

# 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。

No.	Time	Source	Destination	Protocol	Length	Status Code	Info
137	2022-06-18 21:43:59.967419	192.168.174.158	192.168.174.157	ICMP	60		Echo (ping) reply id=0x0001, seq
141	2022-06-18 21:44:00.183774	192.168.174.157	192.168.174.158	ICMP	42		Echo (ping) request id=0x0001, seq
142	2022-06-18 21:44:00.185140	192.168.174.158	192.168.174.157	ICMP	60		Echo (ping) reply id=0x0001, seq
143	2022-06-18 21:44:00.386677	192.168.174.157	192.168.174.158	ICMP	42		Echo (ping) request id=0x0001, seq
144	2022-06-18 21:44:00.387474	192.168.174.158	192.168.174.157	ICMP	60		Echo (ping) reply id=0x0001, seq
146	2022-06-18 21:44:00.589935	192.168.174.157	192.168.174.158	ICMP	42		Echo (ping) request id=0x0001, seq
147	2022-06-18 21:44:00.590402	192.168.174.158	192.168.174.157	ICMP	60		Echo (ping) reply id=0x0001, seq
148	2022-06-18 21:44:00.792753	192.168.174.157	192.168.174.158	ICMP	106		Echo (ping) request id=0x0001, seq
149	2022-06-18 21:44:00.793316	192.168.174.158	192.168.174.157	ICMP	60		Echo (ping) reply id=0x0001, seq
150	2022-06-18 21:44:00.996342	192.168.174.157	192.168.174.158	ICMP	50		Echo (ping) request id=0x0001, seq
151	2022-06-18 21:44:00.997566	192.168.174.158	192.168.174.157	ICMP	60		Echo (ping) reply id=0x0001, seq

Wireshark · 分组 148 · VMware Network Adapter VMnet8 1秒10包

Frame 148: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF\_{C284BC5B-8DD8-4937-A0C9-09B5D84AB1E2}, id 0  
Ethernet II, Src: VMware\_a8:6e:27 (00:0c:29:a8:6e:27), Dst: VMware\_e3:6e:2e (00:0c:29:e3:6e:2e)  
Internet Protocol Version 4, Src: 192.168.174.157, Dst: 192.168.174.158  
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x8900 [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 87 (0x0057)

00 00 29 e3 6e 2e 00 0c 29 a8 6e 27 08 00 45 00 ..).n...).n'..E-  
10 00 5c 7a 1c 00 00 ff 01 62 f7 c0 a8 ae 9d c0 a8 \z.....b.....  
20 ae 9e 08 00 89 00 00 01 00 57 77 68 6f 61 6d 69 .....-whoami  
30 0a 64 65 73 6b 74 6f 70 2d 33 37 34 6c 68 70 36 desktop-3741hp6  
40 5c 63 68 65 6e 67 71 69 61 6e 67 0d 0a 0d 0a 43 ch.....C  
50 3a 5c 55 73 65 72 73 5c 63 68 65 6e 67 71 69 61 :Users\ ch  
60 6e 67 5c 44 65 73 6b 74 6f 70 ng\Desk op

whoami 命令与执行结果