攻防世界 Crypto高手进阶区 4分题 工控安全取证

原创

思源湖的鱼 于 2020-12-21 14:31:25 发布 495 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111474153

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

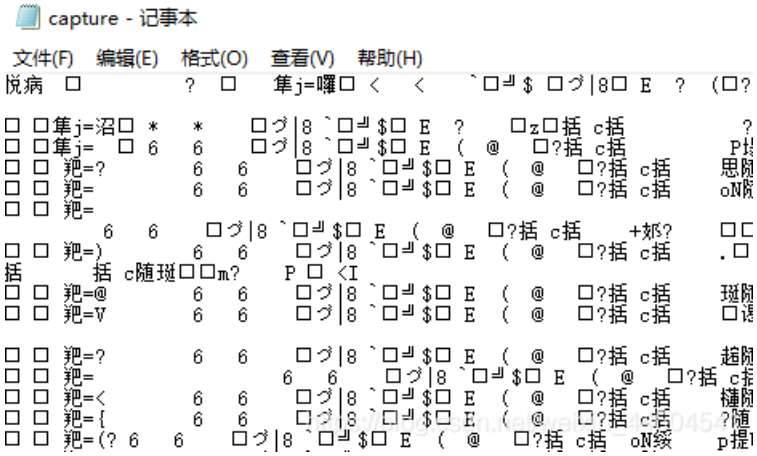
本篇是工控安全取证的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一个log文本

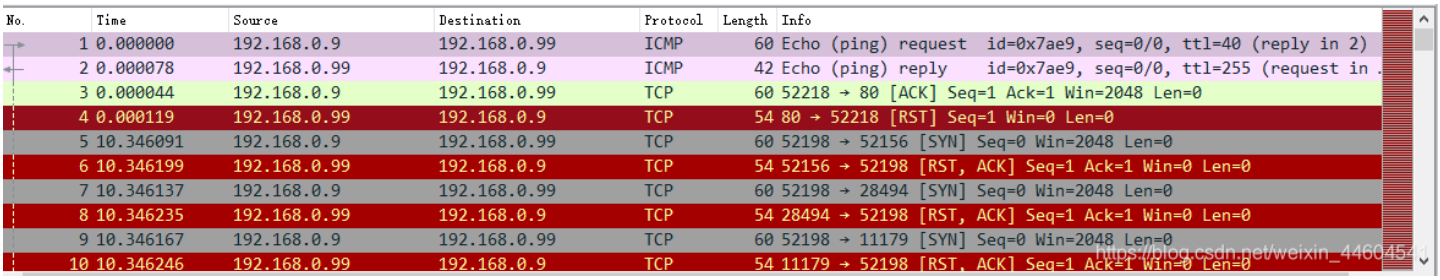


根据提示

有黑客入侵工控设备后在内网发起了大量扫描，而且扫描次数不止一次。 请分析日志，指出对方第4次发起扫描时的数据包的编号，

应该是个流量
就改为pcapng
然后扔进wireshark

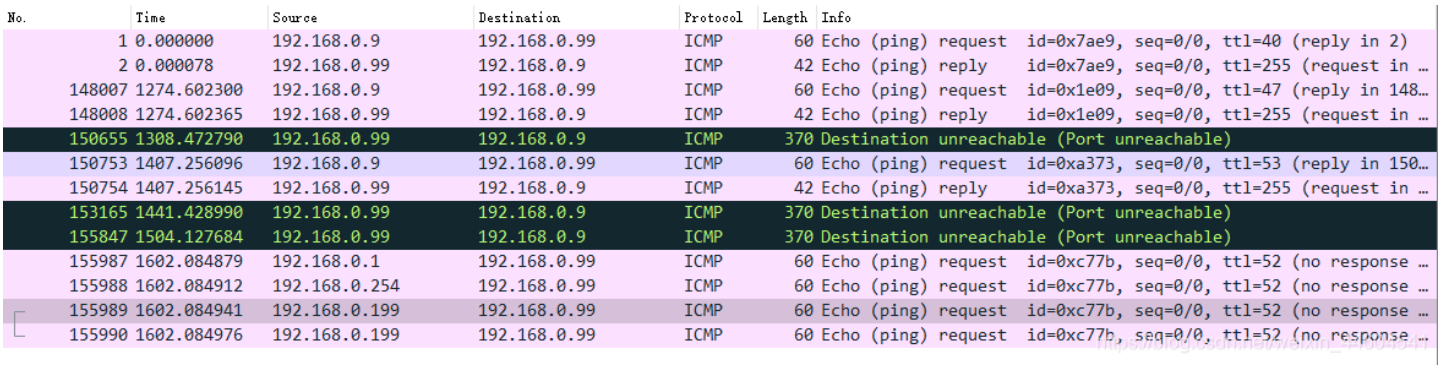
得到一大堆tcp



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 …
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
6	10.346199	192.168.0.99	192.168.0.9	TCP	54	52156 → 52198 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	10.346137	192.168.0.9	192.168.0.99	TCP	60	52198 → 28494 [SYN] Seq=0 Win=2048 Len=0
8	10.346235	192.168.0.99	192.168.0.9	TCP	54	28494 → 52198 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	10.346167	192.168.0.9	192.168.0.99	TCP	60	52198 → 11179 [SYN] Seq=0 Win=2048 Len=0
10	10.346246	192.168.0.99	192.168.0.9	TCP	54	11179 → 52198 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

注意到少量ICMP
发起扫描多半先一个ICMP
然后一堆TCP

所以看看ICMP



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 …
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 148…
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 …
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 150…
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 …
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 …
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 …
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 …
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 …

他要求第四次
那应该是在155987到155990

最终发现IP为192.168.0.199的ICMP的Ping请求对应的数据包编号155989为Flag

结语

有点不太明白为什么认为是155989