0trace.sh

0trace.sh主要用于路由追踪，需要与对方服务器建立一个连接，之后0trace.sh发送数据包进行链路追踪。

——by lcamtuf@coredump.cx

一，帮助手册

0trace 网卡 目标 端口

Usage: /usr/bin/0trace.sh iface target_ip [target_port]

二，命令实例与原理

首先需要有一个SADDR（地址），还要有一个DADDR（设备地址）而之后需要Sport（来源端口）和（Dport）之后对数据包进行Seq（发送）然后服务端发返回给主机Ack（确认包）之后返回结果。

通过向目标发送不同的ip ttl和“Internet控制消息协议（ICMP）”所回应的数据包，然后Tracert盘打un程序确定到目标所采取的路由，所以要求路径撒谎那个的每台路由器在转发数据包之前至少将数据包上的TTL递减1，数据包上的TTL为0时，路由器将ICMP以超时的消息发挥源系统

模拟过程

路由器为192.168.0.1和192.168.0.2，目标主机为192.168.0.3

> Tracing route to 172.16.0.99 over a maximum of 30 hops
>
> 1 2s 3s 2s 192.168.0.1
>
> 2 75 ms 83 ms 88 ms 192.168.0.2
>
> 3 73 ms 79 ms 93 ms 192.168.0.3

命令实例

0trace wlan0 sogo.com 443

追踪sogo.com的链路路由信息[^443为https协议端口]