# 1.通用标准v2版（CC）的安全等级是以EAL来表示的。( )

A、正确

B、错误

**正确答案：** A

# 2.在信息安全领域，CIA通常是指：保密性、完整性和可用性。( )

A、正确

B、错误

**正确答案：** A

# 3.信息安全的威胁主体包括内部人员、准内部人员、外部人员、系统自身等方面。( )

A、正确

B、错误

**正确答案：** B

# 4.安全审计是从管理和技术两个方面检查公司的安全策略和控制措施的执行情况，发现安全隐患的过程。( )

A、正确

B、错误

**正确答案：** A

# 5.计算机系统安全是指应用系统具备访问控制机制，数据不被泄露、丢失、篡改等。( )

A、正确

B、错误

**正确答案：** B

# 6.黑客在进行信息收集时，通常利用Windows的IPC漏洞可以获得系统用户的列表的信 息。( )

A、正确

B、错误

**正确答案：** A

# 7.HP-UX系统加固中在设置ROOT环境变量不能有相对路径设置。( )

A、正确

B、错误

**正确答案：** A

# 8.AIX系统加固时，对系统配置一般需要自编脚本完成。( )

A、正确

B、错误

**正确答案：** A

# 9.操作系统普通用户账号审批记录应编号、留档。( )

A、正确

B、错误

**正确答案：** A

# 10.主机系统加固时根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。( )

A、正确

B、错误

**正确答案：** A

# 11.4A系统的接入管理可以管理到用户无力访问的接入。( )

A、正确

B、错误

**正确答案：** B

# 12.Cisco设备的AUX端口默认是启用的。( )

A、正确

B、错误

**正确答案：** A

# 13.Inbound方向的NAT使用一个外部地址来代表内部地址，用于隐藏外网服务器的实际IP地址。( )

A、正确

B、错误

**正确答案：** B

# 14.IPS的过滤器规则不能自由定义。( )

A、正确

B、错误

**正确答案：** B

# 15.IPS和IDS都是主动防御系统。( )

A、正确

B、错误

**正确答案：** B

# 16.Netscreen的ROOT管理员具有的最高权限，为了避免ROOT管理员密码被窃取后造成威胁，应该限制ROOT只能通过CONSOLE接口访问设备，而不能远程登录。( )

A、正确

B、错误

**正确答案：** A

# 17.OSI是开放的信息安全的缩写。( )

A、正确

B、错误

**正确答案：** B

# 18.OSI中会话层不提供机密性服务。( )

A、正确

B、错误

**正确答案：** A

# 19.TCP/IP模型从下至上分为四层：物理层，数据链路层，网络层和应用层。( )

A、正确

B、错误

**正确答案：** B

# 20.TCP/IP协议体系结构中，IP层对应OSI/RM模型的网络层。( )

A、正确

B、错误

**正确答案：** A

# 21.缺省情况下，防火墙工作模式为路由模式，切换工作模式后可直接进行进一步配置。( )

A、正确

B、错误

**正确答案：** B

# 22.入侵检测可以处理数据包级的攻击。( )

A、正确

B、错误

**正确答案：** B

# 23.统计分析的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。( )

A、正确

B、错误

**正确答案：** B

# 24.透明代理服务器在应用层工作，它完全阻断了网络报文的传输通道。因此具有很高的安全性。可以根据协议、地址等属性进行访问控制、隐藏了内部网络结构，因为最终请求是有防火墙发出的。外面的主机不知道防火墙内部的网络结构。解决IP地址紧缺的问题。使用代理服务器只需要给防火墙设置一个公网的IP的地址。( )

