攻击类型可分为哪些，及各自的特点
木马的含义及木马攻击的过程
DOS 的含义以及 DOS 的攻击过程
TCP 三次握手为例描述 DOS 攻击基本原理
为什么 DOS 难根除

攻击类型：物理攻击，非物理攻击
网络攻击按照是否影响通信分为被动攻击（如截取攻击，主要是收集信息而不是进行访问一般察觉不到）和主动攻击（如阻断攻击、篡改攻击、伪造攻击、重放攻击

网络攻击从安全属性上可分为五类：
1. 截取攻击：
   针对机密性的攻击 如：窃听攻击、流量分析
2. 篡改攻击：（部分篡改
   针对完整性 如：替换攻击
3. 伪造攻击：（完全伪造
   针对认证性 如：欺骗攻击如 DNS
4. 阻断攻击：
   针对可用性 如 DOS 攻击
5．重放攻击：通常使用随机数方法抵御重放攻击

木马的含义：
指附着或单独存在的恶意程序，分为客户端（坏人）和服务端，利用网络远程响应另一端的控制命令，实现对感染木马计算的控制

木马和病毒的主要区别是：木马不具有自我复制性，病毒主要干破坏而木马主要干偷盗

木马的攻击过程：
木马攻击核心技术在植入，植入，连接请求，远程控制，响应，

木马植入的方式：主动（利用漏洞、利用病毒）被动（诱骗，点开网页

DNS 是可以将域名和 ip 地址相互映射的一个分布式数据库

拒绝服务攻击：DoS,阻止或拒绝合法用户存取网络服务的一种破坏性攻击方式，发送大量虚假请求导致网络交通堵塞、毁坏服务器、断电断网

Tcp 三次握手为例的 dos 攻击：
用户向服务器发送 SYN 报文，服务器向用户发出 SYN+ACK 应答报文后收不到用户的 ACK 报文，第三次握手无法完成，期间需要一端时间“SYN 超时”一般是分钟级，攻击者通过伪造 tcp 连接请求来使服务器消耗资源，或无暇理睬，最终系统崩溃

僵尸网络可以实现一对多控制，利用僵尸网络可以同时对目标网站进行分布式拒绝服务攻击 DDoS

拒绝服务攻击永远不会消失，而且没有根本的解决办法
因为可以通过使用一些公开的软件进行攻击，发动较简单，能产生迅速效果，同时防止这种攻击又非常困难