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 = $6*10^4$ bps

2Mbps：

n = 125 * 4 =500（个）

W = 500 * 60 * 8 = $2.4*10^5$ bps

10Mbps：

500 * 5 = 2500（个）

W = 2500 * 60 * 8 = $1.2*10^6$ bps