BugKu CTF(杂项篇MISC)—ping

原创

网络安全研究所 于 2021-02-01 11:11:21 发布 2128 收藏 5
文章标签： css 微软 html 数据可视化 less

本文链接：https://blog.csdn.net/zjzqxzhj/article/details/113507243

CTF

BugKu CTF

(杂项篇MISC)

攻与防

ping

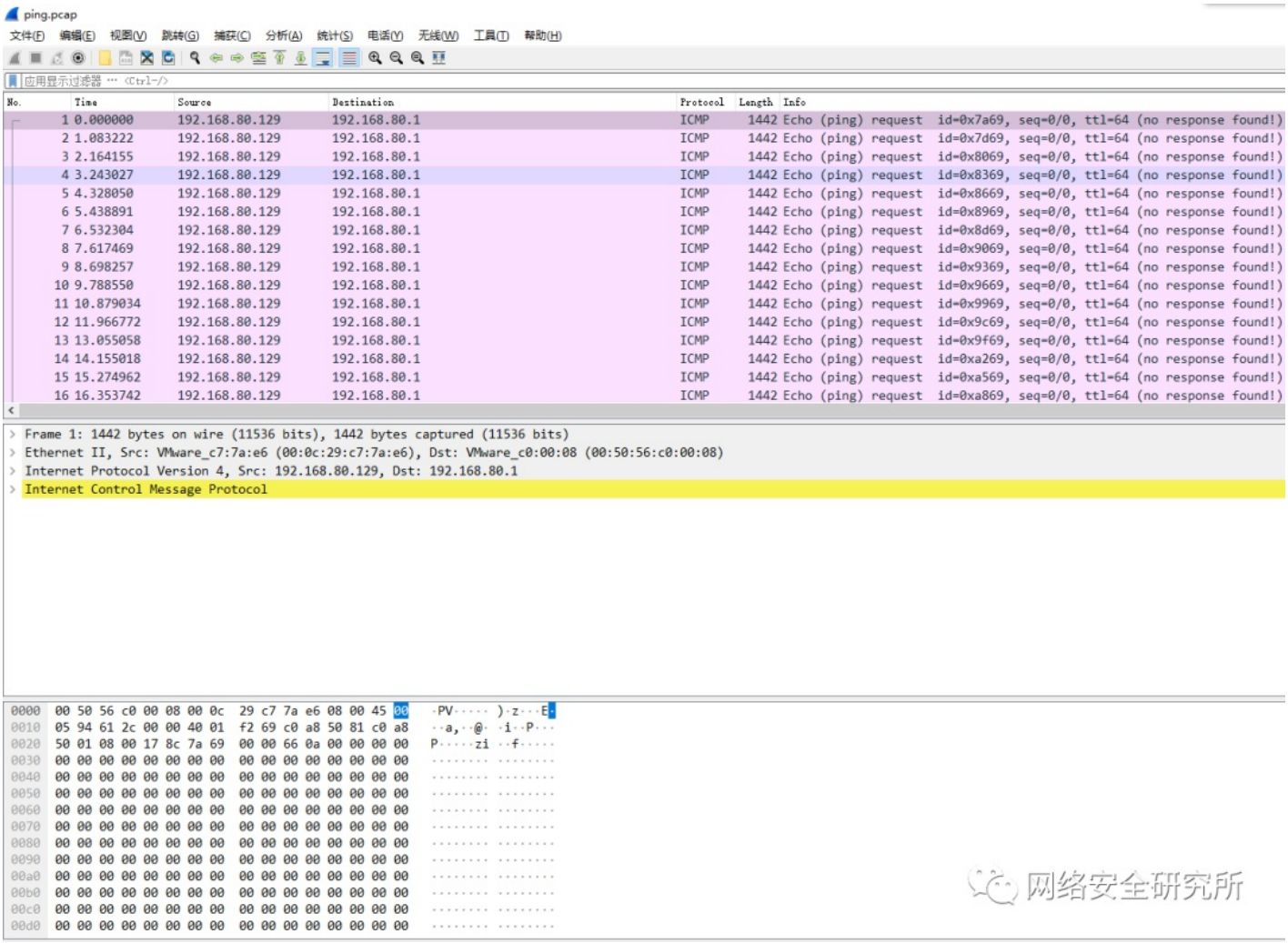
题目是1个压缩包，里面放了1个pcap文档。pcap文件是wireshark配置脚本文件。可以用Wireshark软件打开，wireshark是网络流量分析工具。

