1. 网络攻击的一般流程：

包括系统调查、系统安全缺陷探测、实施攻击，巩固攻击成果和及痕迹清理五个阶段。

① 系统调查是攻击者通过攻击目标主机台，利用公开的协议或工具通过网络收集目标主机相关信息的过程

② 收集到攻击目标的相关特性后攻击者常用自行编制或特定的软件扫描攻击目标，寻找攻击目标系统内的漏洞。

③ 获取到足够的信息后，攻击者就可以结合自身的水平及经验总结制出相应的攻击方法，实施真正的网络攻击。

④ 前期的侵入结果，控制目标系统，完成既定攻击任务。

⑤ 在成功实施攻击后，攻击者会自清除攻击的痕迹。

2. 基本原理：

攻击者通过向目标程序的缓冲区写超过其长度的内容，造成缓冲区溢出，从而破坏程序的堆栈，使程序转而执行其它指令，以达致攻击的目的。

3.

1) SYN洪泛攻击：利用TCP缺陷，发送大量伪造的TCP连接请求，使TCP连接无法第三步完成握手。

2) UDP洪泛攻击：攻击者利用简单的TCP/IP服务来传送占满带宽的线路垃圾数据。通过伪造与某一对主机的服务之间的UDP连接

3) Ping 泛洪攻击：操作系统对TCP/IP堆栈的实现在ICMP包上都是规定为64KB，对包的标题头读取后，根据标题头里包含的信息为有效载荷生成数据缓冲区。产生畸形时，声称自己的尺寸超过ICMP上限的包，也就是加载的尺寸超过64KB上限，就会出现内存分配错误。

4) 泪滴攻击：利用在TCP/IP堆栈中，实现信任IP碎片中包的标题头所附包含的信息来实现自己的攻击。

5) Land攻击：设计一个特殊的SYN包，它的源地址和目标地址都被设置成某个服务器地址。创建一个空连接直至超时。

6) Smurf攻击：通过向一个局域网的广播地址发出ICMP回应请求，并将请求的返回地址设为被攻击的目标主机，导致被大量的应答包淹没，最终导致目标主机崩溃。

4. 1) 感染目标主机，构建僵尸网络

攻击者会通过各种方式侵入主机，植入程序构建僵尸网络。

2) 发布命令，控制僵尸程序

根据命令发布的不同，可以分为推模式和拉模式。推模式是指僵尸程序主机在平时处于等待状态，僵尸控制程序主动向僵尸主机发布命令，僵尸主机只有在被动接收到控制端命令后才进入下一步动作。拉模式是指控制端程序将代码放入在特定位置，僵尸程序会定期读取代码，作为进行下一步动作的命令。

3) 展开攻击

本地攻击指发起针对僵尸网络内部被控制主机的攻击，比如对用户隐私

信息的窃取。远程攻击是指攻击非僵尸网络内部的主机，根据目的不同又分为两类，一类是扩展僵尸网络规模，这类攻击目的是让外部主机感染同样的僵尸程序，最终成为僵尸网络的一部份。另一类攻击是打击，渗透等方式，比如分布式拒绝服务，垃圾邮件等。

4) 攻击善后：主要目的是隐藏攻击痕迹，防止被追踪溯源。

5. 0xbffff02c - 0xbffffeja5 = 135