。

A．引导型病毒

B．宏病毒

C．多态病毒

D．隐蔽病毒

信管网参考答案：A

查看解析：www.cnitpm.com/st/5227127305.html

51、网络蠕虫是恶意代码的一种类型，具有自我复制和传播能力，可以独立自动运行。网络蠕虫的四个功能模块包括（　　）。

A．扫描模块、感染模块、破坏模块、负载模块

B．探测模块、传播模换、蠕虫引擎模块、负载模块

C．扫描模块、传播模块、蠕虫引擎模块、破坏模块

D．探测模块、传播模块、负载模块、破坏模块

信管网参考答案：B

查看解析：www.cnitpm.com/st/522727239.html

52、入侵防御系统 IPS 的主要作用是过滤掉有害网络信息流，阻断入侵者对目标的攻击行为。IPS 的主要安全功能不包括（　　）。

A．屏蔽指定 IP 地址

B．屏蔽指定网络端口

C．网络物理隔离

D．屏蔽指定域名

信管网参考答案：C

查看解析：www.cnitpm.com/st/5227318744.html

53、隐私保护技术的目标是通过对隐私数据进行安全修改处理，使得修改后的数据可以公开发布而不会遭受隐私攻击。隐私保护的常见技术有抑制、泛化、置换、扰动、裁剪等。其中在数据发布时添加一定的噪声的技术属于(　　)。

A．抑制

B．泛化

C．置换

D．扰动

信管网参考答案：D

查看解析：www.cnitpm.com/st/52274841.html

54、为了保护个人信息安全，规范 App 的应用，国家有关部门已发布了《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（草案）》，其中，针对 Android 6.0 及以上可收集个人信息的权限，给出了服务类型的最小必要权限参考范围。根据该规范，具有位置权限的服务类型包括(　　)

A．网络支付、金融借贷

B．网上购物、即时通信

C．餐饮外卖、运动健身

D．问诊挂号、求职招聘

信管网参考答案：C

查看解析：www.cnitpm.com/st/5227510992.html

55、威胁效果是指威胁成功后，给网络系统造成的影响。电子邮件炸弹能使用户在很短的时间内收到大量电子邮件，严重时会使系统崩溃、网络瘫痪，该威胁属于(　　)。

A．欺骗

B．非法访问

C．拒绝服务

D．暴力破解

信管网参考答案：C

查看解析：www.cnitpm.com/st/5227617355.html

56、通过网络传播法律法规禁止的信息，炒作敏感问题并危害国家安全、社会稳定和公众利益的事件，属于（　　）。

A．信息内容安全事件

B．信息破坏事件

C．网络攻击事件

D．有害程序事件

信管网参考答案：A

查看解析：www.cnitpm.com/st/52277298.html

57、文件完整性检查的目的是发现受害系统中被篡改的文件或操作系统的内核是否被替换，对于Linux 系统，网络管理员可使用(　　)命令直接把系统中的二进制文件和原始发布介质上对应的文件进行比较。

A．who

B．find

C．arp

D．cmp

信管网参考答案：D

查看解析：www.cnitpm.com/st/522785103.html

58、入侵取证是指通过特定的软件和工具，从计算机及网络系统中提取攻击证据。以下网络安全取证步骤正确的是（　　）。

A．取证现场保护-证据识别-保存证据-传输证据-分析证据-提交证据

B．取证现场保护-证据识别-传输证据-保存证据-分析证据-提交证据

C．取证现场保护-保存证据-证据识别-传输证据-分析证据-提交证据

D．取证现场保护-证据识别-提交证据-传输证据-保存证据-分析证据

信管网参考答案：B

查看解析：www.cnitpm.com/st/5227922808.html

59、端口扫描的目的是找出目标系统上提供的服务列表。以下端口扫描技术中，需要第三方机器配合的是（　　）。

A．完全连接扫描

B．SYN 扫描

C．ID 头信息扫描

D．ACK 扫描

信管网参考答案：C

查看解析：www.cnitpm.com/st/522807413.html

60、安全渗透测试通过模拟攻击者对测评对象进行安全攻击，以验证安全防护机制的有效性。其中需要提供部分测试对象信息，测试团队根据所获取的信息，模拟不同级别的威胁者进行渗透测试，这属于（　　）。

