《计算机信息安全技术》综合测试试卷​（5）

**考试时间**：120 分钟​

**满分**：100 分​

一、单项选择题（每题 2 分，共 30 分）​

1. 在密码学中，凯撒密码属于（ ）。​

A. 对称加密算法 B. 非对称加密算法 C. 哈希函数 D. 数字签名技术​

1. 信息认证技术中，用于验证消息完整性的是（ ）。​

A. 数字证书 B. 消息认证码 C. 生物识别技术 D. 口令认证​

1. 计算机病毒按寄生方式分类，不包括以下哪种类型？（ ）​

A. 引导型病毒 B. 文件型病毒 C. 网络型病毒 D. 复合型病毒​

1. 以下哪种网络攻击方式是通过向目标服务器发送海量请求，耗尽其资源，从而导致服务器瘫痪？（ ）​

A. 木马攻击 B. 拒绝服务攻击（DoS） C. 网络钓鱼 D. 社交工程攻击​

1. 防火墙技术中，能对应用层数据进行深度检测和过滤的是（ ）。​

A. 包过滤防火墙 B. 状态检测防火墙 C. 应用代理防火墙 D. 分布式防火墙​

1. 入侵检测系统按照检测对象可分为基于主机的入侵检测系统和（ ）。​

A. 基于网络的入侵检测系统 B. 基于行为的入侵检测系统​

C. 基于特征的入侵检测系统 D. 基于异常的入侵检测系统​

1. 数据备份方式中，每次备份都包含全部数据的是（ ）。​

A. 完全备份 B. 增量备份 C. 差异备份 D. 按需备份​

1. 虚拟专用网（VPN）实现安全通信主要采用的技术不包括（ ）。​

A. 隧道技术 B. 加密技术 C. 数字证书技术 D. 身份认证技术​

1. 在电子商务安全中，保障交易双方身份真实性的核心技术是（ ）。​

A. 数据加密 B. 数字签名 C. 防火墙 D. 入侵检测​

1. 网络安全检测预评估中，用于发现系统中存在的安全漏洞的工具是（ ）。​

A. 杀毒软件 B. 防火墙 C. 漏洞扫描器 D. 入侵检测系统​

1. 以下关于对称密码体制和非对称密码体制的说法，正确的是（ ）。​

A. 对称密码体制加密和解密使用相同的密钥，非对称密码体制使用不同的密钥

B. 对称密码体制加密速度慢，非对称密码体制加密速度快​

C. 对称密码体制安全性高，非对称密码体制安全性低​

D. 对称密码体制用于数字签名，非对称密码体制用于数据加密​

1. 生物识别技术在信息认证中属于（ ）。​

A. 基于知识的认证 B. 基于拥有物的认证 C. 基于生物特征的认证 D. 基于口令的认证​

1. 计算机病毒传播速度最快的途径通常是（ ）。​

A. 移动存储设备 B. 电子邮件 C. 网络共享 D. 光盘​

1. 以下哪种防火墙体系结构具有较高的安全性，但成本也相对较高？（ ）

A. 双重宿主主机体系结构 B. 屏蔽主机体系结构​

C. 屏蔽子网体系结构 D. 单宿主主机体系结构​

1. 数据恢复的关键在于（ ）。​

A. 备份数据的完整性和可用性 B. 恢复工具的先进性​

C. 系统管理员的技术水平 D. 恢复时间的长短​

二、填空题（每题 2 分，共 20 分）​

1. 密码学中，将密文转换为明文的过程称为（解密 ）。​
2. 常见的信息认证方式有消息认证码和（ 哈希函数）。​
3. 计算机病毒的主要特点包括传染性、隐蔽性、（ 潜伏性）和破坏性。​
4. 网络攻击类型中，（ 网络钓鱼）攻击是通过欺骗手段获取用户敏感信息。
5. 防火墙的主要功能包括访问控制、（ 数据过滤）和地址转换。​
6. 入侵检测系统的主要功能是检测网络中的（ 异常）行为和潜在攻击。​
7. 数据备份策略通常包括完全备份、增量备份和（ 差异）备份。​
8. VPN 的中文全称是（虚拟专用网络 ）。​
9. 电子商务安全面临的主要威胁有信息泄露、篡改、（ 假冒）和抵赖。​
10. 网络安全检测预评估方法主要有漏洞扫描、（渗透测试 ）和安全审计等。（渗透测试是通过模拟黑客攻击来检测系统的安全性。）

