

The Magic Modbus


CSAW 2021 CTF

XAngryChairX

The Magic Modbus

429

Climb on the Magic Modbus and see if you can find some of the messages being passed around!

 modbus.pcap

2021-09-10

Contents

The Magic Modbus **3**

Initial Research 3

PCAP Download 3

Follow the stream 4

TCP Stream 4

Solution 4

The Magic Modbus

Writeup by: XAngryChairX

Team: OnlyFeet

Writeup URL: GitHub

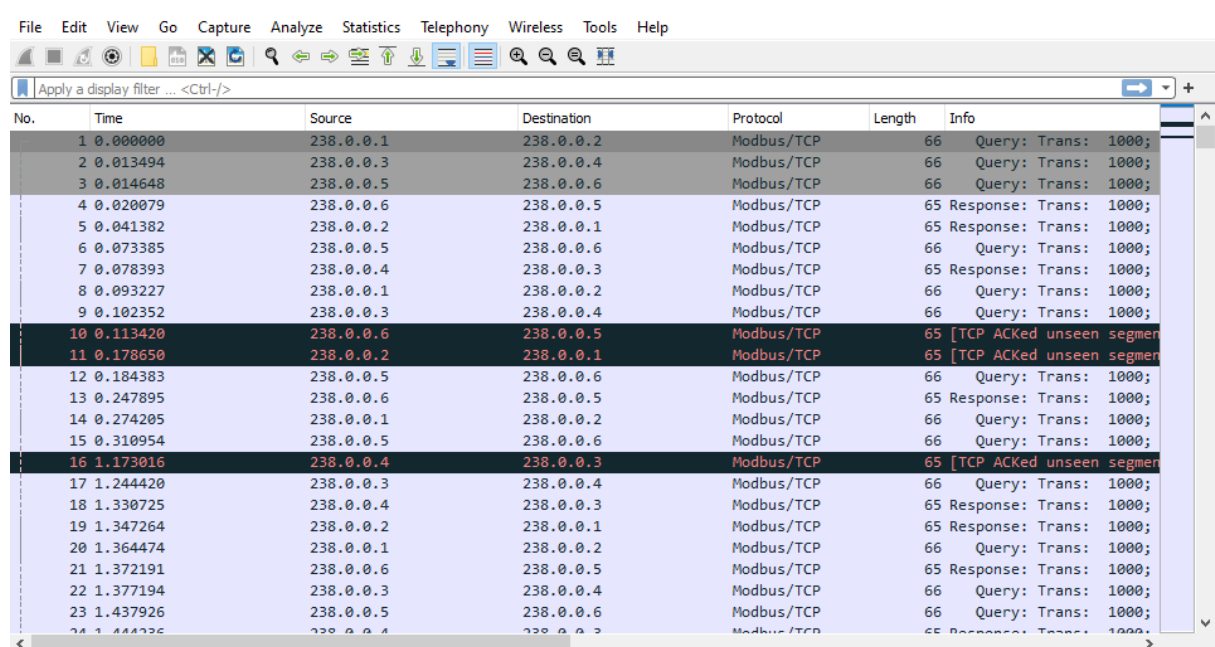
Climb on the Magic Modbus and see **if** you can find some of the messages being passed around!

Initial Research

This challenge presents the security researcher with a pcap file download as the entry point to the challenge.

PCAP Download

Download the pcap file and open it in Wireshark or a related pcap analysis application.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	238.0.0.1	238.0.0.2	Modbus/TCP	66	Query: Trans: 1000;
2	0.013494	238.0.0.3	238.0.0.4	Modbus/TCP	66	Query: Trans: 1000;
3	0.014648	238.0.0.5	238.0.0.6	Modbus/TCP	66	Query: Trans: 1000;
4	0.020079	238.0.0.6	238.0.0.5	Modbus/TCP	65	Response: Trans: 1000;
5	0.041382	238.0.0.2	238.0.0.1	Modbus/TCP	65	Response: Trans: 1000;
6	0.073385	238.0.0.5	238.0.0.6	Modbus/TCP	66	Query: Trans: 1000;
7	0.078393	238.0.0.4	238.0.0.3	Modbus/TCP	65	Response: Trans: 1000;
8	0.093227	238.0.0.1	238.0.0.2	Modbus/TCP	66	Query: Trans: 1000;
9	0.102352	238.0.0.3	238.0.0.4	Modbus/TCP	66	Query: Trans: 1000;
10	0.113420	238.0.0.6	238.0.0.5	Modbus/TCP	65	[TCP ACKed unseen segment]
11	0.178650	238.0.0.2	238.0.0.1	Modbus/TCP	65	[TCP ACKed unseen segment]
12	0.184383	238.0.0.5	238.0.0.6	Modbus/TCP	66	Query: Trans: 1000;
13	0.247895	238.0.0.6	238.0.0.5	Modbus/TCP	65	Response: Trans: 1000;
14	0.274205	238.0.0.1	238.0.0.2	Modbus/TCP	66	Query: Trans: 1000;
15	0.310954	238.0.0.5	238.0.0.6	Modbus/TCP	66	Query: Trans: 1000;
16	1.173016	238.0.0.4	238.0.0.3	Modbus/TCP	65	[TCP ACKed unseen segment]
17	1.244420	238.0.0.3	238.0.0.4	Modbus/TCP	66	Query: Trans: 1000;
18	1.330725	238.0.0.4	238.0.0.3	Modbus/TCP	65	Response: Trans: 1000;
19	1.347264	238.0.0.2	238.0.0.1	Modbus/TCP	65	Response: Trans: 1000;
20	1.364474	238.0.0.1	238.0.0.2	Modbus/TCP	66	Query: Trans: 1000;
21	1.372191	238.0.0.6	238.0.0.5	Modbus/TCP	65	Response: Trans: 1000;
22	1.377194	238.0.0.3	238.0.0.4	Modbus/TCP	66	Query: Trans: 1000;
23	1.437926	238.0.0.5	238.0.0.6	Modbus/TCP	66	Query: Trans: 1000;
24	1.444336	238.0.0.4	238.0.0.3	Modbus/TCP	65	Response: Trans: 1000;