A．黑盒测试

B．白盒测试

C．灰盒测试

D．盲盒测试

信管网参考答案：C

查看解析：www.cnitpm.com/st/5228114241.html

61、《计算机信息系统安全保护等级划分准则（GB 17859-1999）》规定，计算机信息系统安全保护能力分为五个等级，其中提供系统恢复机制的是(　　)。

A．系统审计保护级

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：D

查看解析：www.cnitpm.com/st/522829251.html

62、Android 是一个开源的移动终端操作系统，共分成 Linux 内核层、系统运行库层、应用程序框架层和应用程序层四个部分。显示驱动位于 （ ）。

A. Linux 内核层

B. 系统运行库层

C. 应用程序框架层

D. 应用程序层

信管网参考答案：A

查看解析：www.cnitpm.com/st/522834306.html

63、网络安全管理是对网络系统中网管对象的风险进行控制。给操作系统打补丁属于（ ）方法。

A. 避免风险

B. 转移风险

C. 减少风险

D. 消除风险

信管网参考答案：D

查看解析：www.cnitpm.com/st/522847715.html

64、日志文件是 Windows 系统中一个比较特殊的文件，它记录 Windows 系统的运行状况，如各种系统服务的启动、运行、关闭等信息。Windows 日志中，安全日志对应的文件名为（ ）。

A. SecEvent.evt

B. AppEvent.evt

C. SysEvent.evt

D. CybEvent.evt

信管网参考答案：A

查看解析：www.cnitpm.com/st/5228525497.html

65、最小化配置服务是指在满足业务的前提下，尽量关闭不需要的服务和网络端口，以减少系统潜在的安全危害。以下实现 Linux 系统网络服务最小化的操作，正确的是（ ）。

A. inetd.conf 的文件权限设置为 644

B. services 的文件权限设置为 600

C. inetd.conf 的文件属主为 root

D. 关闭与系统业务运行有关的网络通信端口

信管网参考答案：C

查看解析：www.cnitpm.com/st/52286269.html

66、数据库脱敏是指利用数据脱敏技术将数据库中的数据进行变换处理，在保持数据按需使用目标的同时，又能避免敏感数据外泄。以下技术中，不属于数据脱敏技术的是（　　）。

A. 屏蔽

B. 变形

C. 替换

D. 访问控制

信管网参考答案：D

查看解析：www.cnitpm.com/st/522872170.html

67、Oracle 数据库提供认证、访问控制、特权管理、透明加密等多种安全机制和技术。以下关于 Oracle 数据库表述，错误的是（　　）。

A. Oracle 数据库的认证方式采用“用户名＋口令”的方式

B. Oracle 数据库不支持三方认证

C. Oracle 数据库具有口令加密和复杂度验证等安全功能

D. Oracle 数据库提供细粒度访问控制

信管网参考答案：B

查看解析：www.cnitpm.com/st/5228821589.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。交换机根据功能变化分为五代，其中第二代交换机又称为以太网交换机，其工作于 OSI（开放系统互连参考模型）的（　　）。

A. 物理层

B. 数据链路层

C. 网络层

D. 应用层

信管网参考答案：B

查看解析：www.cnitpm.com/st/5228911774.html

69、Apache Httpd 是一个用于搭建 Web 服务器的开源软件。Apache Httpd 配置文件中，负责基本读取文件控制的是（ ）。

A. httpd.conf

B. srm.conf

C. access.conf

D. mime.conf

信管网参考答案：C

查看解析：www.cnitpm.com/st/522904931.html

70、口令是保护路由器安全的有效方法，一旦口令信息泄露就会危及路由器安全。因此，路由器的口令存放应是密文。在路由器配置时，使用（ ）命令保存口令密文。

A. Enable secret

B. key chain

C. key-string

D. no ip finger

信管网参考答案：A

查看解析：www.cnitpm.com/st/5229114195.html

71~75、 Methods for (71)people differ significantly from those for authenticating machines and programs, and this is because of the major differences in the capabilities of people versus computers.Computers are great at doing(72) calculations quickly and correctly, and they have large memories into which they can store and later retrieve Gigabytes of information. Humans don't. So we need to use different methods to

authenticate people. In particular, the(73) protocols we've already discussed are not well suited if the principal being authenticated is a person (with all the associated limitations).

All approaches for human authentication rely on at least one of the followings:

Something you know (eg. a password).This is the most common kind of authentication used for humans.We use passwords every day to access our systems. Unfortunately,something that you know can become something you just forgot. And if you write it down, then other people might find it.

Something you(74)(eg.a smart card).This form of human authentication removes the problem of forgetting something you know, but some object now must be with you any time you want to be authenticated. And such an object might be stolen and then becomes something the attacker has.

Something you are (eg. a fingerprint).Base authentication on something (75)to the principal being authenticated. It's much harder to lose a fingerprint than a wallet. Unfortunately,biometric sensors are fairly expensive and (at present) not very accurate.

71、（）

A. authenticating

B. authentication

C. authorizing

D. authorization

72、（）

A. much

B. huge

C. large

D. big

73、（）

A. network

B. cryptographic

C. communication

D. security

74、（）

A. are

B. have

C. can

D. owned

75、（）

A. unique

B. expensive

C. important

D. intrinsic

信管网参考答案：A、C、B、B、D

查看解析：www.cnitpm.com/st/5229210411.html