《计算机信息安全技术》综合测试试卷​

**考试时间**：120 分钟​

**满分**：100 分​

一、选择题（每题 2 分，共 30 分）​

1. 计算机病毒的主要特点不包括（ ）。​

A. 传染性​ B. 隐蔽性​ . 可预测性​ . 破坏性​

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

A. 木马攻击​ . 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，能根据应用层协议进行过滤的是（ ）。​

A. 包过滤防火墙​ B. 状态检测防火墙​ . 应用代理防火墙​

* D. 网络地址转换防火墙​

1. 入侵检测系统按照检测技术可分为基于特征检测和基于（ ）检测。​

* A. 行为​
* B. 流量​
* C. 协议​
* D. 端口​

1. 数据备份的方式不包括（ ）。​

* A. 完全备份​
* B. 增量备份​
* C. 差异备份​
* D. 随机备份​

1. 虚拟专用网（VPN）主要用于（ ）。​

* A. 提高网络速度​
* B. 实现远程安全通信​
* C. 增加网络带宽​
* D. 防止病毒入侵​

1. 在电子商务安全中，用于保障交易双方身份真实性的技术是（ ）。​

* A. 数字证书​
* B. 加密技术​
* C. 防火墙​
* D. 入侵检测系统​

1. 网络安全检测预评估的主要目的不包括（ ）。​

* A. 发现系统漏洞​
* B. 评估安全风险​
* C. 修复系统故障​
* D. 提供安全改进建议​

1. 宏病毒通常感染的文件类型是（ ）。​

* A. EXE 文件​
* B. COM 文件​
* C. DOC 文件​
* D. SYS 文件​

1. 以下哪种网络攻击利用了用户的心理弱点，通过欺骗手段获取敏感信息？（ ）​

* A. 分布式拒绝服务攻击（DDoS）​
* B. 恶意软件攻击​
* C. 社会工程攻击​
* D. 语义攻击​

1. 防火墙部署在网络的（ ）。​

* A. 内部网络​
* B. 外部网络​
* C. 内部网络与外部网络之间​
* D. 服务器上​

1. 入侵检测系统的主要功能是（ ）。​

* A. 阻止网络攻击​
* B. 检测网络中的异常行为和潜在攻击​
* C. 对网络数据进行加密​
* D. 修复系统漏洞​

1. 数据恢复是指（ ）。​

* A. 将备份的数据还原到系统中​
* B. 对损坏的数据进行修复​
* C. 清理系统中的垃圾数据​
* D. 重新安装操作系统​

1. VPN 采用的主要技术不包括（ ）。​

* A. 隧道技术​
* B. 加密技术​
* C. 身份认证技术​
* D. 数据压缩技术​

1. 在电子商务交易中，防止交易抵赖的措施是（ ）。​

* A. 加密传输​
* B. 数字签名​
* C. 防火墙防护​
* D. 入侵检测​

二、填空题（每题 2 分，共 20 分）​

1. 计算机病毒按寄生方式可分为引导型、文件型和（ ）。​
2. 常见的网络攻击类型除了拒绝服务攻击，还有（ ）、网络钓鱼等。​
3. 防火墙的主要功能包括访问控制、（ ）和地址转换。​
4. 入侵检测系统可分为基于主机的入侵检测系统和基于（ ）的入侵检测系统。​
5. 数据备份策略通常包括完全备份、增量备份和（ ）备份。​
6. VPN 的中文全称是（ ）。​
7. 电子商务安全的主要威胁有信息泄露、篡改、（ ）和抵赖等。​
8. 网络安全检测预评估方法主要有漏洞扫描、（ ）和安全审计等。​
9. 计算机病毒的传播途径主要有网络传播、（ ）传播和存储设备传播。​
10. 防火墙的体系结构有双重宿主主机体系结构、（ ）体系结构和屏蔽子网体系结构。​

三、简答题（每题 10 分，共 30 分）​

1. 简述计算机病毒的防治措施。​
2. 说明防火墙的工作原理及主要类型。​
3. 阐述数据备份与恢复的重要性，并举例说明常用的数据恢复场景。​

四、论述题（20 分）​

结合实际情况，论述在企业网络环境中，如何综合运用网络攻击与防范技术、入侵检测技术、防火墙技术以及 VPN 技术来构建一个安全可靠的网络架构，保障企业信息安全。

参考答案及分析：

**《计算机信息安全技术》综合测试试卷答案及分析**

**一、选择题（每题 2 分，共 30 分）**

**1. 计算机病毒的主要特点不包括（ ）。**

* **答案**：C
* **分析**：计算机病毒具有传染性、隐蔽性、破坏性等特点。它可以自我复制并传播到其他程序或系统中，具有很强的隐蔽性，不易被发现，同时会对系统或数据造成破坏。而可预测性并非其特点，病毒的传播和发作往往具有不确定性。

