ICMP隧道

坏虾 / 2018-06-07 09:42:06 / 浏览数 6954 安全工具 工具 顶(0) 踩(0)

很老的东西了，感觉还是有点用处，大家看看就好。用的时候别忘记了。
http://www.cs.uit.no/~daniels/PingTunnel/PingTunnel-0.72.tar.gz
这个是源码。

下面附件有编译好的windows版本。 其实就是用的cygwin而已。

下面描述场景。

内网有一台win，连不上外网，但是能ping通。
现在通过ICMP进行穿透。
在外网的一台linux或者win的机器上，运行ptunnel 啥参数也不用加，OK，这个server段就起来了。

在win上安装winpcap。运行ptunnel -h
看一下自己的网卡信息。

然后开始穿透。

ptunnel.exe -p VPSIP -lp 888 -da 127.0.0.1 -dp 22 -c "\Device\NPF{1EB81540-24xxxxx2120F780}"

结果是，内网机器直接访问本机的888端口，就是访问VPS的22端口啦。

参考场景：
VPS上开启SOCKS5代理服务，OK，内网可以直接通过代理访问外网。

icmp.zip (0.933 MB) 下载附件
点击收藏 | 1 关注 | 1
上一篇：【译】Metasploit：Wik... 下一篇：【译】Metasploit：如何在...
1. 0 条回复
   - 动动手指，沙发就是你的了！