《计算机网络安全》 重点内容 1

1.信息安全的目标。

1. 保护机密性：确保信息只能被授权人员访问，防止未经授权的人员获取信息。
2. 保护完整性：确保信息没有被篡改或者损坏，保证信息的准确性和真实性。
3. 保护可用性：确保信息能够在需要的时间和地点被授权人员使用，防止信息被恶意破坏或者拒绝服务攻击。
4. 保护可靠性：确保信息系统的稳定性和可靠性，防止发生系统故障、崩溃和数据丢失等情况。
5. 遵守法律法规：确保信息系统和信息处理过程的合法性和规范性，遵守相关的法律法规和规章制度。

2.防火墙的作用。

1. 访问控制：防火墙可以根据预设的访问规则，对进出网络的数据进行检查和过滤，防止网络攻击和非法访问。
2. 地址转换：防火墙可以进行网络地址转换（NAT），将内部网络的私有地址转换成公网 IP 地址，这样使得内部网络暴露的 IP 地址更少，提高了网络的安全性。
3. 网络监控：防火墙可以对网络的所有数据流量进行监控，包括传输协议、数据包大小、来源地址、目的地地址等，从而对攻击、病毒等安全威胁进行检测和预防。
4. VPN 支持：防火墙可以支持虚拟专用网络（VPN），通过加密数据传输，保证数据传输的安全性和机密性。

3.黑客攻击的一般过程。

1. 侦察（Reconnaissance）：黑客通过各种方式收集关于目标网络系统和安全配置的信息，包括目标网络的 IP 地址、域名、系统架构、运营商等。黑客可以利用搜索引擎、社交网络、WHOIS 查询、端口扫描等方式进行侦察。
2. 扫描（Scanning）：黑客利用专门工具扫描目标网络的漏洞和弱点，寻找可以入侵的漏洞。扫描时间一般会比较长，因为黑客需要探测目标网络的开放端口、安全漏洞和系统弱点。
3. 入侵（Exploitation）：黑客通过发现的漏洞和技术手段，入侵目标网络，并获取足够的权限。这可能包括猜测密码、使用暴力破解工具或利用网站漏洞等方式，获取目标系统的访问权限。
4. 控制（Control）：黑客获得足够的权限后，还可能对目标系统进行控制，例如安装后门等恶意软件，使得黑客可以在任意时间进入目标系统控制。
5. 数据窃取（DataExfiltration）：黑客在掌控目标系统后，可以窃取敏感数据，如用户凭证、信用卡号、个人信息等。这些数据可用于盗窃身份、进行诈骗等。
6. 清除痕迹（CoveringTracks）：最后，黑客会试图清除自己的痕迹，使得被攻击者难以追踪

他们的活动。他们可能会删除系统日志、删除攻击工具和脚本、卸载恶意软件等。
总之，黑客攻击是一个复杂的过程，需要通过多个阶段来获得目标网络的访问权限和控制权，因此需要采取多种方法来防范黑客攻击。

4.分布式拒绝服务攻击技术。

分布式拒绝服务（DDoS）攻击是一种通过利用大量的计算机来同时向一个目标发起攻击的攻击方式，从而让目标系统无法正常工作。这种攻击方式通常由多个被攻击者控制的计算机（也称为“僵尸网络”或“肉鸡”）共同发起攻击，从而难以追溯攻击来源。因为攻击来源的多样性，分布式拒绝服务攻击也很难被防御和缓解。分布式拒绝服务攻击是一种恶意攻击方式，其攻击方式具有高效、隐蔽、高峰等特点，对目标系统造成的影响会很大，因此需要采取多种手段进行防御和缓解。

5.TCP/IP 参考模型

TCP/IP 参考模型是网络通信协议中最基本的模型，由若干个层次组成，每一层次都有对应的协议和规范。该模型分为 4 层，自下而上分别是：
1. 网络接口层（Network Interface Layer）：负责控制计算机硬件设备和操作系统内核之间的通信，以及与物理网络进行通信。该层次包括网卡驱动程序、MAC 地址、物理连接等内容，对应协议是以太网等。
2. 网际层（Internet Layer）：负责实现数据在网络中的传输和寻址。该层次包括 IP 地址和路由器等内容，对应协议是 Internet Protocol（IP）。
3. 运输层（Transport Layer）：负责在网络节点之间的数据传输和管理。该层次包括传输协议（如 TCP 和 UDP）和端口号等内容。
4. 应用层（ApplicationLayer）：负责支持应用程序的数据传输和处理。该层次包括 HTTP、FTP、SMTP 等协议和应用程序的接口。