A、正确

B、错误

**正确答案：** A

# 25.网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。( )

A、正确

B、错误

**正确答案：** B

# 26.针对不同的攻击行为，IPS只需要一个过滤器就足够了。( )

A、正确

B、错误

**正确答案：** B

# 27.状态检测防火墙检测每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。( )

A、正确

B、错误

**正确答案：** B

# 28.防火墙安全策略定制越多的拒绝规则，越有利于网络安全。( )

A、正确

B、错误

**正确答案：** B

# 29.侵检测的手机的被容包括系统、网络、数据及用户活动的状态和行为。( )

A、正确

B、错误

**正确答案：** A

# 30.入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。( )

A、正确

B、错误

**正确答案：** A

# 31.传输层协议使用端口号（Port）来标示和区分上层应用程序，如：Telnet协议用的是23号端口、DNS协议使用69号端口。( )

A、正确

B、错误

**正确答案：** B

# 32.如果Web应用没有对攻击者的输入进行适当的编码和过滤，就用于构造数据库查询或操作系统命令时，可能导致注入漏洞。( )

A、正确

B、错误

**正确答案：** A

# 33.HTTP协议是文本协议，可利用回车换行做边界干扰。( )

A、正确

B、错误

**正确答案：** A

# 34.Mysqldump是采用SQL级别的备份机制，它将数据表导成SQL脚本文件，在不同的MySQL版本之间升级时相对比较合适，这也是最常见的备份方法。( )

A、正确

B、错误

**正确答案：** A

# 35.Oracle的SYS账户在数据库中具有最高权限，能够做任何事情，包括启动/关闭Oracle数据库。即使SYS被锁定，也已然能够访问数据库。( )

A、正确

B、错误

**正确答案：** A

# 36.Oracle默认情况下，口令的传输方式是加密。( )

A、正确

B、错误

**正确答案：** B

# 37.OSI网络安全体系结构的八类安全机制分别是加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公正。( )

A、正确

B、错误

**正确答案：** A

# 38.SQL Server数据库应禁止使用除tcp/ip以外的协议，保护数据库通信安全。( )

A、正确

B、错误

**正确答案：** A

# 39.Web应用对网络通讯中包含的敏感信息进行加密，就不会被窃听。( )

A、正确

B、错误

**正确答案：** B

# 40.对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是DNS服务器。( )

A、正确

B、错误

**正确答案：** B

# 41.访问控制、强制登陆、自动安全更新都属于Window2000的安全组件( )

A、正确

B、错误

**正确答案：** B

# 42.攻击者可以通过SQL注入手段获取其他用户的密码。( )

A、正确

B、错误

**正确答案：** A

# 43.简单身份验证和安全层（Simple Authentication and Security Layer，SASL）是一种为系统账号提供身份验证和可选安全性服务的框架( )

A、正确

B、错误

**正确答案：** B

# 44.如果sa是空口令，那就意味着攻击者可能侵入系统执行任意操作，威胁系统安全。( )

A、正确

B、错误

**正确答案：** A

# 45.网络拓扑分析为检查是否有配置错误项泄露内部IP地址，从而推断网站系统拓扑。( )

A、正确

B、错误

**正确答案：** A

# 46.为了维护数据库中数据的正确性和一致性，在对关系数据库执行插入、删除和修改操作时必须遵循三类完整性规则：实体完整性规则、引用完整性规则、用户定义的完整性规则。( )

A、正确

B、错误

**正确答案：** A

# 47.系统漏洞扫描为检查目标的操作系统与应用系统信息。( )

A、正确

B、错误

**正确答案：** B

# 48.一封电子邮件可以拆分成对个IP包，每个IP包可以沿不同的路径到达目的地。( )

A、正确

B、错误

**正确答案：** A

# 49.用Sqlplus登陆到Oracle数据库，使用slesct username, password form dba\_users命令可查看数据库中的用户名和密码明文。( )

A、正确

B、错误

**正确答案：** B

# 50.在Oracle所有版本在安装的时候都没有提示修改SYS的默认密码。( )

A、正确

B、错误

**正确答案：** B

# 51.在SQL Server安装SP3补丁时不需要系统中已经安装了SP1或SP2。( )

A、正确

B、错误

**正确答案：** B

# 52.Oracle默认配置下，每个账户如果有30次的失败登陆，此账户将被锁定。( )

A、正确

B、错误

**正确答案：** B

# 53.对MySQL注入攻击时，经常用到注释符号#来屏蔽剩下的内置SQL语句。( )

A、正确

B、错误

**正确答案：** A

# 54.Web错误信息可能泄露服务器型号版本、数据库型号、路径、代码。( )

A、正确

