

A Pain in the BAC(net)

CSAW 2021 CTF

SinDaRemedy

A Pain in the BAC(net)

50

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

 bacnet.pcap

2021-09-10

Contents

A Pain in the BAC(net)	3
Initial Research	3
Victory	6

A Pain in the BAC(net)

Writeup by: SinDaRemedy

Team: OnlyFeet

Writeup URL: GitHub

```
1 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.)
2
3 Author: CISA
```

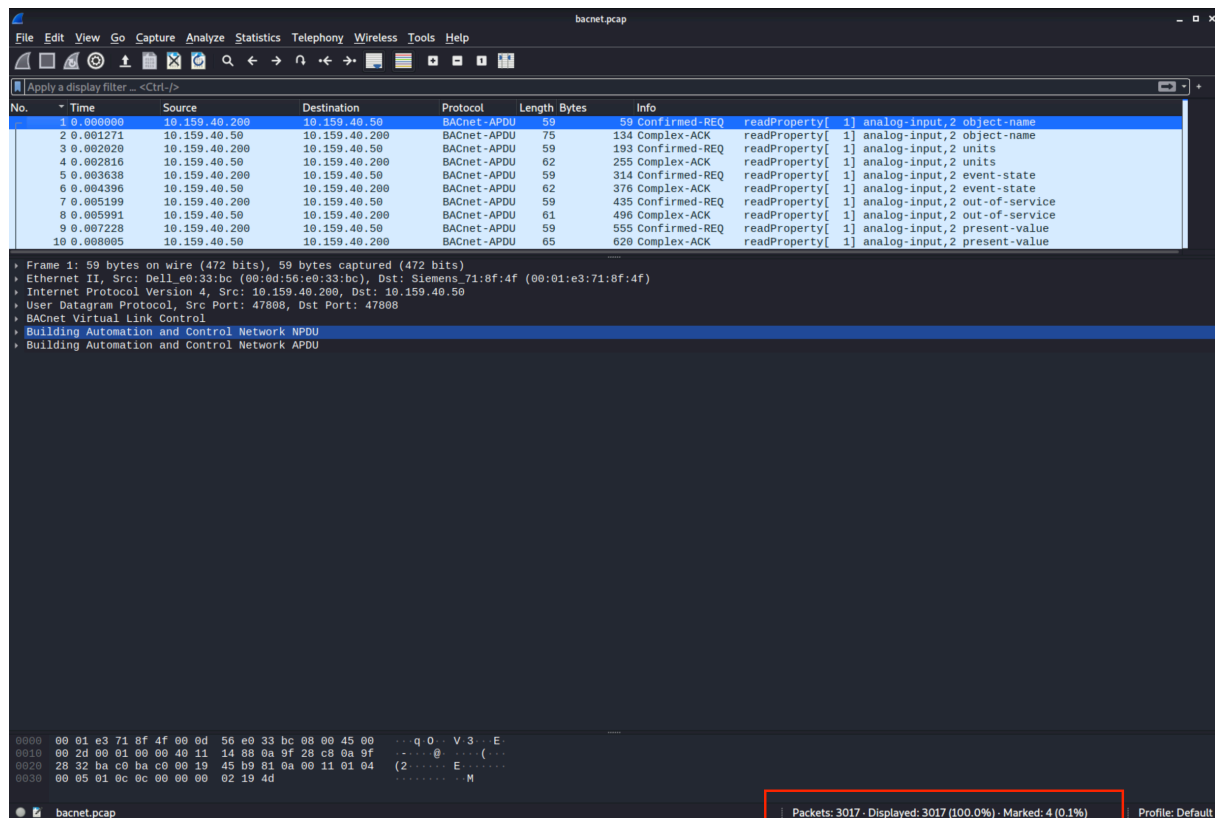
Initial Research

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.

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.



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 object 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.

Wireshark packet capture showing BACnet traffic. The top pane displays a list of packets sorted by info, with packet 1883 highlighted. The middle pane shows the packet details for packet 1883, which is a BACnet-APDU readProperty request for analog-input, 7 present-value. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Bytes	Info
2284	188.668343	10.159.40.55	10.159.40.200	BACnet-APDU	65	18352	Complex-ACK readProperty[1] analog-input,7 present-value
2113	178.382641	10.159.40.55	10.159.40.200	BACnet-APDU	65	17698	Complex-ACK readProperty[1] analog-input,7 present-value
2033	167.815365	10.159.40.55	10.159.40.200	BACnet-APDU	65	16616	Complex-ACK readProperty[1] analog-input,7 present-value
1973	157.460874	10.159.40.55	10.159.40.200	BACnet-APDU	65	15872	Complex-ACK readProperty[1] analog-input,7 present-value
1833	146.646600	10.159.40.55	10.159.40.200	BACnet-APDU	65	14136	Complex-ACK readProperty[1] analog-input,7 present-value
1883	136.468441	10.159.40.55	10.159.40.200	BACnet-APDU	65	13764	Complex-ACK readProperty[1] analog-input,7 present-value
1793	125.876346	10.159.40.55	10.159.40.200	BACnet-APDU	65	12524	Complex-ACK readProperty[1] analog-input,7 present-value
1572	115.296047	10.159.40.55	10.159.40.200	BACnet-APDU	65	11284	Complex-ACK readProperty[1] analog-input,7 present-value
1172	104.713164	10.159.40.55	10.159.40.200	BACnet-APDU	65	10944	Complex-ACK readProperty[1] analog-input,7 present-value
1112	94.360899	10.159.40.55	10.159.40.200	BACnet-APDU	65	9300	Complex-ACK readProperty[1] analog-input,7 present-value