6.漏洞扫描的三个阶段

1. 识别：在这个阶段，漏洞扫描器将确定待测系统上运行的服务、开放端口，以及系统的操作系统类型和版本等信息。漏洞扫描器利用这些信息来判断系统的漏洞库，并确定必须执行哪些漏洞检测脚本。
2. 探测：在这个阶段，漏洞扫描器对目标系统进行测试，以寻找漏洞和弱点。漏洞扫描器将尝试使用已知的漏洞或未公开的漏洞来攻击目标系统。如果该系统存在漏洞，则漏洞扫描器将能够利用漏洞跨越系统的安全边界。漏洞扫描器可以执行端口扫描、漏洞脚本扫描、弱密码枚举、SQL 注入、跨站点脚本等攻击方法来探测漏洞。
3. 报告：在这个阶段，漏洞扫描器将生成包含漏洞和弱点信息的报告。报告将详细说明哪些漏洞是存在的、漏洞的严重性、以及可能的威胁和风险。漏洞扫描器还将提供一些漏洞修复建议和安全措施，以帮助组织修复这些漏洞并提高系统的安全性。

7.典型的社会工程学攻击方法

1. 钓鱼攻击（Phishing attack）：攻击者通过伪造的网站、电子邮件或短信等方式骗取个人和机构的敏感信息，比如账号、密码、信用卡号等。攻击者通常会假装成银行、政府机构、电商等信誉好的机构进行欺骗，让用户自己输密码或安装恶意软件。
2. 电话诈骗（Vishing attack）：攻击者通过电话欺骗的方式，以声音欺骗来获取个人信息或敏感信息。攻击者通常会假扮成银行、警局、政府机构等重要组织，以信誉好的机构身份骗取个人信息。
3. 假冒攻击（Impersonation attack）：攻击者冒充有权的身份、访问和操作受保护资源，以达到获取机密的目的。攻击者可能会伪装成合法的用户或管理员，通过伪造证书、信息或其他手段来进行攻击。
4. 社交工程学攻击（Social engineering attack）：攻击者通过利用人性弱点、社交工程学原理和心理学技巧，以欺骗或其他欺诈行为为钓鱼攻击的前提，达到获取信息、侵犯安全和骗取财产等目的。
5. 垃圾邮件攻击（Spamming attack）：攻击者通过 FTP、电子邮件和即时消息等途径向用户发送广告、诈骗信息、病毒等恶意代码。

8.计算机病毒的特点

1. 自我复制：计算机病毒可以自我复制并传播，感染更多的计算机系统。病毒会将自身代码复制到其他程序中，或者将自己作为附件传播。
2. 隐藏性：计算机病毒被设计为隐蔽或伪装，以逃避安全软件的检测和防范。病毒可能会修改自己的文件名或位置，并将自己隐藏在其他程序中。
3. 危害性：计算机病毒的目的是破坏、修改或窃取系统数据和信息，或者在计算机用户不知情的情况下控制计算机系统。病毒可以销毁数据、加密文件、挂马、勒索等危害用户。
4. 传播性：计算机病毒可以利用计算机系统和网络传播，通过电子邮件、网络分享、广告等方式进行传播，造成更广泛的影响。
5. 难以防范：计算机病毒可以很难被发现和防范，因为它们经常会隐蔽地感染计算机系统，利用计算机程序和用户行为的漏洞，隐藏自己以逃避检测。

9.IPv6 的优点

1. IP 地址空间扩大：IPv6 地址空间远远超过 IPv4 地址空间，可满足更多的 IP 地址需求。IPv4 的地址只有 4 个字节的长度，共计 32 位，约 42 亿个地址，而 IPv6 的地址则为 128 位，理论上可以提供 340 万亿亿亿亿个地址，远远满足当前和未来的需求。
2. 提高网络效率：IPv6 使用了分层的地址结构和简化的头部格式，并支持多种传输方式和多播组播，使得网络数据流更加高效和流畅。
3. 提供更好的安全性：IPv6 引入了 IPSec（Internet Protocol Security）协议，支持数据加密和身份验证，大大提高了网络的安全性和保密性。
4. 简化网络管理：IPv6 提供了新的配置选项（如自动配置和无状态配置），使网络管理更加简单和灵活，同时还提供了更好的负载平衡和路由功能，有助于提高整个网络系统的处理效率。

