

# Modbus协议

---

## 题目描述

---

黑客通过外网进入一家工厂的控制网络，之后对工控网络中的操作员站系统进行了攻击，最终通过工控协议破坏了正常的业务。我们得到了操作员站在攻击前后的网络流量数据包，我们需要分析流量中的蛛丝马迹，找到FLAG,flag形式为 flag{}

## 题目来源

---

纵横网络靶场社区 <https://game.fengtaisec.com/>

## 主要知识点

---

## 题目分值

---

10

## 部署方式

---

## 解题思路

---

筛选modbus包，并排序包大小，最大的那个就是flag

modbus

No.	Time	Source	Destination	Protocol	Length	Info
7506	330.837557	172.16.3.23	172.16.1.33	Modbus/TCP	117	Query: Trans: 0; Unit: 1, Fu
7697	350.004671	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 35064; Unit: 1, Fu
7695	350.002802	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 34808; Unit: 1, Fu
7688	349.004556	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 34040; Unit: 1, Fu
7686	349.002422	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 33784; Unit: 1, Fu
7678	348.004526	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 33016; Unit: 1, Fu
7676	348.003321	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 32760; Unit: 1, Fu
7669	347.003531	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 31992; Unit: 1, Fu
7667	347.002208	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 31736; Unit: 1, Fu
7659	346.003324	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 30968; Unit: 1, Fu
7657	346.002162	172.16.1.33	172.16.3.23	Modbus/TCP	75	Response: Trans: 30712; Unit: 1, Fu

> Frame 7506: 117 bytes on wire (936 bits), 117 bytes captured (936 bits)

> Ethernet II, Src: RealtekU\_f8:5c:21 (52:54:00:f8:5c:21), Dst: RealtekU\_a4:30:12 (52:54:00:a4:30:12)

> Internet Protocol Version 4, Src: 172.16.3.23, Dst: 172.16.1.33

> Transmission Control Protocol, Src Port: 1073, Dst Port: 502, Seq: 1, Ack: 1, Len: 63

> Modbus/TCP

> Modbus

0000	52 54 00 a4 30 12 52 54	00 f8 5c 21 08 00 45 00	RT..0.RT ..\!..E-
0010	00 67 5f 09 40 00 80 06	3f 2f ac 10 03 17 ac 10	.g_..@... ?/.....
0020	01 21 04 31 01 f6 b7 37	1f 3f 64 97 30 51 50 18	..!1...7 ..?d-0QP-
0030	fa f0 e9 50 00 00 00 00	00 00 00 39 01 10 00 01	...P.... ..9....
0040	00 19 32 00 54 00 68 00	65 00 4d 00 6f 00 64 00	..2.T.h e-M.o.d-
0050	62 00 75 00 73 00 50 00	72 00 6f 00 74 00 6f 00	b-u-s-P- r-o-t-o-
0060	63 00 6f 00 6c 00 49 00	73 00 46 00 75 00 6e 00	c-o-l-I- s-F-u-n-
0070	6e 00 79 00 21		n-y-!

Flag

flag{TheModbusProtocollsFunny!}

参考