一、介绍

1、原理

利用ICMP的请求和应答数据包，伪造Ping命令的数据包形式，实现绕过防火墙和入侵检测。

进行隐蔽传输时，肉鸡运行并接受外部供给端的ICMP_ECHO数据包，攻击端把需要执行的命令隐藏在ICMP_ECHO数据包中，肉鸡接收到该数据包，解出其中隐藏的命令，并在防火墙内部主机上执行，再把执行结果隐藏在ICMP_ECHOREPLY数据包中，发送给外部攻击端。

2、优势

由于ICMP报文可以携带数据，而且ICMP报文是由系统内核处理的，不占用任何端口，因此具有很高的隐蔽性。

二、流量特征

1、观察数量

检测同一来源的ICMP数据包的数量，一个正常的ping命令每秒最多发送两个数据包，而用ICMP隧道会在短时间内发送大量的ICMP数据包。由于ICMP协议无法保持连接，只能通过一问一答式心跳包不断Ping进行保持连接，受控端发送ping，控制端在reply返回包中夹带要执行的命令，受控端在requestb。