什么是 DDoS攻击?

分布式拒绝服务攻击 (DDoS)

可以使很多的计算机在同一时间遭受到攻击，使攻击的目标无法正常使用，分布式拒绝服务攻击已经出现了很多次，导致很多的大型网站都出现了无法进行操作的情况，这样不仅仅会影响用户的正常使用，同时造成的经济损失也是非常巨大的。

分布式拒绝服务攻击方式在进行攻击的时候，可以对源 IP 地址进行伪造，这样就使得这种攻击在发生的时候隐蔽性是非常好的，同时要对攻击进行检测也是非常困难的，因此这种攻击方式也成为了非常难以防范的攻击。

一个完整的 DDoS 攻击体系由攻击者、主控端、代理端和攻击目标四部分组成。主控端和代理端分别用于控制和实际发起攻击，其中主控端只发布命令而不参与实际的攻击，代理端发出 DDoS 的实际攻击包。对于主控端和代理端的计算机，攻击者有控制权或者部分控制权．它在攻击过程中会利用各种手段隐藏自己不被别人发现。真正的攻击者一旦将攻击的命令传送到主控端，攻击者就可以关闭或离开网络．而由主控端将命令发布到各个代理主机上。这样攻击者可以逃避追踪。每一个攻击代理主机都会向目标主机发送大量的服务请求数据包，这些数据包经过伪装，无法识别它的来源，而且这些数据包所请求的服务往往要消耗大量的系统资源，造成目标主机无法为用户提供正常服务。甚至导致系统崩溃。

DDoS攻击的分类

针对网络层的攻击 :

攻击源 (傀儡机)

向受害者系统发送大量的数据流，导致被攻击者的带宽满载，影响小的则降低受害者提供的服务，影响大的则使整个网络带宽持续饱和，以至于网络服务瘫痪，典型的攻击类型有 UDP洪水攻击， ICMP洪水攻击。

部分攻击也行也会对受害主机的网络协议栈产生巨大压力，比如 SYN Flood攻击与 ACK Flood攻击，是利用 TCP 三次握手的漏洞实现的。

简单理解 :

去饭店吃饭，攻击者叫了几千个人到你店里，但是不点菜不付款，导致新来的顾客无法正常点菜，达到拒绝服务的效果。

针对应用层的攻击 :

[illegible] CPU

[illegible] CC

[illegible]

[illegible]: [illegible]

Revision #3

Created 21 October 2024 07:50:30 by Admin

Updated 21 October 2024 08:49:46 by Admin