B、错误

**正确答案：** A

# 55.产品的定制开发是应用安全中最薄弱的一环。( )

A、正确

B、错误

**正确答案：** A

# 56.网上营业厅对资源控制制的要求包括：应用软件对访问用户进行记录，当发现相同用户二次进行登录和操作，系统将要求二次认证，验证通过后提供服务。( )

A、正确

B、错误

**正确答案：** B

# 57.EMC测试盒约束用户关心的信息信号的电磁发射、TEMPEST只测试盒约束系统和设备的所有电磁发射。( )

A、正确

B、错误

**正确答案：** B

# 58.出现在导线或电器、电子设备上的超过线路或设备本身正常工作电压和电流并对线路或设备可能造成电气损害的电压和电流，称过电压和过电流。( )

A、正确

B、错误

**正确答案：** B

# 59.机房应设置相应的活在报警和灭火系统。( )

A、正确

B、错误

**正确答案：** A

# 60.计算机系统接地包括：直流地、交流工作地、安全保护地、电源零线和防雷保护地。( )

A、正确

B、错误

**正确答案：** B

# 61.提到防雷，大家很容易联想到避雷针。其实我们平常看到的避雷针是用来保护房屋免遭雷电直击即防直击雷的。计算机信息系统的电子设备雷害一般有感应雷击产生，英因此防护的方法完全不一样。( )

A、正确

B、错误

**正确答案：** A

# 62.只要手干净就可以直接触摸或者插拔电路组件，不必有进一步的措施。( )

A、正确

B、错误

**正确答案：** B

# 63.防雷措施是在和计算机连接的所有外线上（包括电源线和通信线）加设专用防雷设备——防雷保安器，同时规范底线，防止雷击时在底线上产生的高电位反击。( )

A、正确

B、错误

**正确答案：** A

# 64.信息网络的物理安全要从环境安全和设备安全两个角度来考虑。( )

A、正确

B、错误

**正确答案：** A

# 65.为防止信息非法泄露，需要销毁存储介质时，应该批准后自行销毁。( )

A、正确

B、错误

**正确答案：** B

# 66.机密信息纸介质资料废弃应用碎纸机粉碎或焚毁。( )

A、正确

B、错误

**正确答案：** A

# 67.“一次一密”属于序列密码的一种。( )

A、正确

B、错误

**正确答案：** A

# 68.DES3和RSA是两种不同的安全加密算法，主要是用来对敏感数据进行安全加密。( )

A、正确

B、错误

**正确答案：** A

# 69.DSS(Digital Signature Standard)是利用了安全散列函数（SHA）提出了一种数字加密技术。( )

A、正确

B、错误

**正确答案：** A

# 70.PGP协议缺省的压缩算法是ZIP，压缩后数据由于冗余信息很少，更容易抵御来自分析类型的攻击。( )

A、正确

B、错误

**正确答案：** A

# 71.RC4是典型的的序列密码算法。( )

A、正确

B、错误

**正确答案：** A

# 72.安全全加密技术分为两大类：对称加密技术和非对称加密技术。两者的主要区别是对称加密算法在加密、解密过程中使用同一个秘钥；而非对称加密算法在加密、解密过程中使用两个不同的秘钥。( )

A、正确

B、错误

**正确答案：** A

# 73.当通过浏览器一在线方式申请数字证书时，申请证书和下载证书的计算机必须是同一台计算机。( )

A、正确

B、错误

**正确答案：** A

# 74.分组密码的优点是错误扩展小、速度快、安全程度高。( )

A、正确

B、错误

**正确答案：** B

# 75.古典加密主要采用的主要方法是置换，代换。( )

A、正确

B、错误

**正确答案：** A

# 76.基于公开秘钥体制（PKI）的数字证书是电子商务安全体系的核心。( )

A、正确

B、错误

**正确答案：** A

# 77.链路加密方式适用于在广域网系统中应用。( )

A、正确

B、错误

**正确答案：** B

# 78.日常所见的校园饭卡是利用身份认证的单因素法。( )

A、正确

B、错误

**正确答案：** A

# 79.身份认证与权限控制是网络社会的管理基础。( )

A、正确

B、错误

**正确答案：** A

# 80.数字签名比较的是摘要结果长度是否都是128位。( )

A、正确

B、错误

**正确答案：** B

# 81.文件压缩变换是一个单向加密过程。( )

A、正确

B、错误

**正确答案：** B

# 82.以当前的技术来说，RSA体制是无条件安全的。( )

A、正确

B、错误

**正确答案：** B

# 83.在PKI中，注册机构RA是必要的组件。( )

A、正确

B、错误

**正确答案：** B

# 84.在密码学的意义上，只要存在一个方向，比暴力搜索秘钥还要更有效率，就能视为一种“破解”。 ( )

A、正确

B、错误

**正确答案：** A

# 85.整个PKI系统有证书服务器AS、票据许可服务器TGS、客户机和应用服务器四部分组成。 ( )

A、正确

B、错误

**正确答案：** B

# 86.最小特权、纵深防御是网络安全原则之一。( )

A、正确

B、错误

**正确答案：** A

# 87.数字证书是由权威机构PKI发行的一种权威性的电子文档，是网络环境中的一种身份证。 ( )

A、正确

B、错误

**正确答案：** B

# 88.病毒能隐藏在电脑的CMOS存储器里。( )

A、正确

B、错误

**正确答案：** B

# 89.已知某应用程序感染了文件型病毒，则该文件的大小变化情况一般是变小。( )

A、正确