三、简答题（每题 10 分，共 30 分）​

1. 简述对称密码体制和非对称密码体制的优缺点。​
2. 说明计算机病毒的防治措施有哪些。​
3. 阐述防火墙的工作原理，并比较包过滤防火墙、状态检测防火墙和应用代理防火墙的特点。​

四、论述题（20 分）​

结合企业实际情况，论述如何综合运用信息认证技术、入侵检测技术、数据备份与恢复技术以及虚拟专用网技术来保障企业信息安全，提高企业网络的安全性和稳定性。

**参考答案及分析：**

**一、单项选择题**

1. **答案**：A

**答案分析**：凯撒密码是一种典型的对称加密算法，它使用一个固定的密钥对明文进行加密，加密和解密使用相同的规则，所以答案是 A。非对称加密算法有不同的公私钥对，哈希函数主要用于数据摘要，数字签名技术是基于非对称加密等实现的一种认证技术，均不符合凯撒密码特点。

1. **答案**：B

**答案分析**：消息认证码用于验证消息的完整性，通过对消息进行特定的运算生成一个代码，接收方可以通过验证该代码来确定消息是否被篡改。数字证书主要用于身份认证，生物识别技术用于身份识别，口令认证主要用于验证用户身份，所以答案是 B。

1. **答案**：C

**答案分析**：计算机病毒按寄生方式可分为引导型病毒、文件型病毒和复合型病毒。网络型病毒是按照传播途径来分类的，不属于按寄生方式分类的类型，所以答案是 C。

1. **答案**：B

**答案分析**：拒绝服务攻击（DoS）的原理就是向目标服务器发送海量请求，耗尽其资源，导致服务器无法正常响应合法请求，从而瘫痪。木马攻击是通过植入木马程序控制目标主机，网络钓鱼是通过欺骗手段获取用户信息，社交工程攻击是利用人的弱点进行攻击，所以答案是 B。

1. **答案**：C

**答案分析**：应用代理防火墙工作在应用层，能对应用层数据进行深度检测和过滤，它可以对特定的应用程序进行代理服务，检查应用层的协议和数据。包过滤防火墙主要在网络层和传输层对数据包进行过滤，状态检测防火墙也主要在网络层和传输层，通过跟踪连接状态进行过滤，分布式防火墙是一种部署方式，不是按检测深度分类的，所以答案是 C。

1. **答案**：A

**答案分析**：入侵检测系统按照检测对象可分为基于主机的入侵检测系统和基于网络的入侵检测系统。基于行为、特征、异常的入侵检测系统是按照检测方法来分类的，所以答案是 A。

1. **答案**：A

**答案分析**：完全备份每次都会对全部数据进行备份，增量备份是只备份自上次备份以来更改过的数据，差异备份是备份自上次完全备份以来更改过的数据，按需备份是根据特定需求进行的备份，不一定是全部数据，所以答案是 A。

1. **答案**：C

**答案分析**：虚拟专用网（VPN）实现安全通信主要采用隧道技术、加密技术和身份认证技术等。数字证书技术通常用于身份认证和数字签名等方面，但不是 VPN 实现安全通信的主要核心技术，所以答案是 C。

1. **答案**：B

**答案分析**：在电子商务安全中，数字签名技术可以通过使用私钥对交易信息进行签名，接收方可以使用相应的公钥验证签名，从而保障交易双方身份的真实性。数据加密主要是保护数据的保密性，防火墙和入侵检测主要是保护网络安全，防止外部攻击，所以答案是 B。

