TCP SYN 泛洪：

对于TCP协议，当客户端向服务器发起连接请求并初始化时，服务器一端的协议栈会留一块缓冲区来处理“握手”过程中的信息交换。请求建立连接时发送的数据包的包头SYN位就表明了数据包的顺序，攻击者可以利用在短时间内快速发起大量连接请求，以致服务器来不及响应。同时攻击者还可以**伪造源IP** **地址**。也就是说攻击者发起大量连接请求，然后挂起在半连接状态，以此来占用大量服务器资源直到拒绝服务。虽然缓冲区中的数据在一段时间内（通常是三分钟）都没有回应的话，就会被丢弃，但在这段时间内，大量半连接足以耗尽服务器资源。

TCP LAND:

LAND攻击利用了TCP连接建立的三次握手过程，通过向一个目标主机发送一个用于建立请求连接的TCP SYN报文而实现对目标主机的攻击。与正常的TCP SYN报文不同的是：LAND攻击报文的源IP地址和目的IP地址是相同的，都是目标主机的IP地址。这样目标主机接在收到这个SYN 报文后，就会向该报文的源地址发送一个ACK报文，并建立一个TCP连接控制结构，而该报文的源地址就是自己。由于目的IP地址和源IP地址是相同的，都是目标主机的IP地址，因此这个ACK 报文就发给了目标主机本身。