通过修改注册表来增强系统抵抗DDOS攻击 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/274/2021_2022__E9_80_9A_E8_BF_87_E4_BF_AE_E6_c67_274987.htm 防范DDOS攻击并不一定非要用防火墙。一部份DDOS我们可以通过DOS命令netstat -an more或者网络综合分析软件：sniff等查到相关攻击手法、如攻击某个主要端口、或者对方主要来自哪个端口、对方IP等。这样我们可以利用w2k自带的远程访问与路由或者IP策略等本身自带的工具解决掉这些攻击。做为无法利用这些查到相关数据的我们也可以尝试一下通过对服务器进行安全设置来防范DDOS攻击。如果通过对服务器设置不能有效解决，那么就可以考虑购买抗DDOS防火墙了。 其实从操作系统角度来说，本身就藏有很多的功能，只是很多是需要我们慢慢的去挖掘的。这里我给大家简单介绍一下如何在Win2000环境下通过修改注册表，增强系统的抗DoS能力。请注意，以下的安全设置均通过注册表进行修改，该设置的性能取决于服务器的配置，尤其是CPU的处理能力。如按照如下进行安全设置，采用双路至强2.4G的服务器配置，经过测试，可承受大约1万个包的攻击量。 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters] 关闭无效网关的检查。当服务器设置了多个网关，这样在网络不通畅的时候系统会尝试连接 第二个网关，通过关闭它可以优化网络。 "EnableDeadGWDetect"=dword:00000000 禁止响应ICMP重定向报文。此类报文有可能用以攻击，所以系统应该拒绝接受ICMP重定向报文。 "EnableICMPRedirects"=dword:00000000

不允许释放NETBIOS名。当攻击者发出查询服务器NETBIOS名的请求时，可以使服务器禁止响应。 注意系统必须安装SP2以上 "NonameReleaseOnDemand"=dword:00000001 发送验证保持活动数据包。该选项决定TCP间隔多少时间来确定当前连接还处于连接状态，不设该值，则系统每隔2小时对TCP是否有闲置连接进行检查，这里设置时间为5分钟。 "KeepAliveTime"=dword:000493e0 禁止进行最大包长度路径检测。该项值为1时，将自动检测出可以传输的数据包的大小，可以用来提高传输效率，如出现故障或安全起见，设项值为0，表示使用固定MTU值576bytes。 "EnablePMTUDiscovery"=dword:00000000 启动syn攻击保护。缺省项值为0，表示不开启攻击保护，项值为1和2表示启动syn攻击保护，设成2之后 安全级别更高，对何种状况下认为是攻击，则需要根据下面的TcpMaxHalfOpen和cpMaxHalfOpenRetried值设定的条件来触发启动了。这里需要注意的是，NT4.0必须设为1，设为2后在某种特殊数据包下会导致系统重启。 "SynAttackProtect"=dword:00000002 同时允许打开的半连接数量。所谓半连接，表示未完整建立的TCP会话，用netstat命令可以看到呈SYN_RCVD状态的就是。这里使用微软建议值，服务器设为100，高级服务器设为500。建议可以设稍微小一点。 "TcpMaxHalfOpen"=dword:00000064 判断是否存在攻击的触发点。这里使用微软建议值，服务器为80，高级服务器为400。 "TcpMaxHalfOpenRetried"=dword:00000050 设置等待SYN-ACK时间。缺省项值为3，缺省这一过程消耗时间45秒。项值为2，消耗时间为21秒。 项值为1，消耗时间为9秒。最低可以设

为0，表示不等待，消耗时间为3秒。这个值可以根据遭受攻击规模修改。 微软站点安全推荐为2。 设置TCP重传单个数据段的次数。缺省项值为5，缺省这一过程消耗时间240秒。微软站点安全推荐为3。
"TcpMaxDataRetransmissions"=dword:00000003 设置syn攻击保护的临界点。当可用的backlog变为0时，此参数用于控制syn攻击保护的开启，微软站点安全推荐为5。
"TCPMaxPortsExhausted"=dword:00000005 禁止IP源路由。缺省项值为1，表示不转发源路由包，项值设为0，表示全部转发，设置为2，表示丢弃所有接受的 源路由包，微软站点安全推荐为2。 "DisableIPSourceRouting"=dword:0000002 限制处于TIME_WAIT状态的最长时间。缺省为240秒，最低为30秒，最高为300秒。建议设为30秒。
"TcpTimedWaitDelay"=dword:0000001e
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters] 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