

xctf攻防世界 CRYPTO高手进阶区 工控安全取证

原创

[18947943](#) 于 2022-02-24 18:58:11 发布 133 收藏

分类专栏: [攻防世界crypto之路](#) 文章标签: [安全](#) [web安全](#) [网络](#)

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/18947943/article/details/123118324>

版权



[攻防世界crypto之路](#) 专栏收录该内容

26 篇文章 0 订阅

订阅专栏

0x01. 进入环境，下载附件

题目给的是一个日志文件，放入kali中查看文件类型：

```
file capture.log
```

可以看到，该文件是一个pcapng流量包文件，如图：



0x02. 问题分析

将文件的后缀修改为pcapng，用wireshark打开，发现是一堆tcp链接和少量的ICMP链接。题目提示是对端口进行多次扫描，扫描端口一般是利用ICMP回显请求，那么我们对icmp进行排序，如图：

capture.pcapng

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(I) 帮助(H)

应用显示过滤器 ... <Ctrl- />

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.9	192.168.0.99	ICMP	60	Echo (ping) request id=0x7ae9, seq=0/0, ttl=40 (reply in 2)
2	0.000078	192.168.0.99	192.168.0.9	ICMP	42	Echo (ping) reply id=0x7ae9, seq=0/0, ttl=255 (request in 1)
148007	1274.602300	192.168.0.9	192.168.0.99	ICMP	60	Echo (ping) request id=0x1e09, seq=0/0, ttl=47 (reply in 148008)
148008	1274.602365	192.168.0.99	192.168.0.9	ICMP	42	Echo (ping) reply id=0x1e09, seq=0/0, ttl=255 (request in 148007)
150655	1308.472790	192.168.0.99	192.168.0.9	ICMP	370	Destination unreachable (Port unreachable)
150753	1407.256096	192.168.0.9	192.168.0.99	ICMP	60	Echo (ping) request id=0xa373, seq=0/0, ttl=53 (reply in 150754)
150754	1407.256145	192.168.0.99	192.168.0.9	ICMP	42	Echo (ping) reply id=0xa373, seq=0/0, ttl=255 (request in 150753)
153165	1441.428990	192.168.0.99	192.168.0.9	ICMP	370	Destination unreachable (Port unreachable)
155847	1504.127684	192.168.0.99	192.168.0.9	ICMP	370	Destination unreachable (Port unreachable)
155987	1602.084879	192.168.0.1	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
155988	1602.084912	192.168.0.254	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
155989	1602.084941	192.168.0.199	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
155990	1602.084976	192.168.0.199	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
3	0.000044	192.168.0.9	192.168.0.99	TCP	60	52218 → 80 [ACK] Seq=1 Ack=1 Win=2048 Len=0
4	0.000119	192.168.0.99	192.168.0.9	TCP	54	80 → 52218 [RST] Seq=1 Win=0 Len=0
5	10.346091	192.168.0.9	192.168.0.99	TCP	60	52198 → 52156 [SYN] Seq=0 Win=2048 Len=0

> Frame 148007: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 > Ethernet II, Src: XircorRe_c5:7c:38 (00:10:a4:c5:7c:38), Dst: 3com_a8:61:24 (00:60:08:a8:61:24)
 > Internet Protocol Version 4, Src: 192.168.0.9, Dst: 192.168.0.99
 > Internet Control Message Protocol

CSDN @I8947943

我们可以看到，题目让找到第四次的扫描编号，如图，对流量进行分析

capture.pcapng

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(I) 帮助(H)

应用显示过滤器 ... <Ctrl- />

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.9	192.168.0.99	ICMP	60	Echo (ping) request id=0x7ae9, seq=0/0, ttl=40 (reply in 2)
2	0.000078	192.168.0.99	192.168.0.9	ICMP	42	Echo (ping) reply id=0x7ae9, seq=0/0, ttl=255 (request in 1)
148007	1274.602300	192.168.0.9	192.168.0.99	ICMP	60	Echo (ping) request id=0x1e09, seq=0/0, ttl=47 (reply in 148008)
148008	1274.602365	192.168.0.99	192.168.0.9	ICMP	42	Echo (ping) reply id=0x1e09, seq=0/0, ttl=255 (request in 148007)
150655	1308.472790	192.168.0.99	192.168.0.9	ICMP	370	Destination unreachable (Port unreachable)
150753	1407.256096	192.168.0.9	192.168.0.99	ICMP	60	Echo (ping) request id=0xa373, seq=0/0, ttl=53 (reply in 150754)
150754	1407.256145	192.168.0.99	192.168.0.9	ICMP	42	Echo (ping) reply id=0xa373, seq=0/0, ttl=255 (request in 150753)
153165	1441.428990	192.168.0.99	192.168.0.9	ICMP	370	Destination unreachable (Port unreachable)
155847	1504.127684	192.168.0.99	192.168.0.9	ICMP	370	Destination unreachable (Port unreachable)
155987	1602.084879	192.168.0.1	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
155988	1602.084912	192.168.0.254	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
155989	1602.084941	192.168.0.199	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
155990	1602.084976	192.168.0.199	192.168.0.99	ICMP	60	Echo (ping) request id=0xc77b, seq=0/0, ttl=52 (no response found!)
3	0.000044	192.168.0.9	192.168.0.99	TCP	60	52218 → 80 [ACK] Seq=1 Ack=1 Win=2048 Len=0
4	0.000119	192.168.0.99	192.168.0.9	TCP	54	80 → 52218 [RST] Seq=1 Win=0 Len=0
5	10.346091	192.168.0.9	192.168.0.99	TCP	60	52198 → 52156 [SYN] Seq=0 Win=2048 Len=0

> Frame 155987: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 > Ethernet II, Src: XircorRe_c5:7c:38 (00:10:a4:c5:7c:38), Dst: 3com_a8:61:24 (00:60:08:a8:61:24)
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.99
 > Internet Control Message Protocol

CSDN @I8947943

ICMP请求第一组编号有发出也有回显正常的信息，我们认为该次扫描为一次正常的扫描；第二组和第三组同理！！

第四组为什么是155989？第四次我们可以推测在155987到155990之间。

但在一个c类地址网段中，一般地址为1-254可用，第四个字节全0和全1都是不可用，一般首位地址和末尾地址用于特殊设备使用，因此推测第四次扫描编号为155989。

最终答案为： `flag{155989}`