高手教你如何针对DDos部署防御措施 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/237/2021_2022__E9_AB_98_E6_89_8B_E6_95_99_E4_c101_237170.htm DDoS（Distributed Denial of Service，分布式拒绝服务）攻击的主要手段是通过大于管道处理能力的流量淹没管道或通过超过处理能力的任务使系统瘫痪，所以理论上只要攻击者能够获得比目标更强大的“ 动力 ”，目标是注定会被攻陷的。 对于DDoS攻击来说并没有100%有效的防御手段。但是由于攻击者必须付出比防御者大得多的资源和努力才能拥有这样的“ 动力 ”，所以只要我们更好的了解DDoS攻击，积极部署防御措施，还是能够在很大程度上缓解和抵御这类安全威胁的。 增强防御力 对抗DDoS攻击一个很重要的要素就是增强自身的防御能力。使用更大的带宽及提升相关设备的性能是面对 DDoS攻击最直接的处理方法。虽然这必定需要耗用一定的资源，但是对于那些将生存寄托于这些在线系统的企业来说，进行这种投入是具备足够理由的。只是在执行这类“ 硬性增幅 ”的时候，我们需要把握适度的原则。 因为我们的资源是有限的，如果增加100%的投入仅能在相关性能及DDoS防御力上获得10%的提升，明显是一种得不偿失的处理方式，毕竟这并不是我们仅有的选择。而且攻击者的资源同样是有限的，在我们增加防御强度的同时，就意味着攻击者必须集合比原来多得多的攻击傀儡机来实施攻击，并且会提高攻击者暴露的风险。不过应该记住的是，真正有效的DDoS防御并不是陷入与攻击者“ 角力 ”的恶性循环当中，而是应该综合各种方法，为攻击者设置足够的障碍。 目标系统处理 攻击者的最终目标可能是

一台主机，也可能是一台网络设备。除了对其目标的硬件能力进行增强之外，我们同样应该充分发挥系统自身的潜能，通过对目标系统的针对性处理，可以有效地放大现有资源的能量。最基本的任务是做好更新补丁的工作。特别是一些操作系统的通讯协议堆栈存在着问题，很容易成为拒绝服务攻击的利用对象。因为利用漏洞实施拒绝服务攻击相对于纯粹的设施能力比拼要容易的多。如果不能保证消除明显可被拒绝服务攻击利用的漏洞，其它的防御工作将只能成为摆设。好在现在各类系统的补丁更新速度还是比较令人满意的，只要根据自身环境的情况注意对相关系统的补丁发布情况进行跟踪就可以了。一些经常被使用的方法还包括限制连接队列的长度以及减少处理延时等。前者可以缓解系统资源的耗尽，虽然不能完全避免“拒绝服务”的发生，但是至少在一定程度上降低了系统崩溃的可能性。而后者能够加强系统的处理能力，通过减少延时，我们可以以更快的速度抛弃队列里等待的连接，而不是任其堆满队列；不过这种方法也不是在所有情况下都有效，因为很多DDoS的攻击机制并不是建立在类似SYN Flood这样以畸形连接淹没队列的方式之上。 100Test下载频道开通，各类考试题目直接下载。详细请访问www.100test.com