B、错误

**正确答案：** B

# 90.专业安全评估服务对目标系统通过工具扫描和人工检查，进行专业安全的技术评定，并根据评估结果提供评估报告。 ( )

A、正确

B、错误

**正确答案：** A

# 91.HTTPS可以完全保证Web应用的安全性。

A、正确

B、错误

**正确答案：** B

# 92.跨站请求伪造（CSRF）攻击可以通过在Web页面中使用验证码来防止。

A、正确

B、错误

**正确答案：** B

# 93.在Web应用中使用安全的编码实践可以有效防止SQL注入攻击。

A、正确

B、错误

**正确答案：** A

# 94.操作系统级别的防火墙可以防止Web应用攻击。

A、正确

B、错误

**正确答案：** B

# 95.应用程序级别的防火墙可以防止Web应用攻击。

A、正确

B、错误

**正确答案：** A

# 96.数据库级别的防火墙可以防止Web应用攻击。

A、正确

B、错误

**正确答案：** A

# 97.安全编码标准是一种指南，用于帮助开发人员编写安全的Web应用代码。

A、正确

B、错误

**正确答案：** A

# 98.使用最新的安全技术和最佳实践可以提高Web应用的安全性。

A、正确

B、错误

**正确答案：** A

# 99.动态SQL语句容易受到SQL注入攻击，而静态SQL语句不会受到攻击。

A、正确

B、错误

**正确答案：** B

# 100.在Web应用中使用预编译的SQL语句（如 Prepared Statements 或 Parameterized Queries）可以防止SQL注入攻击。

A、正确

B、错误

**正确答案：** A

# 101.对用户输入进行严格的验证和过滤可以有效防止SQL注入攻击。

A、正确

B、错误

**正确答案：** A

# 102.数据库用户权限越高，Web应用越容易受到SQL注入攻击。

A、正确

B、错误

**正确答案：** A

# 103.使用 ORMs（对象关系映射）可以完全避免SQL注入攻击。

A、正确

B、错误

**正确答案：** B

# 104.在Web应用中，SQL注入攻击通常通过输入框、搜索框等输入接口进行。

A、正确

B、错误

**正确答案：** A

# 105.限制数据库操作的频率可以防止SQL注入攻击造成的严重后果。

A、正确

B、错误

**正确答案：** A

# 106.数据库加密可以防止SQL注入攻击。

A、正确

B、错误

**正确答案：** B

# 107.大部分SQL注入攻击都是通过自动化工具进行的。

A、正确

B、错误

**正确答案：** A

# 108.安全审计可以发现SQL注入漏洞。

A、正确

B、错误

**正确答案：** A

# 109.避免使用管理员权限运行数据库操作可以防止SQL注入攻击。

A、正确

B、错误

**正确答案：** A

# 110.数据库注入漏洞测试是Web应用安全测试的一部分。

A、正确

B、错误

**正确答案：** A

# 111.针对特定数据库的SQL注入攻击更难防御。

A、正确

B、错误

**正确答案：** A

# 112.及时更新和修补Web应用和数据库系统可以降低SQL注入攻击的风险。

A、正确

B、错误

**正确答案：** A

# 113.XSS攻击是指攻击者通过在Web页面中插入恶意脚本，窃取用户信息或对其他用户造成伤害的一种攻击方式。

A、正确

B、错误

**正确答案：** A

# 114.XSS攻击只能在客户端执行，因此服务器端无法受到此类攻击。

A、正确

B、错误

**正确答案：** B

# 115.存储型XSS攻击发生在Web应用将恶意脚本存储在服务器上，如数据库、消息论坛、访客留言板等。

A、正确

B、错误

**正确答案：** A

# 116.反射型XSS攻击发生在恶意脚本通过URL、电子邮件或其他方式从服务器反射到客户端执行。

A、正确

B、错误

**正确答案：** A

# 117.DOM-based XSS攻击是存储型和反射型XSS攻击的综合，主要利用DOM解析漏洞执行恶意脚本。

A、正确

B、错误

**正确答案：** A

# 118.跨站脚本攻击（XSS）和跨站请求伪造（CSRF）是两种不同的攻击方式，它们的攻击目标和原理都不相同。

A、正确

B、错误

**正确答案：** A

# 119.对用户输入进行严格的验证和编码可以有效防止XSS攻击。

A、正确

B、错误

**正确答案：** A

# 120.浏览器自带的防御机制可以完全防止XSS攻击。

A、正确

B、错误

**正确答案：** B

# 121.在Web应用中，避免使用客户端脚本可以防止XSS攻击。

A、正确

B、错误

**正确答案：** B

# 122.在Web应用中，对客户端脚本进行内容安全策略可以防止XSS攻击。

A、正确

B、错误

**正确答案：** A

# 123.XSS攻击主要针对Web应用的客户端，因此与服务器端语言无关。

A、正确

B、错误

**正确答案：** B

# 124.避免在Web应用中使用动态渲染技术可以防止XSS攻击。

A、正确

B、错误

**正确答案：** B

# 125.及时更新和修补Web应用可以降低XSS攻击的风险。

A、正确

B、错误

**正确答案：** A

# 126.CSRF攻击是一种利用用户已登录状态，诱导用户访问恶意网站从而执行非法操作的攻击方式。

A、正确

B、错误