**2. 以下哪种网络攻击通过向目标服务器发送海量请求，耗尽其资源，导致服务器瘫痪？（ ）**

* **答案**：B
* **分析**：拒绝服务攻击（DoS）就是通过大量的请求消耗目标服务器的资源，使其无法正常响应合法用户的请求，最终导致服务器瘫痪。木马攻击主要是通过植入恶意程序来控制目标系统；网络钓鱼是通过欺骗手段获取用户的敏感信息；社交工程攻击是利用人的心理弱点来获取信息。

**3. 防火墙技术中，能根据应用层协议进行过滤的是（ ）。**

* **答案**：C
* **分析**：应用代理防火墙工作在应用层，它可以对应用层协议进行深入分析和过滤。包过滤防火墙主要根据数据包的源 IP 地址、目的 IP 地址、端口号等进行过滤；状态检测防火墙在包过滤的基础上增加了对连接状态的检测；网络地址转换防火墙主要用于实现内部网络和外部网络之间的地址转换。

**4. 入侵检测系统按照检测技术可分为基于特征检测和基于（ ）检测。**

* **答案**：A
* **分析**：入侵检测系统的检测技术主要分为基于特征检测和基于行为检测。基于特征检测是通过匹配已知的攻击特征来发现入侵行为；基于行为检测则是通过分析系统或网络的正常行为模式，当出现异常行为时发出警报。

**5. 数据备份的方式不包括（ ）。**

* **答案**：D
* **分析**：常见的数据备份方式有全量备份、增量备份和差异备份。全量备份是备份所有数据；增量备份只备份自上次备份以来发生变化的数据；差异备份是备份自上次全量备份以来发生变化的数据。随机备份不是一种标准的数据备份方式。

**6. 虚拟专用网（VPN）主要用于（ ）。**

* **答案**：B
* **分析**：虚拟专用网（VPN）的主要作用是在公共网络上建立一条安全的专用通道，实现远程安全通信。它可以隐藏用户的真实 IP 地址，加密数据传输，保护数据的安全性和隐私性。虽然 VPN 可能会对网络速度和带宽有一定影响，但提高网络速度和增加网络带宽并不是其主要目的，它也不能直接防止病毒入侵。

**7. 在电子商务安全中，用于保障交易双方身份真实性的技术是（ ）。**

* **答案**：A
* **分析**：数字证书是由权威的证书颁发机构（CA）颁发的，用于证明用户或实体的身份。在电子商务交易中，交易双方可以通过验证对方的数字证书来确认其身份的真实性。加密技术主要用于保护数据的保密性和完整性；防火墙用于网络访问控制；入侵检测系统用于检测网络中的入侵行为。

**8. 网络安全检测预评估的主要目的不包括（ ）。**

* **答案**：C
* **分析**：网络安全检测预评估的主要目的是发现系统漏洞、评估安全风险并提供安全改进建议。它可以帮助企业提前发现潜在的安全问题，采取相应的措施进行防范。但修复系统故障不是网络安全检测预评估的主要目的，修复故障通常是在发现问题之后进行的后续操作。

**9. 宏病毒通常感染的文件类型是（ ）。**

* **答案**：C
* **分析**：宏病毒主要感染包含宏代码的文件，如 DOC 等办公文档。EXE 文件和 COM 文件通常是可执行文件，宏病毒一般不会直接感染这类文件；SYS 文件是系统文件，也不是宏病毒的主要感染对象。

**10. 以下哪种网络攻击利用了用户的心理弱点，通过欺骗手段获取敏感信息？（ ）**

* **答案**：C
* **分析**：社交工程攻击是利用人的心理弱点，如信任、好奇、恐惧等，通过欺骗手段获取用户的敏感信息。分布式拒绝服务攻击（DDoS）是通过大量的请求消耗目标服务器的资源；恶意软件攻击是通过植入恶意程序来破坏或控制目标系统；语义攻击是针对信息的语义进行攻击。

**11. 防火墙部署在网络的（ ）。**

* **答案**：C
* **分析**：防火墙通常部署在内部网络与外部网络之间，用于控制和过滤进出网络的流量，保护内部网络的安全。它可以阻止外部网络的非法访问，同时也可以对内部网络的访问进行限制。

