

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zjqxzhj/article/details/113507243>

版权

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。

The screenshot shows the Wireshark interface with a list of 16 ICMP Echo (ping) requests. The packet list pane shows the following details:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|--------------|----------|--------|---|
| 1 | 0.000000 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!) |
| 2 | 1.083222 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!) |
| 3 | 2.164155 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!) |
| 4 | 3.243027 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!) |
| 5 | 4.328050 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!) |
| 6 | 5.438891 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!) |
| 7 | 6.532304 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!) |
| 8 | 7.617469 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x9069, seq=0/0, ttl=64 (no response found!) |
| 9 | 8.698257 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x9369, seq=0/0, ttl=64 (no response found!) |
| 10 | 9.788550 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x9669, seq=0/0, ttl=64 (no response found!) |
| 11 | 10.879034 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x9969, seq=0/0, ttl=64 (no response found!) |
| 12 | 11.966772 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x9c69, seq=0/0, ttl=64 (no response found!) |
| 13 | 13.055058 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0x9f69, seq=0/0, ttl=64 (no response found!) |
| 14 | 14.155018 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0xa269, seq=0/0, ttl=64 (no response found!) |
| 15 | 15.274962 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0xa569, seq=0/0, ttl=64 (no response found!) |
| 16 | 16.353742 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request id=0xa869, seq=0/0, ttl=64 (no response found!) |

The packet details pane for the selected packet shows:

- 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

The hex dump at the bottom shows the raw data of the packet, starting with:

```

0000 00 50 56 c0 00 08 00 0c 29 c7 7a e6 08 00 45 00  ·PV·····)·z···E·
0010 05 94 61 2c 00 00 40 01 f2 69 c0 a8 50 81 c0 a8  ··a··@··i··P···
0020 50 01 08 00 17 8c 7a 69 00 00 66 0a 00 00 00 00  P····zi··f·····
0030 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  ······
0050 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  ······
0070 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  ······
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ······
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ······
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ······
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ······
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ······

```

2.挨个协议包看看，发现每个包里有字段不一样。

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 (ping) request |
| 2 | 1.083222 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) reply |
| 3 | 2.164155 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 4 | 3.243027 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) reply |
| 5 | 4.328050 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 6 | 5.438891 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) reply |
| 7 | 6.532304 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 8 | 7.617469 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) reply |
| 9 | 8.698257 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 10 | 9.788550 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) reply |
| 11 | 10.879034 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |

> Frame 1: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits) on interface 0

> 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 | ·PV·...·)·z·...·E· |
| 0010 | 05 94 61 2c 00 00 40 01 | f2 69 c0 a8 50 81 c0 a8 | ··a··@· ·i··P·... |
| 0020 | 50 01 08 00 17 8c 7a 69 | 00 00 66 0a 00 00 00 00 | P·...·zi· ·f·...· |
| 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

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 (ping) request |
| 2 | 1.083222 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 3 | 2.164155 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 4 | 3.243027 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 5 | 4.328050 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 6 | 5.438891 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 7 | 6.532304 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 8 | 7.617469 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 9 | 8.698257 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 10 | 9.788550 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |
| 11 | 10.879034 | 192.168.80.129 | 192.168.80.1 | ICMP | 1442 | Echo (ping) request |

> Frame 2: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits) on interface 0

> 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: 0x0e8c [correct]
- [Checksum Status: Good]
- Identifier (BE): 32105 (0x7d69)
- Identifier (LE): 27005 (0x697d)
- Sequence Number (BE): 0 (0x0000)

```

0000  00 50 56 c0 00 08 00 0c 29 c7 7a e6 08 00 45 00  .PV.....)z...E.
0010  05 94 bf 9e 00 00 40 01 93 f7 c0 a8 50 81 c0 a8  .....@...P...
0020  50 01 08 00 0e 8c 7d 69 00 00 6c 0a 00 00 00 00  P.....}i...l...
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  .....

```

ping.pcap | 分组: 38 · 已显示: 38 (100.0%) | 配置: Default

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