1. **答案**：C

**答案分析**：漏洞扫描器是用于发现系统中存在的安全漏洞的工具，它可以对网络设备、主机、应用程序等进行扫描，检测出可能存在的安全隐患。杀毒软件主要用于查杀病毒，防火墙用于访问控制，入侵检测系统用于检测入侵行为，所以答案是 C。

1. **答案**：A

**答案分析**：对称密码体制加密和解密使用相同的密钥，加密速度快，但密钥管理复杂，安全性相对较低，常用于数据加密；非对称密码体制使用不同的密钥，加密速度慢，但安全性高，常用于数字签名等，所以答案是 A。其他选项说法均错误。

1. **答案**：C

**答案分析**：生物识别技术是基于人体的生物特征，如指纹、虹膜、面部识别等进行身份认证的，属于基于生物特征的认证。基于知识的认证如口令、密码等，基于拥有物的认证如智能卡等，所以答案是 C。

1. **答案**：C

**答案分析**：网络共享环境下，计算机病毒可以通过网络快速传播到多个主机，传播速度通常最快。移动存储设备、电子邮件、光盘等也能传播病毒，但传播范围和速度相对网络共享来说要慢一些，所以答案是 C。

1. **答案**：C

**答案分析**：屏蔽子网体系结构具有较高的安全性，它通过设置多个安全区域和过滤规则，形成一个相对独立的子网来保护内部网络，但这种结构需要较多的设备和复杂的配置，成本相对较高。双重宿主主机体系结构、屏蔽主机体系结构安全性相对较低，单宿主主机体系结构一般不存在这种说法，所以答案是 C。

1. **答案**：A

**答案分析**：数据恢复的关键在于备份数据的完整性和可用性，如果备份数据不完整或不可用，那么即使有先进的恢复工具和技术水平高的系统管理员，也无法成功恢复数据。恢复时间长短是数据恢复的一个重要指标，但不是关键因素，所以答案是 A。

**二、填空题**

1. **答案**：解密

**答案分析**：密码学中，将密文转换为明文的过程就是解密，与加密过程相对应。

1. **答案**：哈希函数

**答案分析**：常见的信息认证方式有消息认证码和哈希函数。

1. **答案**：潜伏性

**答案分析**：计算机病毒的主要特点包括传染性、隐蔽性、潜伏性和破坏性。潜伏性是指病毒可能在系统中潜伏一段时间，在特定条件下才发作。

1. **答案**：网络钓鱼

**答案分析**：网络钓鱼攻击是通过欺骗手段，如伪造网站、发送虚假邮件等，获取用户敏感信息，如账号、密码等。

1. **答案**：数据过滤

**答案分析**：防火墙的主要功能包括访问控制、数据过滤和地址转换。数据过滤可以根据规则对数据包进行筛选，阻止不符合安全策略的数据通过。

1. **答案**：异常

**答案分析**：入侵检测系统的主要功能是检测网络中的异常行为和潜在攻击，通过对网络流量、系统日志等进行分析，发现可能的入侵行为。

1. **答案**：差异

**答案分析**：数据备份策略通常包括完全备份、增量备份和差异备份，这三种备份方式各有特点，可以结合使用来满足不同的备份需求。

1. **答案**：虚拟专用网络

**答案分析**：VPN 的中文全称是虚拟专用网络，它是一种通过公共网络建立安全的专用网络连接的技术。

1. **答案**：假冒

**答案分析**：电子商务安全面临的主要威胁有信息泄露、篡改、假冒和抵赖。假冒是指攻击者冒充合法用户进行交易等操作，威胁交易安全。

1. **答案**：渗透测试

**答案分析**：网络安全检测预评估方法主要有漏洞扫描、渗透测试和安全审计等。渗透测试是通过模拟黑客攻击来检测系统的安全性。

**三、简答题**

1. **参考答案**：

**对称密码体制**：

* + - **优点**：加密和解密速度快，效率高；密钥长度相对较短，加密强度较高；适合对大量数据进行加密。
    - **缺点**：密钥管理困难，需要安全的渠道来分发和共享密钥；通信双方必须事先约定好密钥，不适合网络环境下的大规模应用；无法实现数字签名等功能。

**非对称密码体制**：

* + - **优点**：密钥管理方便，公钥可以公开分发，私钥由用户自己保管；可以实现数字签名和身份认证等功能，适合网络环境下的安全通信。
    - **缺点**：加密和解密速度慢，效率较低；密钥长度较长，计算量较大；加密强度依赖于密钥长度和算法的安全性。

