洪水攻击

洪水攻击是现在黑客比较常用的一种攻击技术，特点实施简单，威力巨大，大多无视防御
洪水攻击通俗的理解就是让你的服务器资源耗尽，无法提供正常的服务

ddos只不过是洪水攻击的一种。

网络泛洪包括Smurf和DDos： smurf发生在OSI第三层，就是假冒ICMP广播ping，如果路由器没有关闭定向广播，那攻击者就可以在某个网络内对其它网络发送定向广播ping，哪个网络中的主机越是多，造成的结果越是严重，因为每个主机默认都会响应这个ping，导致链路流量过大而拒绝服务，所以属于增幅泛洪攻击，当然也可以对本网络发送广播ping。

DDos发生在OSI第三、四层，攻击侵入许多因特网上的系统，将DDos控制软件安装进去，然后这些系统再去感染其它系统，通过这些代理，攻击者将攻击指令发送给DDos控制软件，然后这个系统就去控制下面的代理系统去对某个IP地址发送大量假冒的网络流量，然后受攻击者的网络将被这些假的流量所占据就无法为他们的正常用户提供服务了。

TCP SYN泛洪发生在OSI第四层，这种方式利用TCP协议的特性，就是三次握手。攻击者发送TCP SYN，SYN是TCP三次握手中的第一个数据包，而当服务器返回ACK后，该攻击者就不对其进行再确认，那这个TCP连接就处于挂起状态，也就是所谓的半连接状态，服务器收不到再确认的话，还会重复发送ACK给攻击者。这样更加会浪费服务器的资源。攻击者就对服务器发送非常大量的这种TCP连接，由于每一个都没法完成三次握手，所以在服务器上，这些TCP连接会因为挂起状态而消耗CPU和内存，最后服务器可能死机，就无法为正常用户提供服务了。

最后应用程序泛洪发生在OSI第七层，目的是消耗应用程序或系统资源，比较常见的应用程序泛洪是什么呢？没错，就是垃圾邮件，但一般无法产生严重的结果。其它类型的应用程序泛洪可能是在服务器上持续运行高CPU消耗的程序或者用持续不断的认证请求对服务器进行泛洪攻击，意思就是当TCP连接完成后，在服务器提示输入密码的时候停止响应。

对于大部分的攻击都能通过IDS来防御或日志分析来判断。

常见的洪水攻击方式

阿拉丁洪水攻击器 局域网ARP攻击
以及ddos攻击