网络空间安全技术大赛 misc3 writep

原创

L1am3s 于 2018-05-14 09:10:08 发布 963 收藏
分类专栏： CTF 文章标签： misc 流量分析 CTF

misc3 test.pcapng

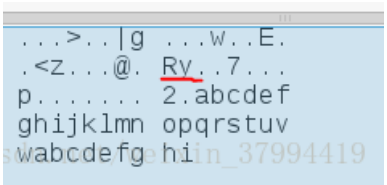
ps:(用于自己记录)

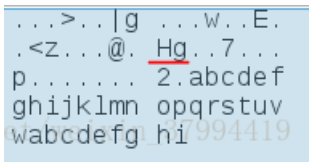
打开发现,是一个流量包,用wireshark打开,

协议	按分组百分比	分组	按字节百分比	字节	比特/秒	End Packets	End Bytes	End Bits/s
▾ Frame	100.0	131	100.0	17286	1970	0	0	0
▾ Ethernet	100.0	131	10.6	1834	209	0	0	0
▾ Internet Protocol Version 4	100.0	131	15.2	2620	298	0	0	0
▾ Transmission Control Protocol	81.7	107	68.1	11770	1341	84	3671	418
Secure Sockets Layer	9.2	12	36.6	6331	721	11	5993	683
▾ Hypertext Transfer Protocol	9.2	12	23.4	4046	461	3	1884	214
Media Type	0.8	1	0.9	162	18	1	162	18
Line-based text data	3.1	4	2.3	398	45	4	398	45
HTML Form URL Encoded	3.1	4	1.1	190	21	4	190	21
Internet Control Message Protocol	18.3	24	5.6	960	109	24	960	109

发现存在icmp,所以先查看一下icmp包.

观察了一下,并没有存在什么特别的信息.然后再看看数据,发现request包那里有数据会改变,下面上两张图





...(后面的不列出来了)

然后尝试一下把这个当做flag值提交.

= =居然就是这个O__O"…