Figure 1: PCAP Contents

Follow the stream

Note that a few packets have a dark background. These stand out, and provide an opportune entry point. Click the first packet with a dark background and follow the TCP stream.

TCP Stream

Upon inspection of the TCP stream, you can see some key characters of interest. Specifically, { and }. Also, the characters f, l, a, and g.

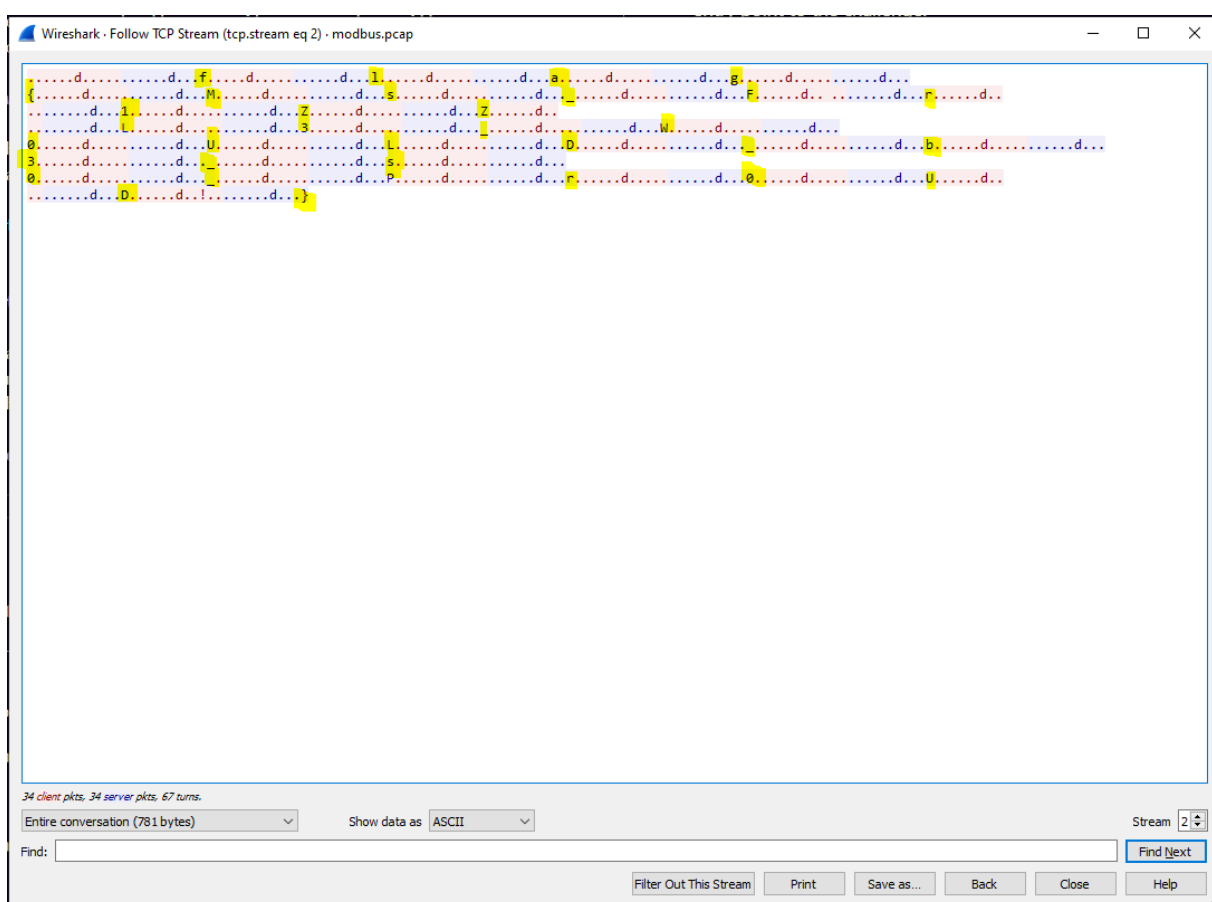


Figure 2: tcp stream

Solution

Following the pattern above, you can decipher the flag.

Submit the flag and claim the points:

flag{Ms_Fr1ZZL3_W0ULD_b3_s0_Pr0UD}