1.工具

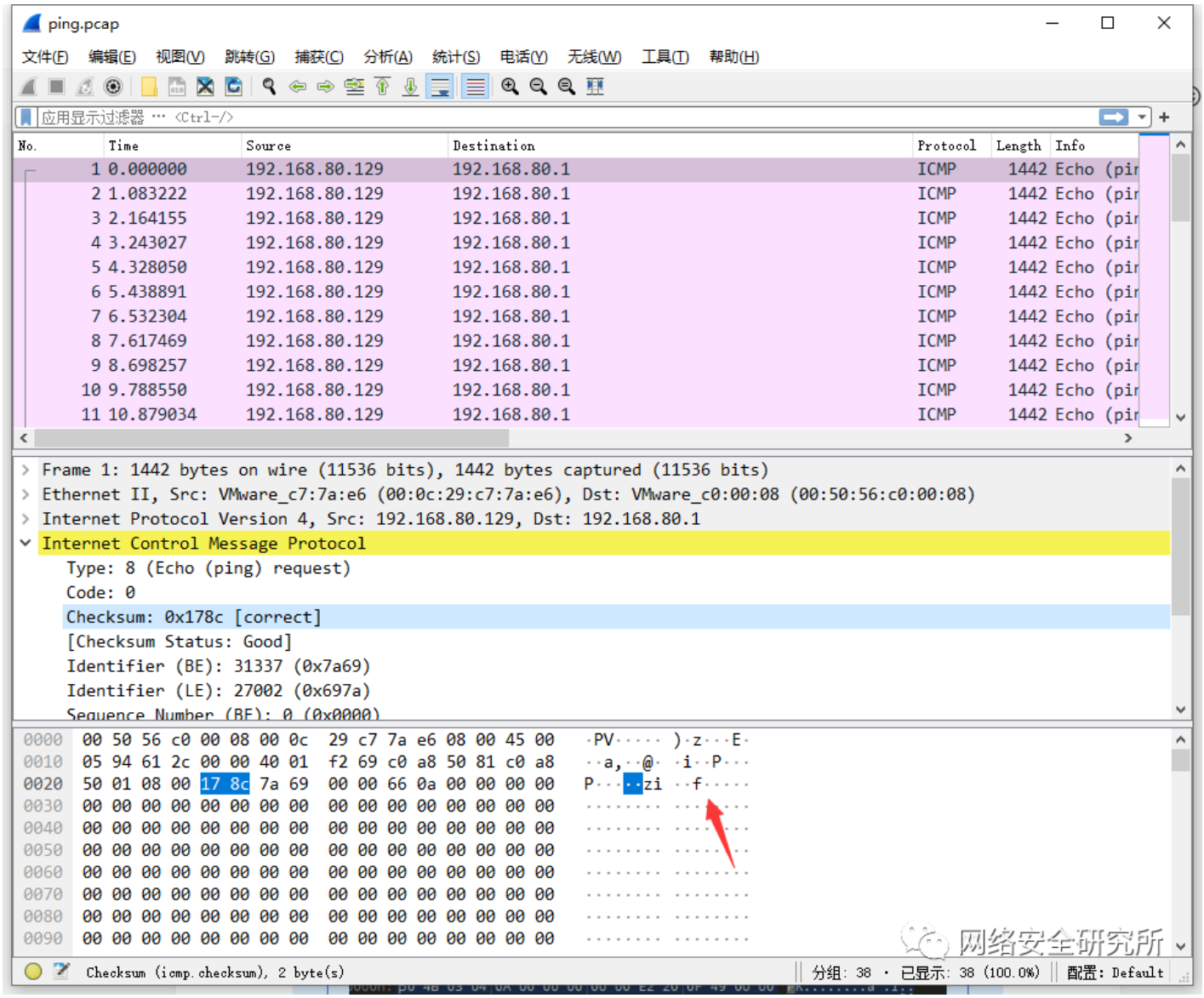
wireshar网络流量分析工具

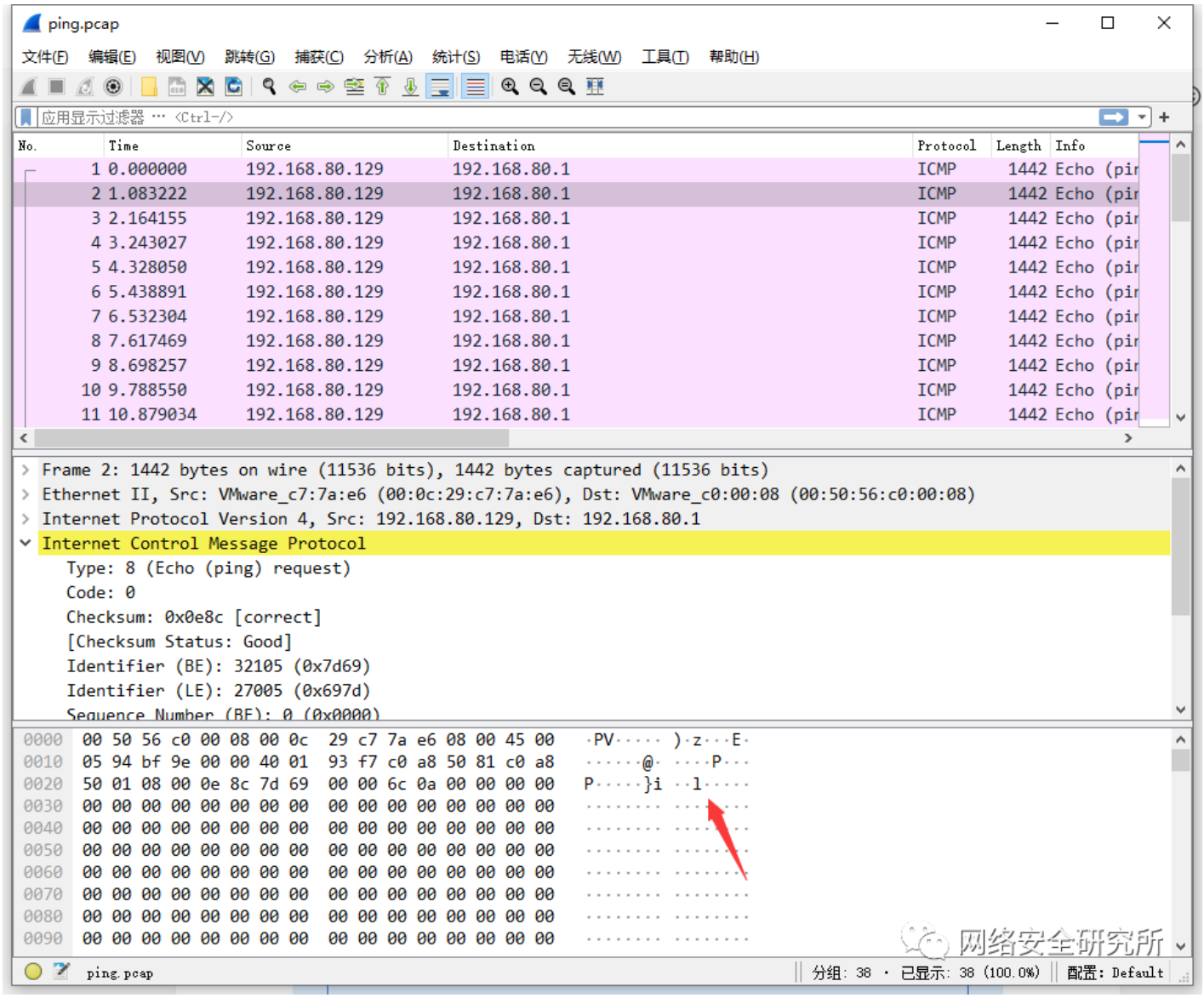
2.解题思路

1.对于pcap包，直接用wireshark软件打开，全都是ICMP协议，无法用TCP流追踪。



2.挨个协议包看看，发现每个包里有个字段不一样。


ping.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
2 1.083222 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
3 2.164155 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
4 3.243027 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
5 4.328050 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
6 5.438891 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
7 6.532304 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
8 7.617469 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
9 8.698257 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
10 9.788550 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
11 10.879034 192.168.80.129 192.168.80.1 ICMP 1442 Echo (pi
Frame 1: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits)
Ethernet II, Src: VMware_c7:7a:e6 (00:0c:29:c7:7a:e6), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.80.129, Dst: 192.168.80.1
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x178c [correct]
[Checksum Status: Good]
Identifier (BE): 31337 (0x7a69)
Identifier (LE): 27002 (0x697a)
Sequence Number (BE): 0 (0x0000)
0000 00 50 56 c0 00 08 00 0c 29 c7 7a e6 08 00 45 00
0010 05 94 61 2c 00 00 40 01 f2 69 c0 a8 50 81 c0 a8
0020 50 01 08 00 17 8c 7a 69 00 00 66 0a 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Checksum (icmp.checksum), 2 byte(s)
分组: 38 · 已显示: 38 (100.0%)
配置: Default
网络安全研究所



3.挨个包查看该位置，组合起来就是flag{***}，中间内容自己找一下。

3.总结

本题需要掌握wireshark网络流量分析工具，多观察每个包不同的地方。

Wireshark(前称Ethereal)是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。

wireshark的具体使用方法在另一篇文章会具体介绍。

END

扫码关注

网络安全研究所

更多精彩等着你


网络安全研究所