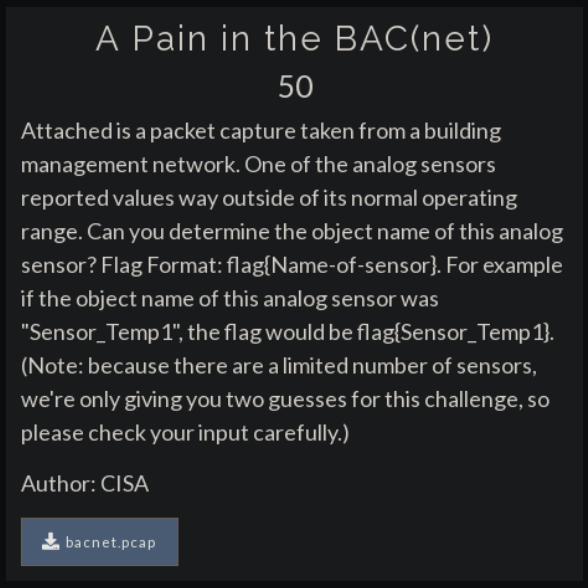
# A Pain in the BAC(net)

CSAW 2021 CTF

SinDaRemedy




2021-09-10

# Contents

# A Pain in the BAC(net)

Writeup by: SinDaRemedy

Team: OnlyFeet

Writeup URL: GitHub

---

```
Attached is a packet capture taken from a building management network.
    One of the analog sensors reported values way outside of its normal
    operating range. Can you determine the object name of this analog
    sensor? Flag Format: flag{Name-of-sensor}. For example if the object
     name of this analog sensor was "Sensor_Temp1", the flag would be
    flag{Sensor_Temp1}. (Note: because there are a limited number of
    sensors, we're only giving you two guesses for this challenge, so
    please check your input carefully.)

Author: CISA
```

## Initial Research

Looking at the name of the challenge you immediately notice that the author is referring to Building Automation Control Networks(BACnet). Additionally, when you look at the attachment you see that is a pcap that could be analyzed with WireShark.

[[Screen Shot 2021-09-12 at 1.50.39 PM.png]]

After reading the question see that there are two main items you need to search/filter for.

- The object-name of the analog sensor.
- Abnormal reported values

Upon opening the pcap in Wireshark you see there are 3017 packets.

[[Screen Shot 2021-09-12 at 2.09.42 PM.png]]

Then I began to look through the packets that had the object name “analog-input, (0)”. I noticed looking through the ADPU section of the capture that the packets could be filtered by obect identifier “analog-input”.

Once filtering by the analog-input identifier I started to notice that there was also a present-value identifier. In the ADPU you can see that it is a property identifier you can filter by. Filtering by both now displays 320 packets to sort through.

[[Screen Shot 2021-09-12 at 1.45.44 PM.png]]

I sorted the packets by info so the analog inputs would be in order and opened up the ADPU and present and started to scan for abnormalities in values. Most of the values were between 1 and 4 digits except for the present value in 4 of the packets in analog input 7.

Now that I spotted the abnormality in the value I started to search for the name of the sensors by object name. After sorting by the info column again you go to the analog-input 7 and can look at the ADPU drop-down to see the object name.

[[Screen Shot 2021-09-12 at 1.49.12 PM.png]]

## Victory

The flag was in the format of “flag{Sensor_#}”, so from here you just submit the flag and claim the points:

**flag{Sensor_12345}**