基于http的DDOS攻击的原理与实验

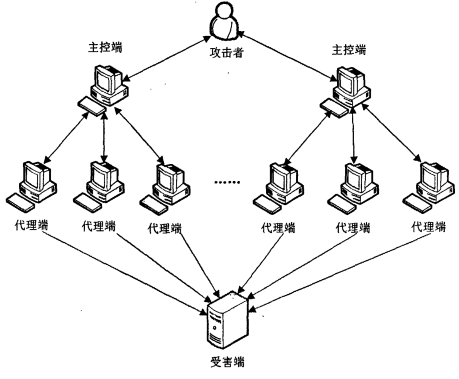
一、基于http的ddos攻击的原理与cc攻击器的攻击原理

首先对于基于http的ddos攻击的原理进行了解。基于http的ddos攻击也叫做基于http的flood攻击，在国内也被称为cc（Challenge Collapsar）攻击是针对osi协议的第七层协议发起的攻击。http-flood攻击一般分为两类：

1、请求洪范攻击：原理是通过大量合法的http请求占用目标网络的带宽或者消耗服务器的资源，是正常用户无法进行web访问；

2、高消耗请求攻击：原理是攻击者不断访问web服务器上高耗资源的网页。带来的后果就是服务器的资源（cpu、内存、磁盘）被消耗殆尽，从而达到拒绝服务的效果。

那么，http的flood是如何被引起的呢。攻击者通过代理端向目标主机发起http-flood。根据代理端的不同又可分为两种：一种是使用代理服务器作为代理端，攻击者只需要提前知道互联网上的代理服务器的ip地址和代理端口然后开多线程向这些代理端发送攻击数据包，代理服务器再把数据包发送给目标主机就可以造成flood；另一种是利用“僵尸网络”进行攻击，这时候的代理端就是被黑客控制的“僵尸主机”，黑客利用“僵尸主机”目标主机发起攻击。攻击时的网络拓扑图如下：



图中的主控端和代理端都是攻击者非法入侵并控制的一些主机，根据他们的层次都被植入了不同的非法攻击程序。每个主控端都控制着十几台代理端，有其控制的代理端的地址列表，它接收到攻击者发给它的命令后将命令转发给代理端，然后每个代理端开始向目标主机发起http请求造成flood。

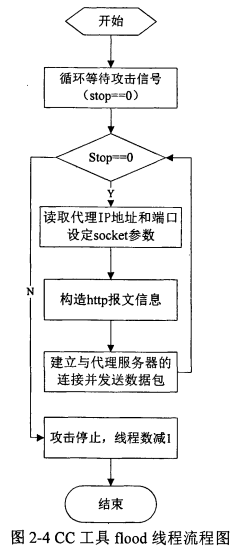
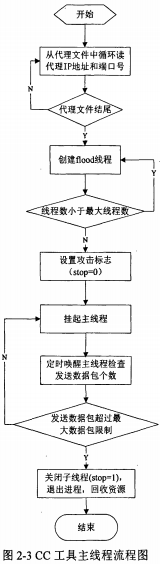
目前国内最出名的的http-flood攻击工具是一款被称为服务器杀手的CC(Challenge Collapsar)攻击器。经过资料查询对CC程序的运行原理有了一个初步了解：

图2-3是CC工具的主线程流程图，图2-4是CC工具的flood线程流程图。当CC工具进行攻击时会产生多个线程，而每个线程都会模拟一个用户对目标服务器进行攻击，方式为发出大量数据包。而在flood线程中CC工具采用了一个技巧——每次向代理服务器发送一个数据包后，立即断开与代理服务器的TCP连接(在程序中的做法就是关掉socket文件描述符)。这样做的效果是当攻击主机与代理服务器的连接断开后，代理服务器与攻击目标的连接依旧保留着，而再次连接的时候，代理服务器会与攻击目标重新建立一个连接，这样代理服务器与目标机的连接数会呈指数级增长，对目标机的资源消耗更大。