**正确答案：** A

# 127.CSRF攻击主要针对Web应用，且攻击者无需知道用户的密码即可实施攻击。

A、正确

B、错误

**正确答案：** A

# 128.防止CSRF攻击的有效方法之一是在HTTP请求中添加一个唯一的令牌（如Token），并在服务器端验证该令牌。

A、正确

B、错误

**正确答案：** A

# 129.只有在用户登录后，才需要担心CSRF攻击。

A、正确

B、错误

**正确答案：** B

# 130.验证HTTP Origin头可以有效防止CSRF攻击。

A、正确

B、错误

**正确答案：** A

# 131.在Web应用中，攻击者可以利用图片标签的src属性实施CSRF攻击。

A、正确

B、错误

**正确答案：** A

# 132.在Web应用中，对所有涉及敏感操作的请求添加验证标记可以防止CSRF攻击。

A、正确

B、错误

**正确答案：** A

# 133.在Web应用中，上传的文件名应该进行过滤和转义，以避免文件名包含特殊字符。

A、正确

B、错误

**正确答案：** A

# 134.在Web应用中，上传的文件应该进行适当的处理和验证，以确保文件的安全性。

A、正确

B、错误

**正确答案：** A

# 135.在Web应用中，上传的文件应该进行MD5或SHA1哈希值检查，以防止恶意文件上传。

A、正确

B、错误

**正确答案：** A

# 136.在Web应用中，上传的文件应该进行访问控制，限制文件的访问权限和操作。

A、正确

B、错误

**正确答案：** A

# 137.浏览器自带的防御机制可以完全防止文件上传漏洞。

A、正确

B、错误

**正确答案：** B

# 138.及时更新和修补Web应用可以降低文件上传漏洞的风险。

A、正确

B、错误

**正确答案：** A

# 139.客户端安全主要关注保护用户的设备和应用程序免受恶意软件和攻击的侵害。

A、正确

B、错误

**正确答案：** A

# 140.浏览器扩展可以增强浏览器的安全性，但也可能引入安全风险。

A、正确

B、错误

**正确答案：** A

# 141.客户端安全包括防范病毒、恶意软件、钓鱼攻击等多种威胁。

A、正确

B、错误

**正确答案：** A

# 142.操作系统自带的防火墙可以有效防止客户端安全威胁。

A、正确

B、错误

**正确答案：** A

# 143.安装杀毒软件可以提高客户端的安全性。

A、正确

B、错误

**正确答案：** A

# 144.定期更新操作系统和应用程序可以减少安全漏洞。

A、正确

B、错误

**正确答案：** A

# 145.使用强密码可以防止未授权访问客户端账户。

A、正确

B、错误

**正确答案：** A

# 146.双因素认证可以提供额外的安全层，防止恶意登录。

A、正确

B、错误

**正确答案：** A

# 147.客户端安全与服务器端安全同等重要。

A、正确

B、错误

**正确答案：** A

# 148.HTTPS可以完全保证客户端安全。

A、正确

B、错误

**正确答案：** B

# 149.使用VPN可以提高客户端数据传输的安全性。

A、正确

B、错误

**正确答案：** A

# 150.客户端安全策略应包括定期备份重要数据。

A、正确

B、错误

**正确答案：** A

# 151.安全配置客户端设备可以减少安全风险。

A、正确

B、错误

**正确答案：** A

# 152.用户教育是提高客户端安全性的关键因素。

A、正确

B、错误

**正确答案：** A

# 153.客户端安全威胁只会来自外部 sources。

A、正确

B、错误

**正确答案：** B

# 154.浏览器安全是指保护浏览器免受恶意网站、钓鱼攻击和恶意软件侵害的措施。

A、正确

B、错误

**正确答案：** A

# 155.浏览器扩展可以增强浏览器的功能，但同时也可能引入安全风险。

A、正确

B、错误

**正确答案：** A

# 156.浏览器安全主要关注保护用户的个人数据和隐私。

A、正确

B、错误

**正确答案：** A

# 157.浏览器自带的隐私模式可以完全保护用户的浏览历史和数据。

A、正确

B、错误

**正确答案：** B

# 158.HTTPS可以保证浏览器安全，因为它加密了数据传输。

A、正确

B、错误

**正确答案：** A

# 159.浏览器安全漏洞主要来源于浏览器本身的不安全设计。

A、正确

B、错误

**正确答案：** B

# 160.浏览器脚本可以读取和修改本地文件，这可能导致安全风险。

A、正确

B、错误

**正确答案：** A

# 161.浏览器插件可能成为攻击者的攻击媒介。

A、正确

B、错误

**正确答案：** A

# 162.定期更新浏览器可以减少安全漏洞。

A、正确

B、错误

**正确答案：** A

# 163.使用强密码可以防止未授权访问浏览器账户。

A、正确

B、错误

**正确答案：** A

# 164.浏览器安全与客户端安全是不同的概念。

A、正确

B、错误

**正确答案：** B

# 165.浏览器安全策略应包括定期备份重要数据。

A、正确

B、错误

**正确答案：** A

# 166.安全配置浏览器可以减少安全风险。

A、正确

B、错误

**正确答案：** A

# 167.用户教育是提高浏览器安全性的关键因素。

A、正确

B、错误

**正确答案：** A

# 168.浏览器安全威胁只会来自外部 sources。

A、正确