5. 支持新兴的应用：IPv6 为支持新兴的应用提供了更好的支持，比如云计算、移动设备、物联网和虚拟现实等应用领域，有助于推动互联网技术向前发展。

10.IPv4 不足之处

1. 地址空间有限：IPv4 地址只有 32 位长度，可以分配的地址数量有限，总共只有 42 亿个可用的地址。随着互联网的快速发展，IPv4 地址已经面临严重短缺的问题。
2. 安全性不足：IPv4 协议并没有内置的安全性功能。许多互联网攻击都会针对地址和数据包进行攻击，如 IP 地址劫持、MAC 地址欺骗等，IPv4 缺乏相应的安全机制，容易受到大规模攻击。
3. 路由表过大：IPv4 网络必须具有一个全局路由系统，每一个路由器都必须维护完整的路由表。这样随着互联网规模的增加，路由器在维护路由表和处理数据包时的开销也在不断增加。
4. 无法满足新兴的需求：IPv4 无法满足新兴需求，例如大规模的物联网和云计算等领域，这些应用需要大量的独立 IP 地址，超出了 IPv4 地址空间所能提供的容量。

11. VPN 的主要优点和局限性。

优点：
1. 加密通信：VPN 可以对通信数据进行加密，保证了数据的机密性。只有正确解密的数据才能被互相理解，保证数据传输的安全性和稳定性。
2. 防止黑客攻击：VPN 可以在公共网络环境下建立安全隧道，防止黑客对数据包进行窃听、欺骗和拦截，能够提高网络安全性，防止企业的机密资料被泄漏。
3. 提升网络的可靠性：VPN 可以有效解决远程访问和数据传输中的网络延迟和带宽瓶颈等问题，提高了网络的可靠性，提高了企业的办公效率和生产效益。
4. 跨区域办公：VPN 可以让企业在不同地区甚至不同国家的办公室间建立虚拟私人网络，在数据和信息共享方面达到无缝协作的目的，便于跨区域办公。
5. 降低成本：VPN 可以降低企业的网络成本，优化企业的网络结构，将数据传输的网络费用降到最低，提高了企业的效益。

局限性：
1. 网络质量的影响：由于公共网络的原因，VPN 中数据传输的稳定性、速度受到网络质量的影响，偶尔会出现断线等问题。
2. 安全威胁：一些不良分子可能会利用 VPN 来进行非法的攻击和入侵，或者通过用户的 VPN 登录来盗用用户的隐私数据。
3. 配置管理难度：VPN 需要进行配置和管理，企业需要专业技术人员进行管理和设置，如果管理不当，可能会出现一些安全隐患和问题。
4. 成本因素：企业需要投入一定量的资金来购买 VPN 解决方案，需要购买专用硬件和软件，以及支付专业技术人员的工资。

12.电子商务中，安全电子交易 SET 系统中双重签名的作用？它是怎样实现的？

双重签名的作用：
在 SET 系统中，每次交易中都需要付款人和收款人都进行数字签名，分别对支付订单进行签名，这种签名称为单向签名。而双重签名则是指，付款人在签署付款订单（单向签名）的基础上，再对整个交易（包括订单和收据）进行签名，以防止收款人伪造交易的情况发生。这样，在交易时，需要付款人通过私钥对整个交易信息进行签名，确保交易的真实性和完整性，同时也提高了交易的可信性。双重签名可以使得 SET 系统中的交易更加安全，防止交易信息被篡改、伪造或者否认。

实现方式：
具体实现中，双重签名可以使用随机数生成器和公、私钥组成的数字签名来实现。付款人可以使用自己的私钥对交易信息进行数字签名，此时接收方可以使用付款人的公钥进行验证签名的真实性和完整性。然后，在签名的基础上，邀请收款人对整个交易再进行一次签名，以生成双重签名，此时接收方必须使用双重签名进行验证。