1. **参考答案**：

安装正版杀毒软件和防火墙，并及时更新病毒库和规则。

不随意下载和安装来路不明的软件和文件，尤其是从不可信的网站下载。

定期对计算机系统和数据进行备份，以便在受到病毒攻击后能够及时恢复。

谨慎打开电子邮件附件，尤其是来自陌生人的邮件附件，先进行病毒扫描。

保持操作系统和应用程序的更新，及时安装安全补丁，修复可能存在的漏洞。

加强用户安全意识教育，提高用户对病毒的防范意识，不轻易点击可疑链接和执行可疑程序。

对于移动存储设备，如 U 盘、移动硬盘等，在接入计算机前先进行病毒扫描。

1. **参考答案**：

**防火墙工作原理**：防火墙是位于内部网络与外部网络之间的一道安全屏障，它根据预设的安全策略，对进出网络的数据包进行检查和过滤。防火墙会检查数据包的源地址、目的地址、端口号、协议等信息，根据规则决定是否允许数据包通过。

**包过滤防火墙特点**：工作在网络层和传输层，根据数据包的头部信息进行过滤，速度快，对网络性能影响小，但不能对应用层数据进行深度检测，安全性相对较低。

**状态检测防火墙特点**：在包过滤防火墙的基础上，增加了对连接状态的跟踪。它可以识别数据包所属的连接状态，如新建连接、已建立连接、连接终止等，从而更有效地防止非法连接和攻击，安全性比包过滤防火墙高，但对网络性能有一定影响。

**应用代理防火墙特点**：工作在应用层，对特定的应用程序进行代理服务。它可以对应用层的数据进行深度检测和过滤，能够有效地防范各种应用层攻击，但由于需要对每个应用程序进行代理，性能相对较低，对系统资源要求较高。

**四、论述题**

**参考答案**：

* **信息认证技术**：在企业中，信息认证技术用于确保用户身份的真实性和信息的完整性。例如，采用数字证书对员工进行身份认证，员工在访问企业关键信息系统时，通过数字证书验证其身份，防止非法用户冒充。同时，使用消息认证码或数字签名技术来确保数据在传输过程中未被篡改，保证信息的完整性。对于重要的业务数据，如合同、财务报表等，通过数字签名技术可以明确数据的来源和完整性，防止抵赖行为。
* **入侵检测技术**：企业部署入侵检测系统（IDS）或入侵防御系统（IPS）来实时监测网络中的异常行为和潜在攻击。基于网络的入侵检测系统可以监测网络流量，发现针对企业网络的各种攻击，如端口扫描、DDoS 攻击等。基于主机的入侵检测系统可以监测主机系统的活动，发现异常的进程、文件访问等行为。当检测到入侵行为时，系统及时发出警报，并采取相应的措施，如阻断攻击源、记录攻击行为等，以保护企业网络和系统的安全。
* **数据备份与恢复技术**：企业应制定完善的数据备份策略，定期对重要数据进行备份。采用完全备份和增量备份相结合的方式，既能保证数据的完整性，又能减少备份时间和存储空间。备份数据应存储在安全的地方，如异地数据中心或云存储。当企业遭受数据丢失事件，如病毒攻击、硬件故障等，能够及时从备份中恢复数据，确保业务的连续性。同时，定期进行数据恢复演练，以验证备份数据的可用性和恢复流程的有效性。
* **虚拟专用网技术**：对于企业有远程办公或分支机构的情况，虚拟专用网（VPN）技术可以提供安全的远程访问通道。通过 VPN，员工可以在外部网络安全地访问企业内部资源，如企业的办公系统、数据库等。VPN 通过隧道技术、加密技术和身份认证技术，将员工的远程连接封装在安全的隧道中，防止数据被窃取或篡改。同时，企业可以对 VPN 连接进行访问控制，限制不同用户的访问权限，进一步提高网络的安全性。

综合运用这些技术，企业可以从身份认证、入侵检测、数据保护和远程访问安全等多个方面保障信息安全，提高企业网络的安全性和稳定性，确保企业业务的正常运行。同时，企业还应不断加强安全管理，提高员工的安全意识，定期进行安全培训和演练，以应对不断变化的安全威胁。