B、错误

**正确答案：** B

# 169.安全编码规范可以提高浏览器的安全性。

A、正确

B、错误

**正确答案：** A

# 170.移动应用安全是指保护移动应用程序及其用户数据免受恶意软件和攻击的侵害。

A、正确

B、错误

**正确答案：** A

# 171.移动应用安全包括防范病毒、恶意软件、钓鱼攻击等多种威胁。

A、正确

B、错误

**正确答案：** A

# 172.移动操作系统自带的安全功能可以完全保护移动应用安全。

A、正确

B、错误

**正确答案：** B

# 173.安装移动安全应用程序可以提高移动设备的安全性。

A、正确

B、错误

**正确答案：** A

# 174.移动应用安全与客户端安全是不同的概念。

A、正确

B、错误

**正确答案：** B

# 175.HTTPS可以保证移动应用数据传输的安全性。

A、正确

B、错误

**正确答案：** A

# 176.移动应用的安全漏洞可能来源于不安全的编程实践。

A、正确

B、错误

**正确答案：** A

# 177.移动应用的隐私政策应该明确说明哪些数据会被收集和使用。

A、正确

B、错误

**正确答案：** A

# 178.移动应用应该使用安全的API进行数据存储和传输。

A、正确

B、错误

**正确答案：** A

# 179.移动应用应该实现适当的身份验证和授权机制。

A、正确

B、错误

**正确答案：** A

# 180.移动应用安全策略应包括定期备份重要数据。

A、正确

B、错误

**正确答案：** A

# 181.安全配置移动设备可以减少安全风险。

A、正确

B、错误

**正确答案：** A

# 182.DES是最典型的对称加密算法。

A、正确

B、错误

**正确答案：** A

# 183.AES（高级加密标准）是目前广泛使用的对称加密算法。

A、正确

B、错误

**正确答案：** A

# 184.在对称加密中，密钥交换是一个难题。

A、正确

B、错误

**正确答案：** B

# 185.使用对称加密时，密钥的安全存储和传输至关重要。

A、正确

B、错误

**正确答案：** A

# 186.对称加密可以用于保护敏感数据，如个人隐私和商业机密。

A、正确

B、错误

**正确答案：** A

# 187.对称加密可以用于加密大量数据。

A、正确

B、错误

**正确答案：** A

# 188.对称加密的优点是加密和解密速度快，但缺点是密钥管理复杂。

A、正确

B、错误

**正确答案：** A

# 189.安全套接层（SSL）和传输层安全性（TLS）协议使用对称加密来保护数据传输。

A、正确

B、错误

**正确答案：** A

# 190.对称加密的密钥可以通过安全通道生成和交换。

A、正确

B、错误

**正确答案：** A

# 191.在对称加密中，相同的密钥用于加密和解密数据。

A、正确

B、错误

**正确答案：** A

# 192.使用强密码学算法和足够长的密钥可以提高对称加密的安全性。

A、正确

B、错误

**正确答案：** A

# 193.对称加密不适用于密钥分发困难的场景。

A、正确

B、错误

**正确答案：** A

# 194.对称加密是现代加密体系结构的基础之一。

A、正确

B、错误

**正确答案：** A

# 195.RSA是最典型的非对称加密算法。

A、正确

B、错误

**正确答案：** A

# 196.公钥和私钥是非对称加密中的两个关键密钥。

A、正确

B、错误

**正确答案：** A

# 197.公钥用于加密数据，私钥用于解密数据。

A、正确

B、错误

**正确答案：** A

# 198.公钥基础设施（PKI）是非对称加密中常用的密钥管理方案。

A、正确

B、错误

**正确答案：** A

# 199.哈希函数是将输入数据（或消息）转换为固定大小的字符串的函数。

A、正确

B、错误

**正确答案：** A

# 200.哈希函数的输出称为哈希值或哈希码。

A、正确

B、错误

**正确答案：** A

# 201.哈希函数的特点是输入数据的微小变化会导致输出哈希值的巨大变化。

A、正确

B、错误

**正确答案：** A

# 202.哈希函数的输出长度通常小于输入长度。

A、正确

B、错误

**正确答案：** A

# 203.MD5是一种常用的哈希函数。

A、正确

B、错误

**正确答案：** A

# 204.SHA-1是一种安全的哈希函数。

A、正确

B、错误

**正确答案：** B

# 205.SHA-256是一种比SHA-1更安全的哈希函数。

A、正确

B、错误

**正确答案：** A

# 206.哈希函数可以用于数据完整性校验。

A、正确

B、错误

**正确答案：** A

# 207.哈希函数可以用于生成数字签名。

A、正确

B、错误

**正确答案：** A

# 208.哈希函数的输出是唯一的，不同的输入数据不会产生相同的输出。

A、正确

B、错误

**正确答案：** A

# 209.哈希函数的输出称为散列值。

A、正确

B、错误

**正确答案：** A

# 210.哈希函数可以用于数据索引。

A、正确

B、错误

**正确答案：** A

# 211.哈希函数可以用于数据检索。

A、正确

B、错误

**正确答案：** A

# 212.哈希函数的计算时间是固定的，与输入数据的大小无关。

A、正确

B、错误

