（1）“零日攻击”是一种什么样的攻击形式？为什么说这种攻击极其危险？

零日（zero-day）攻击是一种利用计算机系统或应用中未知漏洞的攻击，是一种与漏洞的发现几乎同时的攻击行为。

由于漏洞刚被发现，没有任何相应的补丁可以补救，因此零日攻击行为的危险性极大，成功率也极高。

（2）在信息安全的基本属性中，C、I、A 分别是指什么属性？分别可采用哪些保障措施？

C：机密性（Confidentiality）。机密性的保障技术主要包括：物理保密技术（监控、门禁等）、防电磁辐射泄露技术、网络防截获和防窃听技术、加密和解密技术等。

I：完整性（Integrity）。完整性包括数据完整性和系统完整性，完整性的保障技术主要包括：报文摘要、加密、数字签名等技术。

A：可用性（Availability）。可用性的保障技术主要包括：实时的备份与恢复、设备和线路冗余、集群和虚拟化等技术。

（3）社会工程学是一种什么样的黑客攻击方法？

社会工程学是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段以便取得自身利益的方法。

准确来说，社会工程学不是一门科学，而是一种艺术和窍门的方术。因为社会工程学攻击不是总能重复和成功，而且在信息充分多的情况下，会自动失效。社会工程学的窍门也蕴涵了各式各样的灵活的构思与变化因素。

（4）为什么说不可否认性是为了防范来自合法用户的攻击？包括哪几种类型？可采用的保障措施是什么？

因为：防止抵赖。

包括**原发不可否认**和**接收不可否认**：**原发不可否认**用于防止发送者否认自己已发送的数据和数据内容；**接收不可否认**用于防止接收者否认已接收过的数据和数据内容。

不可否认性的保障技术主要包括：身份认证技术（包括数字签名、数字证书、IC 或 USBkey 令牌、指纹、视网膜、掌形、脸形等）来保证。

（5）APT 攻击有哪几种形式？各有什么特点？

APT 攻击：高级持续性渗透攻击（Advanced Persistent Threat, APT）是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。

①鱼叉式网络钓鱼。锁定目标后，黑客假冒各种名义以电子邮件等方式向目标发送难辨真伪文档，诱使其上当，借机在其计算机上安装特洛伊木马或其他间谍软件，以窃取机密或进一步渗透的目的。

②水坑式攻击。水坑式攻击（Waterhole attacks）是近年来新起的一种 APT 攻击行为，是指黑客通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待被攻击者来访时实施攻击。

****

（6）SSL 协议的位置在 TCP/IP 体系结构的哪个层次？由哪几个协议组成？

SSL 协议位于 TCP/IP 协议族的传输层与应用层之间，共有两层，分别是：

上层：握手协议、密码变化协议、警告协议，用于管理 SSL 密钥信息的交换；

底层：记录协议，提供基本的安全服务。

（7）在 OSI 的安全体系结构中，安全服务和安全机制之间有什么关系？分别有哪几种类型？

安全服务：安全服务（也称为安全功能）是指为加强网络信息系统安全性和对抗网络攻击行为而采取的一系列技术措施。包括：鉴别、访问控制、数据机密性、数据完整性、不可否认性。

安全机制：安全机制是安全服务的技术实现手段。一种安全服务可以通过多个安全机制加以实现；同样地，一个安全机制也可以为多种安全服务的实现提供实现的措施。包括：加密机制、数字签名机制、访问控制机制、数据完整性机制、认证机制、业务流填充机制、路由控制机制和公证机制。

每一种安全服务既可以由一种安全机制提供，也可以由几种安全机制联合提供。

OSI：在 OSI 安全体系结构中，定义了五大类安全服务、八类安全机制，以及相应

的安全管理，并指出可根据具体的系统需求在 OSI 七层模型中进行适当的配置。

（8）在 IPSec 协议中，传输模式和隧道模式有什么显著的不同？

IPSEC ×××	原理	加密设备是否等于通信设备	使用条件	举例
传输模式	在原始 IP 头部和 IP 负载之间插入一个 ESP 头部，并且在最后面加上 ESP 尾部和 ESP 验证数据部分	加密设备等于通信设备	相互通信的设备 IP 地址必须在其间的网络可路由	内部网络的主机要安全的访问内部服务器资源。
隧道模式	把原始 IP 数据包整个封装到一个新的 IP 数据包中，在新的 IP 头部和原始 IP 头部之间插入 ESP 头部，并且在最后面加上 ESP 尾部和 ESP 验证数据部分	加密设备不等于通信设备	相互通信的设备 IP 地址在其间的网络是不可路由的	一个内部网络的主机要安全穿越 internet 访问另一个内部网络的资源。如 IPSEC ***

（9）在 TCP/IP 的安全体系结构中，在网络层、传输层和应用层各有什么样的安全协议？

网络层：IP/IPSec；

传输层：TCP、UDP；

应用层：FTP、SMTP、HTTP。

（10）IPSec 的 AH 协议和 ESP 协议有什么显著不同？

AH 验证的区域是除可变字段以外的整个 IP 包，包括 IP 包头部，因此源 IP 地址、目的 IP 地址是不能修改的，否则会被检测出来。

ESP 除了可以提供无连接的完整性验证、数据来源验证和抗重放攻击服务之外，ESP 还提供数据包加密和数据流加密服务。ESP 的验证范围不包括 IP 包首部。

****

（11）说说你对 SSL 特点的认识。

优点：

①SSL 设置简单成本低，无须在自己的电脑 L 安装专门软件，只要浏览器支持即可；

②通信前就已完成加密算法，此后所有数据都会被加密，从而保证通信的安全性。

缺点：

①除了传输过程外不能提供任何安全保证；

②不能提供交易的不可否认性；

③客户认证是可选的，所以无法保证购买者就是该信用卡合法拥有者；

SSL 不是专为信用卡交易而设计，在多方参与的电子交易中，SSL 协议并不能协调各方间的安全传输和信任关系。

（12）说说你对 PDR 模型的认识，如基本思想、基本观点等。

基本思想：

信息系统中不可避免存在各种漏洞，这些漏洞本身不会对信息系统造成损害，但是一旦被利用就会成为系统的威胁；

任何安全防护措施都与时间相关。如果给予无限的时间，任何防护措施都能够被攻破。

基本观点：

PDR 模型中的保护（Protection）：保护是安全的第一步。

PDR 模型中的检测（Detection）：再完美的安全防御措施都无法确保系统 100%的安全。昨天的补丁可能会在今天发现新的漏洞。因此，需要开展实时监控。

（13）在 TCSEC 中，TCB 包含了哪些内容？哪些系统达到了 C2 级？

在 TCSEC 中，TCB 是实施系统安全策略时必须信任和依赖的软件（通常是操作系统内核）、硬件、固件和人等。

达到 C2 级的系统：高版本的 Unix、Windows NT、Windows xp、Windows2000、Oracle

（14）我国的《计算机信息系统安全保护等级划分准则》是按照什么为依据进行信息系统等级的划分？共划分了几个等级？

划分依据：计算机系统安全保护能力。

第一级：用户自主保护级；

第二级：系统审计保护级；

第三级：安全标记保护级；

第四级：结构化保护级；

第五级：访问验证保护级。

（15）说说你所理解的 PDR 模型与 PPDR 模型的显著不同。

和 PDR 不同，PPDR 强调在防护、检测和响应的各个环节都要依据安全策略进行实施。