1. 黑客攻击的一般过程是什么？

（1）预攻击（踩点和扫描）：收集信息，进行进一步攻击决策，内容：获得域名及IP分布，获得拓扑及OS等，获得端口和服务，获得应用系统情况，跟踪新漏洞发布

（2）攻击（入侵、获取权限、提升权限）：进行攻击，获得系统的一定权限。内容：获得远程权限，进入远程系统，提升本地权限，进一步扩展权限，进行实质性操作

（3）后攻击（清除日志、安插后门）：消除痕迹，长期维持一定的权限。内容：植入后门木马，删除日志，修补明显的漏洞，进一步渗透扩展

2. 网络信息安全产生的原因有哪些？

（1）物理安全因素（物理设备和通信线路）

物理设备本身问题:元器件的老化、设计的不合理、电子辐射等;

物理设备的位置安全：设备摆放不当处于易破坏的地方或物理上不安全的地方;

物理设备的环境安全:地震、雷击、潮湿、电子辐射干扰等；

（2）方案设计因素

安全策略不合理或安全配置不当；

方案设计本身存在缺陷：实现异构网络信息系统之间的通信，实现更高的开放性，需要牺牲一定安全机制的设置和实现

（3）系统的安全因素

操作系统的安全性:如Windows系列的Unicode漏洞、 IIS漏洞，UNIX系列的NIS漏洞、Finger漏洞、RPC漏洞、 Sendmail漏洞等；LINUX的“心脏出血”(Heartbleed)漏洞、Bash漏洞、strust远程代码执行漏洞等

网络应用软件的漏洞和“后门”“隐通道”:网络软件包括系统中间件软件（如tomcat）和应用软件。

（4）TCP/IP协议的安全因素

网络的开放性，因特网最初的设计只考虑该网会不会因为局部故障而影响信息的传输,基本没有考虑安全问题,因此TCP/IP协议族软件本身缺乏安全性。

（5）人的因素

人员无意的失误和错误行为,如操作员安全配置不当造成的安全漏洞, 用户口令选择不慎, 帐号随意转让,租借和共享等;

人员的恶意攻击（主动或被动）:如黑客攻击,非法的信息盗取,信息资源的非法使用,篡改，病毒和恶意攻击软件等;

管理上的因素:疏于安全方面的管理, 安全管理制度和规范缺乏或不完善;

3. 什么是社会工程学攻击？

社会工程学（Social Engineering），是一种通过受害者心里弱点、本能反应、好奇心、信任、贪婪等心里陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。

黑客社会工程学是非传统的信息安全，它不是利用软件或系统的漏洞实现入侵的，黑客通过社会工程学攻击的方式只需要拨打一个电话，使用专用的术语，报出内部人员使用的账号信息，获取更多的信息，从而轻松绕过所有技术上的防护，实现恶意攻击的目的。

常用的手段:环境渗透、引诱、伪装、恐吓、恭维、说服

4. 常见的攻击方法有哪些？什么是缓冲区溢出攻击？

(1) 网络监听攻击：网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网络上传输的信息，取得目标主机超级用户权限。

(2) 密码破解/绕过windows登录验证机制

(3) 会话劫持攻击: 在一次正常的通信过程中，黑客作为第三方参与其中，或者是在数据流（例如基于TCP的会话）里注射额外的信息，或者监听双方会话，将双方的通信模式暗中改变，即从直接联系变成有黑客联系。

(4) 缓冲区溢出攻击：缓冲区溢出攻击又称堆栈溢出：简单地说就是程序对接受的输入数据没有进行有效检测导致的错误，后果可能造成程序崩溃或者是执行攻击者的命令。

通过造成缓冲区溢出并用指定地址覆盖返回地址而进入指定程序的方式来获得系统权限。

（5）拒绝服务攻击：即攻击者利用系统缺陷，通过执行一些恶意的操作而使得合法的系统用户不能及时地得到应得的服务或系统资源，即让目标机器停止提供服务或资源访问：这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。

（6）网络蠕虫：蠕虫是一段独立的可执行程序，它可以通过计算机网络把自身的拷贝（复制品）传给其他的计算机，主要利用操作系统和应用程序漏洞传播，通过网络的通信功能将自身从一个结点发送到另一个结点并启动运行的程序，可以造成网络服务遭到拒绝并发生死锁。

（7）木马攻击: 木马实质是一个通过特定端口进行通信的网络客户端/服务器程序，使用多种手段伪装自己

（8）SQL注入攻击：攻击者把SQL命令插入到Web表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的SQL命令。