

网吧被攻击的根源以及解决之道 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/289/2021\\_2022\\_\\_E7\\_BD\\_91\\_E5\\_90\\_A7\\_E8\\_A2\\_AB\\_E6\\_c101\\_289646.htm](https://www.100test.com/kao_ti2020/289/2021_2022__E7_BD_91_E5_90_A7_E8_A2_AB_E6_c101_289646.htm) 最近各地网吧经常发生掉线的现象，经技术人员发现有人恶意攻击网吧，发送大量UDP包堵塞网吧的网络，包小量大，每秒几万条，高时能有150M的流量，很多路由器是直接接在光纤收发器上的，攻击一来根本吃不消，通过专业软件抓包分析，发现都是随机生成的虚假IP，根本查不到来源，如何网吧业主通过电信换IP的技术手段，就会发现第二天还是被攻击。发生这种现象的可能是网吧业主之间的非正常竞争，而发生的互相恶意攻击，这也在全国各地发生多起类似现象。也可能是一些黑客为了表现自己，而产生的个人“英雄主义”行为。不管怎样都对网吧业主的正常业务都带来了非常负面的影响。网吧被攻击的根源在哪里？探究根源，网吧并不是没有技术对黑客的入侵进行防范，而是网吧的技术人员对网吧的网络安全缺乏足够的重视，最终网吧成为一些黑客爱好者的练习黑客技术的演练场。网吧也是一个网络应用非常复杂的经营场所，而且网吧对网络的依赖性比较强，毕竟网吧现有的业务都是依靠网络作为支撑的。网吧是互联网中的一个节点，每台计算机都连接着互联网，这意味着每台计算机都有可能被黑客攻击。网吧是一个经营场所，黑客一般是通过打乱网吧的正常运营秩序来敲诈的，如果网吧经营者想着依靠公安部门来平息黑客的敲诈，这样的想法细细想来是非常荒诞的。公安部门可以帮助网吧将黑客抓获，可是公安部门也需要一定的时间来查找黑客，难道网吧就什么也不做，一直等待公安

部门抓获黑客吗？而且现代黑客攻击的技术手段已经非常先进，找到黑客是一件非常不容易的事情，要多个部门的紧密配合。网吧经营者必须清楚一点，黑客的攻击行为，已经危及到网吧的正常运营，网吧也要积极查找自身的安全漏洞，找不出自身的安全漏洞，网吧的正常经营随时有可能遭遇黑客的破坏。如果网吧一直对自身存在的安全漏洞视而不见，公安部门抓获了黑客又能如何，谁能保证其他黑客不再攻击？其实，要想真正杜绝黑客的攻击，必须加强网吧的网络安全防范。加强网吧安全是解决的根本 要想网吧远离黑客攻击，加强网吧的安全建设才是最有效的解决方法。从技术角度来讲，网吧的安全建设涉及到网吧系统和网络两个方面。在操作系统的安全设置方面，主要有以下几个方面：一是要设置复杂的用户登录密码，这样可以有效防止黑客的攻击；二是要关闭系统中有安全隐患的服务，对于工作在局域网的网吧客户端，系统默认的服务是造成网吧系统不安全的隐患。以Windows XP Professional SP2操作系统为例，Server文件共享服务、远程修改注册表、计划任务等服务，都是具有高安全风险的服务，而网吧的日常应用中又不需要，因此，这些服务是可以禁用的。要想禁用这些服务，可以在“开始”菜单的“运行”中输入“Services.msc”，进入服务设置界面，将有安全隐患的服务禁用即可；三是要及时更新系统的安全补丁，因为一些黑客通常是利用操作系统的漏洞进行攻击的。除操作系统的安全设置之外，代理服务器或路由器的安全设置也不容忽视。目前，大多数网吧已经淘汰了代理服务器改用路由器，殊不知路由器如果设置不当，也会被黑客攻击。网吧的技术人员一定要把路由器超级用户的默认口令修改掉

，重新设置一个较为复杂的安全口令。同时，为了防止其他人DDoS攻击，可以禁止用户Ping路由器的WAN口。在日常经营中，技术人员一定要定期检查路由器的网络配置，以及路由器的日志文件，检查是否有可疑人员登录路由器。一些网吧的路由器中已经内置防火墙，默认状态下，路由器的防火墙功能是关闭的，技术人员可以根据网吧的实际需要选择防火墙的开关，毕竟防火墙一旦启用，网吧的网络速度就要受到一定的影响。针对最新的黑客DDOS拒绝性服务攻击，一般网吧的防火墙和路由器已经不能胜任这种工作了，因为这种防火墙和路由器都是针对正常网路流量来防止网络的非正常的访问的，对于这种大流量的网络攻击，防火墙和路由器或者代理服务器会首先瘫痪，反而成为网吧网络的瓶颈，因此只有配置针对抗DDOS攻击的专用设备才能更好的保护网吧的网络安全，减少网吧的断线率，提高网吧的使用带宽和网络使用效率。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](http://www.100test.com)