DoS和DDoS的攻击方法浅析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022_DoS_E5_92_8CDDoS_c100_140227.htm 对DoS而言其攻击方式很多，主要使用的攻击有3种，分别是TCP-SYN flood、UDP flood和ICMP flood。当用户进行一次标准的TCP连接时，会有一个3次握手过程。首先是请求服务方发送一个SYN消息，服务方收到SYN后会向请求方回送一个SYN-ACK表示确认，当请求方收到SYN-ACK后，再次向服务方发送一个ACK消息，这样，一次TCP连接建立成功。但是TCP-SYN flood在实现过程中只进行前2个步骤：当服务方收到请求方的SYN-ACK确认消息后，请求方由于采用源地址欺骗等手段使得服务方收不到ACK回应。于是，服务方会在一定时间处于等待接收请求方ACK消息的状态。对于某台服务器来说，可用的TCP连接是有限的，如果恶意攻击方快速连续地发送此类连接请求，该服务器可用的TCP连接队列将很快被阻塞，系统可用资源急剧减少，网络可用带宽迅速缩小。长此下去，网络将无法向用户提供正常的服务。 由于UDP（用户数据包协议）在网络中的应用比较广泛，基于UDP攻击种类也较多。如今在Internet上提供WWW和Mail等服务设备通常是使用Unix的服务器，它们默认一些被恶意利用的UDP服务，如echo和chargen服务，它会显示接收到的每一个数据包，而原本作为测试功能的chargen服务会在收到每一个数据包时随机反馈一些字符，如果恶意攻击者将这2个UDP服务互指，则网络可用带宽将很快耗尽。 目前，我们知道的对网络进行DDoS攻击所使用的工具有：Trinoo、Tribe Flood Network（TFN）

、TFN2k和Stacheldraht等。它们的攻击思路基本相近。
1.Trinoo：它是基于UDP flood的攻击软件，它向被攻击目标主机的随机端口发出全零的4字节UDP包，在处理这些超出其处理能力垃圾数据包的过程中，被攻击主机的网络性能不断下降，直到不能提供正常服务，乃至崩溃。它对IP地址不做假，此攻击方法用得不多。 2.TFN：它是利用ICMP给代理服务器下命令，其来源可以做假。它可以发动SYN flood、UDP flood、ICMP flood及Smurf（利用多台服务器发出海量数据包，实施DoS攻击）等攻击。TFN的升级版TFN2k的特点是：对命令数据包加密、更难查询命令内容、命令来源可以做假，还有一个后门控制代理服务器。 3.Stacheldraht：对命令来源做假，而且可以防范一些路由器用RFC2267过滤。若检查出有过滤现象，它将只做假IP地址最后8位，从而让用户无法了解到底是哪几个网段的哪台机器被攻击。此外，它还具有自动更新功能，可随软件的更新而自动更新。 值得一提的是，像Trinoo和TFN等攻击软件都是可以从网上随意找到的公开软件，所以任何一个上网者都可能构成网络安全的潜在威胁。
面对凶多吉少的DDoS险滩，我们该如何对付随时出现的黑客攻击呢？杨宁先生说，那要看用户处于何种状态，是正身处被攻击的困围中，还是准备事先预防。 