(1)计算机网络安全是一门涉及（计算机科学）、（网络技术）、（信息安全技术）

(2)网络信息安全要素特征，分别是（保密性）（完整性）（可用性）（可控性）（不可否认性）。

(3)从层次结构上，计算机网络安全所涉及的内容包括（实体安全）、（运行安全）、（系统安全）、（应用安全）和（管理安全

(4)网络安全的目标是在计算机网络的信息传输、存储与处理的整个过程中，提高（物理上逻辑上）的防护、监控、反应恢复和（对抗）的能力。

(5)VPN技术有哪些特点?安全性高、费用低廉、管理便利、灵活性强、服务质量佳

(1)攻击五部曲（隐藏IP）（踩点扫描）（获得控制权）（种植后门）（隐身退出）。

(2)端口扫描的防范也称为（系统加固），主要有（防止IP地址的扫描）和（关闭闲置及有潜在危险的端口）。

(4)传统加密方法:（代码加密）、（替换加密）、（边位加密）和（一次性加密）。

(5)什么是对称加密？什么是非对称加密？他们各自的优缺点是什么？

对称加密：使用相同密钥进行加密和解密。

非对称加密：使用一对密钥（公钥和私钥）进行加密和解密。

对称加密的优点是速度快，效率高，缺点是密钥需要在通信双方之间共享，存在密钥管理的安全性问题。

非对称加密的优点是安全性高，不需要共享密钥，缺点是加密和解密花费时间长，速度较慢。

(2)数字签名是指用户用自己的（私钥）对原始数据进行（加密）所得到的（特殊数字串），专门用于保证信息来源的（真实性）、数据传输的（完整性）和（防抵赖性）。

(1)简述数字签名技术的实现过程。

- 创建签名：使用私钥加密原始数据生成数字签名。
- 验证签名：使用公钥解密数字签名得到摘要。
- 摘要比对：将解密后的摘要与计算得到的摘要进行比对。
- 比对结果：如果相同，签名有效；如果不同，签名无效。

数字签名技术的目的是确保数据的完整性、真实性和不可抵赖性，同时实现发送者的身份认证和数据的防篡改。

(6)常用的网络身份认证方式

身份认证概念：身份认证是计算机及网络系统识别操作者身份的过程

常用的身份认证方式：

用户名/口令方式 优点：最常用且简单；缺点：密码容易泄露，密码容易在传输过程中被截获

CA认证 采用证书认证方式。

USB key认证 优点：方便、安全、经济；缺点：依赖硬件安全性

生物识别技术 优点：安全性最高；缺点：技术不成熟，准确性和稳定性有待提高

动态口令 优点：一次一密，较高安全性；缺点：使用繁琐可能造成新的安全漏洞

(5)计算机病毒的主要传播途径有（移动式存储介质）和（网络传播）。

(6)计算机运行异常的主要现象包括（无法开机）、（开机速度变慢）、（系统运行速度慢）、（频繁重启）、（无故死机）和（自动关机）等。

(1)简述计算机病毒的特点有哪些。

特点：非授权可执行性、传染性、隐蔽性、潜伏性、触发及控制性、影响破坏性、多态及不可预见性

7)木马和蠕虫病毒的检测与防范

检测：使用防病毒软件进行扫描和更新，配置防火墙，定期进行安全漏洞扫描。

防范：谨慎下载和安装软件，避免点击可疑链接和附件，定期备份数据，更新系统和应用程序

(1)防火墙是什么以及它的主要特性和主要缺陷?

防火墙是软硬件组合的保护屏障，建立内外网安全网关，保护内部网免受非法用户入侵。

主要功能：集中监视、隔离网络、强化安全策略、记录审计、代理转发、网络地址转换NAT、虚拟专用网VPN。

缺陷：无法防范新攻击、无法防止协议缺陷攻击、无法防止系统漏洞攻击、无法防止数据驱动攻击、无法保证服务安全、存在自身安全漏洞、无法防止病毒传输。

(2)简述防火墙的分类及主要技术。

根据物理特性，防火墙分为硬件防火墙和软件防火墙。 按过滤机制可划分为过滤防火墙、代理网关防火墙和状态检测防火墙。 按处理能力可划分为百兆、千兆和万兆防火墙。 按部署方式可划分为终端和网络防火墙。 防火墙的主要技术包括包过滤、应用代理和状态检测。