ACK Flood 攻击原理与防护

1 原理

ACK Flood 攻击是在 TCP 连接建立之后，所有的数据传输 TCP 报文都是带有 ACK 标志位的，主机在接收到一个带有 ACK 标志位的数据包的时候，需要检查该数据包所表示的连接四元组是否存在，如果存在则检查该数据包所表示的状态是否合法，然后再向应用层传递该数据包。如果在检查中发现该数据包不合法，例如该数据包所指向的目的端口在本机并未开放，则主机操作系统协议栈会回应 RST 包告诉对方此端口不存在。

这里，服务器要做两个动作：查表、回应 ACK/RST。这种攻击方式显然没有 SYN Flood 给服务器带来的冲击大，因此攻击者一定要用大流量 ACK 小包冲击才会对服务器造成影响。按照我们对 TCP 协议的理解，随机源 IP 的 ACK 小包应该会被 Server 很快丢弃，因为在服务器的 TCP 堆栈中没有这些 ACK 包的状态信息。但是实际上通过测试，发现有一些 TCP 服务会对 ACK Flood 比较敏感，比如说 JSP Server，在数量并不多的 ACK 小包的打击下，JSP Server 就很难处理正常的连接请求。对于 Apache 或者 IIS 来说，10kpps 的 ACK Flood 不构成危胁，但是更高数量的 ACK Flood 会造成服务器网卡中断频率过高，负载过重而停止响应。可以肯定的是，ACK Flood 不但可以危害路由器等网络设备，而且对服务器上的应用有不小的影响。

如果没有开放端口，服务器将直接丢弃，这将会耗费服务器的 CPU 资源。如果端口开放，服务器回应 RST。

2 ACK Flood 防护

利用对称性判断来分析出是否有攻击存在。所谓对称型判断，就是收包异常大于发包，因为攻击者通常会采用大量 ACK 包，并且为了提高攻击速度，一般采用内容基本一致的小包发送。这可以作为判断是否发生 ACK Flood 的依据，但是目前已知情况来看，很少有单纯使用 ACK Flood 攻击，都会和其他攻击方法混合使用，因此，很容易产生误判。

一些防火墙应对的方法是：建立一个 hash 表，用来存放 TCP 连接“状态”，相对于主机的 TCP stack 实现来说，状态检查的过程相对简化。例如，不作 sequence number 的检查，不作包乱序的处理，只是统计一定时间内是否有 ACK 包在该“连接”(即四元组)上通过，从而“大致”确定该“连接”是否是“活动的”。