**1.什么是IP地址扫描**

利用**ICMP**的回应请求与应答报文，运用**ping**探测目标地址，对此作出响应，表示其存在。

**2.简述CSMA/CA的工作流程**

先听后发，边发边听，冲突停发，随机延迟后重发。

（ 发送数据前 先侦听信道du是否空闲 ,若空闲，则立即发送数据。若信道忙碌，则等待一段时间至信道中的信息传输结束后再发送数据；

若在上一段信息发送结束后，同时有两个或两个以上的节点都提出发送请求，则判定为冲突。若侦听到冲突,则立即停止发送数据，等待一段随机时间,再重新尝试。）

**3.什么是TCP SYN攻击**

攻击主机伪造源IP地址，向目标主机的特定TCP端口发送许多SYN包，目标主机回复确认包，由于源地址是不存在的，目标主机需要不断地重发直至超时，伪造的SYN包将长时间占用连接队列，正常的SYN请求被丢弃，导致目标主机内存资源不断消耗，直至枯竭。

**4.计算机病毒与蠕虫的区别**

（1）存在形式：蠕虫是独立的程序；计算机病毒是寄生于宿主文件的。

（2）攻击目标：蠕虫感染网络；计算机病毒攻击本地文件。

（3）主动性：蠕虫主动攻击；计算机病毒随着宿主而运行。

**5.无限局域网的安全需求有哪些**

（1）数据机密性：对传输数据进行加密。

（2）数据完整性：防止空中传输的数据遭到非授权

**6.什么是泪滴攻击**

将IP数据包分成很多小片段，通过发送伪造的相互重叠的数据包，使其难以被接收主机重新组合，造成资源缺乏甚至机器重启。

**7.Smurf攻击的原理是什么**

攻击者向网络广播地址发送ICMP包,并将回复地址设置成目标网络的广播地址,通过使用ICMP应答请求数据包来淹没目标主机的方式进行,最终导致该网络的所有主机都对次ICMP应答请求作出答复,导致网络阻塞。

**8.简述计算机蠕虫的组成**

（1）扫描模块：探测目标主机。

（2）感染模块：感染目标计算机。

（3）功能执行模块：执行蠕虫设计者预定义的功能。

**9.简述共享密钥的认证过程**

①客户端发送一个认证请求 Authentication Request给无线接入点要求进行共享密钥认证

②无线接入点回复一个认证响应信息Authentication Response,包含挑战信息;

③客户端使用本地配置的WEP密钥加密挑战信息,然后回复一个认证请求;

④无线接入点解密收到的认证信息,如果得到最初的挑战信息,然后回复一个认证响应信息同意客户接入。

**10.虚拟机技术怎么防病毒**

让一个物理平台同时运行多个操作系统，避免病毒导致单一应用崩溃对整个系统的影响，增强可迁移性。利用主流虚拟机技术如：虚拟硬件模式，虚拟操作系统模式和Xen模式等，以及运用VT技术。

**11.VLAN中涉及哪些协议，协议的作用是什么？**

 交换链路内协议（ISL）:给VLAN做标记，维护交换机和路由器间的通信流量；

VLAN中继协议（VTP）:做VLAN同步，管理在同一个域的网络范围内VLANs的建立、删除和重命名，让其自动同步。

**12.网络侦听的原理是什么**

利用共享式的网络传输介质，将网卡设置为混杂模式，并利用数据链路访问技术来实现对 网络的侦听。

**13.DDos攻击主要有哪两种手段**

（1）用大数据，大流量来压垮网络设备和服务器。

（2）有意制造大量无法完成的不完全请求来快速耗尽服务器资源。