**正确答案：** B

# 213.彩虹表是一种利用哈希函数进行密码破解的工具。

A、正确

B、错误

**正确答案：** A

# 214.哈希函数可以抵抗碰撞攻击。

A、正确

B、错误

**正确答案：** B

# 215.碰撞是指两个不同的输入数据产生相同的哈希值。

A、正确

B、错误

**正确答案：** A

# 216.哈希函数的设计目标是尽可能减少碰撞的可能性。

A、正确

B、错误

**正确答案：** A

# 217.哈希函数可以分为单向哈希函数和双向哈希函数。

A、正确

B、错误

**正确答案：** A

# 218.双向哈希函数既可以进行加密也可以进行解密。

A、正确

B、错误

**正确答案：** A

# 219.数字签名用于验证信息的完整性和来源，但不涉及认证和授权。

A、正确

B、错误

**正确答案：** B

# 220.密码学认证是基于密码学方法验证用户身份的过程。

A、正确

B、错误

**正确答案：** A

# 221.生物特征认证使用用户的生物特征（如指纹、虹膜）来验证身份。

A、正确

B、错误

**正确答案：** A

# 222.令牌认证是一种基于令牌（如智能卡、USB令牌）的认证方式。

A、正确

B、错误

**正确答案：** A

# 223.基于角色的访问控制（RBAC）是一种将用户分配给不同角色的方法，以控制他们对资源的访问。

A、正确

B、错误

**正确答案：** A

# 224.数字签名认证可以确保信息来自指定的发送方。

A、正确

B、错误

**正确答案：** A

# 225.数字签名认证可以确保信息在传输过程中未被篡改。

A、正确

B、错误

**正确答案：** A

# 226.密码学认证通常涉及使用密码或其他秘密信息来验证身份。

A、正确

B、错误

**正确答案：** A

# 227.生物特征认证是一种不可伪造的认证方式，因为生物特征是唯一的。

A、正确

B、错误

**正确答案：** A

# 228.基于角色的访问控制可以灵活地管理用户对资源的访问权限。

A、正确

B、错误

**正确答案：** A

# 229.数字签名认证可以用于确保信息的安全性和完整性。

A、正确

B、错误

**正确答案：** A

# 230.密码学认证可以用于确保用户身份的安全传输。

A、正确

B、错误

**正确答案：** A

# 231.生物特征认证可以用于提供高度的安全性，但也可能存在隐私问题。

A、正确

B、错误

**正确答案：** A

# 232.令牌认证可以用于提供安全的远程访问。

A、正确

B、错误

**正确答案：** A

# 233.基于角色的访问控制可以简化权限管理。

A、正确

B、错误

**正确答案：** A

# 234.数字签名认证可以用于电子邮件和文档的安全传输。

A、正确

B、错误

**正确答案：** A

# 235.密码学认证可以用于网络登录和交易验证。

A、正确

B、错误

**正确答案：** A

# 236.生物特征认证可以用于移动设备和智能卡的验证。

A、正确

B、错误

**正确答案：** A

# 237.令牌认证可以用于在线服务和云资源的访问控制。

A、正确

B、错误

**正确答案：** A

# 238.基于角色的访问控制可以与令牌认证结合使用，以提供双重验证。

A、正确

B、错误

**正确答案：** A

# 239.数字签名认证可以确保信息的真实性和可靠性。

A、正确

B、错误

**正确答案：** A

# 240.密码学认证可以用于保护用户密码的安全传输。

A、正确

B、错误

**正确答案：** A

# 241.生物特征认证可以用于替代传统的密码和PIN码。

A、正确

B、错误

**正确答案：** A

# 242.令牌认证可以用于验证用户对特定服务的访问权限。

A、正确

B、错误

**正确答案：** A

# 243.基于角色的访问控制可以应用于组织内的不同部门和团队。

A、正确

B、错误

**正确答案：** A

# 244.数字签名认证可以用于验证数字文档的真实性。

A、正确

B、错误

**正确答案：** A

# 245.生物特征认证可以用于提供安全的身份验证方法，但也需要考虑隐私和数据保护问题。

A、正确

B、错误

**正确答案：** A

# 246.数字签名认证可以防止重放攻击。

A、正确

B、错误

**正确答案：** A

# 247.密码学认证仅依赖于密码的保密性。

A、正确

B、错误

**正确答案：** B

# 248.生物特征认证容易受到仿冒攻击。

A、正确

B、错误

**正确答案：** B

# 249.令牌认证需要用户携带物理设备，不便于移动使用。

A、正确

B、错误

**正确答案：** B

# 250.基于角色的访问控制可以很容易地适应组织结构的变化。

A、正确

B、错误

**正确答案：** A

# 251.数字签名认证可以用于验证软件和固件的真实性。

A、正确

B、错误

**正确答案：** A

# 252.生物特征认证可以用于无人值守的自动服务设施。

A、正确

B、错误

**正确答案：** A

# 253.令牌认证可以用于提供动态访问权限。

A、正确

B、错误

**正确答案：** A

# 254.基于角色的访问控制可以降低安全管理的复杂性。

A、正确

B、错误

**正确答案：** A

# 255.密码学认证可以用于创建安全的通信通道。

A、正确

B、错误

**正确答案：** A

# 256.生物特征认证可以用于提供高度安全的身份验证。

A、正确