**12. 入侵检测系统的主要功能是（ ）。**

* **答案**：B
* **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。它可以实时监测网络流量和系统活动，当发现异常情况时发出警报，但它本身不能直接阻止网络攻击。对网络数据进行加密是加密技术的功能；修复系统漏洞是系统维护和更新的工作。

**13. 数据恢复是指（ ）。**

* **答案**：A
* **分析**：数据恢复是指将备份的数据还原到系统中，以应对数据丢失或损坏的情况。对损坏的数据进行修复是数据修复的概念；清理系统中的垃圾数据是系统优化的操作；重新安装操作系统与数据恢复没有直接关系。

**14. VPN 采用的主要技术不包括（ ）。**

* **答案**：D
* **分析**：VPN 采用的主要技术包括隧道技术、加密技术和身份认证技术。隧道技术用于在公共网络上建立专用通道；加密技术用于保护数据的保密性；身份认证技术用于验证用户的身份。数据压缩技术不是 VPN 的主要技术，虽然在某些情况下可能会使用数据压缩来提高传输效率，但它不是 VPN 的核心技术。

**15. 在电子商务交易中，防止交易抵赖的措施是（ ）。**

* **答案**：B
* **分析**：数字签名是一种用于验证消息来源和完整性的技术，同时也可以防止交易抵赖。在电子商务交易中，发送方使用自己的私钥对交易信息进行签名，接收方可以使用发送方的公钥进行验证。如果签名验证通过，则可以证明消息确实是由发送方发送的，并且在传输过程中没有被篡改。加密传输主要用于保护数据的保密性；防火墙防护用于网络安全防护；入侵检测用于检测网络中的入侵行为。

**二、填空题（每题 2 分，共 20 分）**

**1. 计算机病毒按寄生方式可分为引导型、文件型和（ ）。**

* **答案**：混合型
* **分析**：计算机病毒按寄生方式可分为引导型病毒、文件型病毒和混合型病毒。混合型病毒兼具引导型病毒和文件型病毒的特点，既可以感染引导扇区，也可以感染可执行文件。

**2. 常见的网络攻击类型除了拒绝服务攻击，还有（ ）、网络钓鱼等。**

* **答案**：木马攻击（答案不唯一，其他合理答案如：SQL 注入攻击、暴力破解攻击等亦可）
* **分析**：常见的网络攻击类型有很多，除了拒绝服务攻击和网络钓鱼外，木马攻击是一种常见的攻击方式，它通过植入恶意程序来控制目标系统。SQL 注入攻击是通过在输入字段中注入恶意的 SQL 语句来获取或篡改数据库中的数据；暴力破解攻击是通过尝试所有可能的密码组合来破解用户账户。

**3. 防火墙的主要功能包括访问控制、（ ）和地址转换。**

* **答案**：包过滤
* **分析**：防火墙的主要功能包括访问控制、包过滤和地址转换。访问控制用于限制网络访问权限；包过滤根据预设的规则对数据包进行过滤；地址转换用于实现内部网络和外部网络之间的地址转换。

**4. 入侵检测系统可分为基于主机的入侵检测系统和基于（ ）的入侵检测系统。**

* **答案**：网络
* **分析**：入侵检测系统可分为基于主机的入侵检测系统（HIDS）和基于网络的入侵检测系统（NIDS）。基于主机的入侵检测系统主要监测主机上的系统活动和文件变化；基于网络的入侵检测系统主要监测网络中的数据包和流量。

**5. 数据备份策略通常包括完全备份、增量备份和（ ）备份。**

* **答案**：差分
* **分析**：数据备份策略通常包括完全备份、增量备份和差分备份。完全备份备份所有数据；增量备份只备份自上次备份以来发生变化的数据；差分备份备份自上次完全备份以来发生变化的数据。

**6. VPN 的中文全称是（ ）。**

* **答案**：虚拟专用网
* **分析**：VPN 是 Virtual Private Network 的缩写，中文全称是虚拟专用网。

**7. 电子商务安全的主要威胁有信息泄露、篡改、（ ）和抵赖等。**

* **答案**：假冒
* **分析**：电子商务安全的主要威胁包括信息泄露、篡改、假冒和抵赖等。信息泄露是指敏感信息被非法获取；篡改是指数据在传输过程中被修改；假冒是指攻击者冒充合法用户进行交易；抵赖是指交易双方否认自己的交易行为。

