网络安全技术课堂作业八（二）

朱浩泽 计算机科学与技术 1911530

简述拒绝服务攻击的检测方法

一般来说就是局部区域的流量异常，比如说检测到源地址相同的数据包有很多或者目的地址相同的数据包有很多，即可初步认定为拒绝服务攻击。在现在的潮流中，还有些利用机器学习去检测的，将包的特征比如持续时间等作为输入，对模型进行训练，进行检测。我们还可以进行如下的具体检测：

1. 检查网站后台服务器发现大量无用的数据包
2. 检测服务器主机上是否有大量等待的TCP连接
3. 检测网络流量出现异常变化突然暴涨
4. 检测大量访问源地址是虚假的
5. 当发现Ping超时或丢包严重时，且同一交换机上的服务器也出现了问题，不能进行正常访问