B、错误

**正确答案：** A

# 257.令牌认证可以用于实现快速的用户登录。

A、正确

B、错误

**正确答案：** A

# 258.基于角色的访问控制可以应用于云服务和虚拟环境。

A、正确

B、错误

**正确答案：** A

# 259.数字签名认证可以确保消息的不可否认性。

A、正确

B、错误

**正确答案：** A

# 260.生物特征认证可以用于提高用户体验，因为不需要记住密码。

A、正确

B、错误

**正确答案：** A

# 261.令牌认证可以用于实现单点登录。

A、正确

B、错误

**正确答案：** A

# 262.基于角色的访问控制可以与其他安全控制措施结合使用。

A、正确

B、错误

**正确答案：** A

# 263.密码学认证可以用于防止未授权访问。

A、正确

B、错误

**正确答案：** A

# 264.生物特征认证可以用于提供物理安全。

A、正确

B、错误

**正确答案：** A

# 265.令牌认证可以用于实现跨域访问控制。

A、正确

B、错误

**正确答案：** A

# 266.基于角色的访问控制可以简化用户权限的管理。

A、正确

B、错误

**正确答案：** A

# 267.令牌认证可以用于实现强认证。

A、正确

B、错误

**正确答案：** A

# 268.基于角色的访问控制可以应用于各种类型的系统。

A、正确

B、错误

**正确答案：** A

# 269.数字签名认证可以确保消息的顺序性。

A、正确

B、错误

**正确答案：** A

# 270.密码学认证可以用于保护数据在传输过程中的安全性。

A、正确

B、错误

**正确答案：** A

# 271.生物特征认证可以用于提供用户友好的身份验证方式。

A、正确

B、错误

**正确答案：** A

# 272.基于角色的访问控制可以应用于大型企业网络。

A、正确

B、错误

**正确答案：** A

# 273.数字签名认证可以用于验证数字证书的吊销状态。

A、正确

B、错误

**正确答案：** A

# 274.密码学认证可以用于实现安全的远程访问。

A、正确

B、错误

**正确答案：** A

# 275.生物特征认证可以用于提供不可伪造的身份验证。

A、正确

B、错误

**正确答案：** A

# 276.基于角色的访问控制可以应用于Web服务和API。

A、正确

B、错误

**正确答案：** A

# 277.基于角色的访问控制可以应用于移动设备。

A、正确

B、错误

**正确答案：** A

# 278.数字签名认证可以确保消息的可靠性和真实性。

A、正确

B、错误

**正确答案：** A

# 279.密码学认证可以用于防止中间人攻击。

A、正确

B、错误

**正确答案：** A

# 280.令牌认证可以用于实现安全的身份交换。

A、正确

B、错误

**正确答案：** A

# 281.基于角色的访问控制可以应用于不同类型的用户和资源。

A、正确

B、错误

**正确答案：** A

# 282.数字签名认证可以用于验证数字签名的合法性。

A、正确

B、错误

**正确答案：** A

# 283.密码学认证可以用于确保数据在传输过程中的安全性。

A、正确

B、错误

**正确答案：** A

# 284.网络安全主要指的是硬件和软件的安全。

A、正确

B、错误

**正确答案：** B

# 285.使用公共WiFi时应避免进行敏感信息的传输。

A、正确

B、错误

**正确答案：** A

# 286.网络钓鱼攻击通常通过伪造电子邮件或网站来窃取个人信息。

A、正确

B、错误

**正确答案：** A

# 287.安装防病毒软件后，电脑就不会再受到任何威胁。

A、正确

B、错误

**正确答案：** B

# 288.密码长度越长，安全性就越高。

A、正确

B、错误

**正确答案：** A

# 289.点击未知来源的链接或下载附件是安全的。

A、正确

B、错误

**正确答案：** B

# 290.开启防火墙可以有效防止黑客攻击。

A、正确

B、错误

**正确答案：** A

# 291.在社交媒体上随意分享个人信息是安全的。

A、正确

B、错误

**正确答案：** B

# 292.使用VPN可以确保网络隐私的绝对安全。

A、正确

B、错误

**正确答案：** B

# 293.HTTPS协议比HTTP协议更安全。

A、正确

B、错误

**正确答案：** A

# 294.定期更新操作系统和应用软件可以提高安全性。答案：

A、正确

B、错误

**正确答案：** A

# 295.网络攻击只针对大型企业，个人用户无需担心。答案：

A、正确

B、错误

**正确答案：** B

# 296.启用电脑自动更新可能会导致系统崩溃。答案：

A、正确

B、错误

**正确答案：** B

# 297.在网络上随意分享个人照片是安全的。答案：

A、正确

B、错误

**正确答案：** B

# 298.使用相同的密码可以方便记忆。答案：

A、正确

B、错误

**正确答案：** B

# 299.开启电脑防火墙会降低系统运行速度。答案：

A、正确

B、错误

**正确答案：** B

# 300.只有大型组织才会受到勒索软件的攻击。答案：

A、正确

B、错误

**正确答案：** B

# 301.使用强密码并定期更换可以提高账户安全性。答案：

A、正确

B、错误

**正确答案：** A