**8. 网络安全检测预评估方法主要有漏洞扫描、（ ）和安全审计等。**

* **答案**：渗透测试
* **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。漏洞扫描用于发现系统中的安全漏洞；渗透测试是模拟攻击者的行为，对系统进行攻击测试，以发现潜在的安全风险；安全审计是对系统的活动和操作进行记录和分析，以发现异常行为。

**9. 计算机病毒的传播途径主要有网络传播、（ ）传播和存储设备传播。**

* **答案**：电子邮件
* **分析**：计算机病毒的传播途径主要有网络传播、电子邮件传播和存储设备传播。网络传播可以通过网页、下载文件等方式进行；电子邮件传播是通过发送带有病毒的邮件附件进行；存储设备传播是通过 U 盘、移动硬盘等存储设备进行。

**10. 防火墙的体系结构有双重宿主主机体系结构、（ ）体系结构和屏蔽子网体系结构。**

* **答案**：屏蔽主机
* **分析**：防火墙的体系结构主要有双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构。双重宿主主机体系结构通过一台具有两个网络接口的主机来连接内部网络和外部网络；屏蔽主机体系结构使用一个包过滤路由器和一个堡垒主机来保护内部网络；屏蔽子网体系结构在内部网络和外部网络之间增加了一个屏蔽子网，进一步提高了网络的安全性。

**三、简答题（每题 10 分，共 30 分）**

**1. 简述计算机病毒的防治措施。**

* **答案**：

**技术层面**：

安装杀毒软件和防火墙，并及时更新病毒库和系统补丁，以抵御新出现的病毒攻击。杀毒软件可以实时监控系统，检测和清除病毒；防火墙可以阻止外部网络的非法访问，防止病毒进入系统。

进行数据备份，定期对重要数据进行备份，以便在遭受病毒攻击导致数据丢失时能够恢复。备份可以采用全量备份、增量备份或差异备份等方式。

采用入侵检测系统（IDS）或入侵防御系统（IPS），实时监测网络流量和系统活动，及时发现并阻止病毒的传播和攻击。

**管理层面**：

提高用户的安全意识，教育用户不随意打开来源不明的邮件附件、不下载未经授权的软件、不访问不可信的网站等，避免因用户的不当操作导致病毒感染。

建立安全管理制度，规范计算机的使用和维护流程，对计算机设备进行定期检查和维护，确保系统的安全性。

加强网络安全管理，限制网络访问权限，对网络流量进行监控和分析，及时发现并处理异常情况。

**分析**：该题主要考查对计算机病毒防治措施的理解和掌握。从技术和管理两个层面进行回答，可以全面地涵盖防治计算机病毒的主要方法。技术层面的措施是通过使用各种安全技术来防范和清除病毒；管理层面的措施是通过提高用户的安全意识和建立安全管理制度来减少病毒感染的风险。

**2. 说明防火墙的工作原理及主要类型。**

* **答案**：

**工作原理**：防火墙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。它会分析数据包的源 IP 地址、目的 IP 地址、端口号、协议类型等信息，根据策略决定是否允许数据包通过。如果数据包符合策略，则允许通过；如果不符合策略，则拒绝通过或进行相应的处理。

**主要类型**：

**包过滤防火墙**：工作在网络层和传输层，根据数据包的源 IP 地址、目的 IP 地址、端口号等信息进行过滤。它的优点是速度快、成本低，但安全性相对较低，无法对应用层数据进行深入检查。

**状态检测防火墙**：在包过滤的基础上，增加了对连接状态的检测。它可以跟踪网络连接的状态，根据连接的状态信息来判断数据包是否合法，安全性较高，但对性能有一定影响。

**应用代理防火墙**：工作在应用层，它会对应用层协议进行深入分析和过滤。应用代理防火墙会在客户端和服务器之间建立代理连接，对客户端的请求进行检查和处理，然后再将请求转发给服务器。它的安全性最高，但性能开销较大，对不同应用的支持需要单独配置。

