**第七章 课后作业**

1、为了进行经典的DoS洪泛攻击，攻击者必须能够制造出足够大量的数据包来占据目标系统的链路容量。假设现在有一个利用ICMP回送请求（ping）数据包的DoS攻击，数据包的大小为500字节（忽略成帧开销）。对于一个使用0.5Mbps带宽链路的目标组织来说，攻击者每秒钟至少要发送多少个数据包，才能进行有效的攻击？在链路的带宽为2Mbps和10Mbps的情况下呢？

**0.5Mbps的情况下：**

0.5Mb = 0.5 \* 10^6 / 8 = 625000B

n = 625000/500 = 1250（个）

**2Mbps的情况下：**

n = 1250 \* 4 = 5000（个）

**10Mbps的情况下：**

n = 5000\*5 = 25000（个）

2、在TCP SYN欺骗攻击中，攻击者的目的是使目标系统上的TCP连接请求表溢出，以致系统对合法连接请求不能进行响应。假设目标系统上的TCP连接请求表表项为256项，目标系统的每次超时时间为30秒，允许超时次数为5次。如果一个连接请求超时没有应答，而且超时次数大于5，那么这个请求将会被从TCP连接请求表中清除。在没有相关的应对措施和攻击者已经占满了目标系统的TCP连接请求表的情况下，为了能够持续占满目标系统的TCP连接请求表，攻击者应该以什么样的速率发送TCP连接请求？如果TCP SYN数据包的大小为40字节（忽略成帧开销），那么攻击者所发送的请求数据包将消耗掉目标系统多少带宽？

根据题意，目标系统发出的确认数据包超时6次后，会从连接请求表中删除一项。也就是对于一个TCP连接请求表项，需要180秒才会被删除。为了占满256个表项，需要在180秒内连续发送256个TCP连接请求，发送速度为256/180=1.42个/s，也就是平均每秒发送1.42个TCP请求。同样，在占满目标系统的TCP连接请求表后，每隔1/1.42秒，会由于超时6次，TCP连接请求表会删除前面的表项。因此，为了持续占满目标系统的TCP连接请求表，需要以1.42个/s速度发送TCP连接请求。

由于每180秒目标系统会发出256个40B确认报文，占用带宽为40\*8 \*256/180= 455bps。

3、为了进行DNS放大攻击，攻击者必须制造出足量的数据包，来触发中间媒介产生大量的DNS应答数据包给目标系统，并耗尽目标系统的网络带宽。假设，DNS应答数据包的大小为500字节（不计头部），攻击者每秒钟至少要使中间媒介产生多少个DNS应答数据包才能有效地攻击网络带宽分别为0.5Mbps、2Mbps和10Mbps的目标系统？如果DNS请求数据包的大小为60字节，那么对于上述三种带宽的攻击，攻击者要分别消耗多少的本地带宽？

**0.5Mbps：**

n = 0.5 \* 10^6 / 8 / 500 = 125（个）

W = 125 \* 60 \* 8 = 6\*104 bps

**2Mbps：**

n = 125 \* 4 =500（个）

W = 500 \* 60 \* 8 = 2.4\*105 bps

**10Mbps：**

500 \* 5 = 2500（个）

W = 2500 \* 60 \* 8 = 1.2\*106 bps