**分析**：本题考查防火墙的工作原理和主要类型。工作原理部分需要解释防火墙如何根据策略对数据包进行检查和过滤；主要类型部分需要分别介绍包过滤防火墙、状态检测防火墙和应用代理防火墙的特点和优缺点。

**3. 阐述数据备份与恢复的重要性，并举例说明常用的数据恢复场景。**

* **答案**：

**重要性**：

**数据保护**：数据是企业和个人的重要资产，数据备份可以防止因各种原因（如硬件故障、软件错误、人为失误、病毒攻击、自然灾害等）导致的数据丢失或损坏，确保数据的安全性和完整性。

**业务连续性**：在数据丢失或损坏的情况下，通过数据恢复可以快速将系统恢复到正常运行状态，减少业务中断的时间，保证业务的连续性。

**合规性要求**：某些行业或法规要求企业对重要数据进行备份和恢复，以满足合规性要求。

**常用数据恢复场景**：

**硬件故障**：如硬盘损坏、服务器故障等，导致数据无法正常访问。通过使用备份数据可以将数据恢复到新的硬件设备上，确保业务的正常运行。

**软件错误**：如操作系统崩溃、数据库损坏等，导致数据丢失或无法访问。可以通过恢复备份数据来解决问题。

**人为失误**：如误删除文件、误格式化磁盘等，通过数据恢复可以找回丢失的数据。

**病毒攻击**：计算机受到病毒攻击，数据被加密或破坏。可以使用备份数据进行恢复，避免数据丢失。

**分析**：本题要求阐述数据备份与恢复的重要性，并举例说明常用的数据恢复场景。重要性部分需要从数据保护、业务连续性和合规性要求等方面进行阐述；常用数据恢复场景部分需要列举一些常见的数据丢失或损坏的情况，并说明如何通过数据恢复来解决问题。

**四、论述题（20 分）**

**结合实际情况，论述在企业网络环境中，如何综合运用网络攻击与防范技术、入侵检测技术、防火墙技术以及 VPN 技术来构建一个安全可靠的网络架构，保障企业信息安全。**

* **答案**：  
  在企业网络环境中，构建安全可靠的网络架构需要综合运用多种技术，形成多层次的安全防护体系，具体如下：

**网络攻击与防范技术**：

**加强安全意识培训**：对企业员工进行网络安全意识培训，提高他们对常见网络攻击手段（如网络钓鱼、社会工程学攻击等）的认识，避免因员工的疏忽导致安全漏洞。

**采用加密技术**：对企业内部的敏感数据进行加密处理，确保数据在传输和存储过程中的保密性和完整性。例如，使用 SSL/TLS 协议对网站进行加密，防止数据在传输过程中被窃取。

**实施访问控制**：根据员工的工作职责和权限，对企业网络资源进行访问控制，限制员工对敏感数据和系统的访问权限，防止内部人员的非法操作。

**入侵检测技术**：

**部署入侵检测系统（IDS）和入侵防御系统（IPS）**：实时监测网络流量和系统活动，及时发现并阻止潜在的入侵行为。IDS 可以对入侵行为进行实时报警，IPS 则可以在发现入侵行为时自动采取措施进行阻止。

**进行日志分析**：对系统和网络的日志进行分析，及时发现异常行为和潜在的安全威胁。通过对日志的分析，可以了解攻击者的攻击手段和意图，为后续的安全防护提供依据。

**防火墙技术**：

**在企业网络边界部署防火墙**：将企业内部网络与外部网络隔离开来，根据预设的安全策略对进出网络的流量进行过滤，阻止外部网络的非法访问和攻击。

**配置防火墙规则**：根据企业的业务需求和安全策略，合理配置防火墙规则，确保只允许合法的流量通过。同时，定期对防火墙规则进行审查和更新，以适应不断变化的网络环境。

**VPN 技术**：

**为远程办公人员和分支机构提供安全连接**：通过 VPN 技术，在公共网络上建立安全的专用通道，使得远程办公人员和分支机构能够安全地访问企业内部网络资源。

**采用加密和身份认证技术**：对 VPN 连接进行加密处理，确保数据在传输过程中的保密性和完整性。同时，采用身份认证技术，对用户的身份进行验证，防止非法用户接入企业网络。

通过综合运用以上技术，可以构建一个多层次、全方位的网络安全防护体系，有效保障企业信息安全。同时，企业还需要定期对网络安全进行评估和检测，及时发现并修复安全漏洞，不断完善安全策略和防护措施，以适应不断变化的网络安全环境。

* **分析**：本题要求结合实际情况，论述如何综合运用多种技术构建安全可靠的网络架构。回答时需要分别阐述网络攻击与防范技术、入侵检测技术、防火墙技术和 VPN 技术在企业网络安全中的作用和应用方法，并说明如何将这些技术结合起来形成一个完整的安全防护体系。同时，还需要强调定期进行网络安全评估和检测的重要性。