Packet 1883 details:

- BACnet Virtual Link Control
- Building Automation and Control Network NPDU
- Building Automation and Control Network APDU
 - 0011 ... = APDU Type: Complex-ACK (3)
 - 0000 = PDU Flags: 0x00
 - 0... = Segmented Request: Unsegmented Request
 - 0... = More Segments: No More Segments Follow
 - Invoke ID: 1
 - Service Choice: readProperty (12)
 - ObjectIdentifier: analog-input, 7
 - Context Tag: 0, Length/Value/Type: 4
 - 1... = Tag Class: Context Specific Tag
 - 0000 = Context Tag Number: 0
 - Length Value Type: 4
 - 0000 0000 00... .. = Object Type: analog-input (0)
 - 00 0000 0000 0000 0000 0111 = Instance Number: 7
 - Property Identifier: present-value (85)
 - Context Tag: 1, Length/Value/Type: 1
 - 1... = Tag Class: Context Specific Tag
 - 0001 = Context Tag Number: 1
 - Length Value Type: 1
 - Property Identifier: present-value (85)

Packet 1883 raw data (hex): 00 0d 56 e0 33 bc 00 01 e3 db 6e c0 08 00 45 00 00 33 00 01 00 00 11 14 7d 0a 9f 28 37 0a 9f 28 c8 ba c0 ba c0 00 1f 37 60 81 0a 00 17 01 00 30 01 0c 0c 00 00 07 19 55 3e 44 47 c3 4f 1f 00 00 3f

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.

The image shows a Wireshark capture of BACnet traffic. The top pane displays a list of packets, all of which are BACnet-APDU messages of type Complex-ACK, sent from 10.159.40.55 to 10.159.40.200. The bottom pane shows the detailed view of a selected packet (packet 12, time 115.289688). The packet is a BACnet-APDU message of type Complex-ACK, containing a readProperty request for object-name. The request is a segmented request with no more segments to follow. The object name is 'Sensor_12345'. The response is a segmented response with no more segments to follow, containing the value '6e 73 6f 72 5f 31 32 33 34 35 3f'.

Time	Source	Destination	Protocol	Length	Bytes	Info
136.460275	10.159.40.55	10.159.40.200	BACnet-APDU	75	12463	Complex-ACK readProperty[1] analog-input,7 object-name
125.869144	10.159.40.55	10.159.40.200	BACnet-APDU	75	11713	Complex-ACK readProperty[1] analog-input,7 object-name
115.289688	10.159.40.55	10.159.40.200	BACnet-APDU	75	10963	Complex-ACK readProperty[1] analog-input,7 object-name
104.706700	10.159.40.55	10.159.40.200	BACnet-APDU	75	8144	Complex-ACK readProperty[1] analog-input,7 object-name
94.353689	10.159.40.55	10.159.40.200	BACnet-APDU	75	7694	Complex-ACK readProperty[1] analog-input,7 object-name
84.172018	10.159.40.55	10.159.40.200	BACnet-APDU	75	7469	Complex-ACK readProperty[1] analog-input,7 object-name
73.470289	10.159.40.55	10.159.40.200	BACnet-APDU	75	6569	Complex-ACK readProperty[1] analog-input,7 object-name
63.057009	10.159.40.55	10.159.40.200	BACnet-APDU	75	6044	Complex-ACK readProperty[1] analog-input,7 object-name
52.416192	10.159.40.55	10.159.40.200	BACnet-APDU	75	5219	Complex-ACK readProperty[1] analog-input,7 object-name
41.947619	10.159.40.55	10.159.40.200	BACnet-APDU	75	4619	Complex-ACK readProperty[1] analog-input,7 object-name

```

0011 .... = APDU Type: Complex-ACK (3)
... 0000 = PDU Flags: 0x0
... 0... = Segmented Request: Unsegmented Request
... 0... = More Segments: No More Segments Follow
Invoke ID: 1
Service Choice: readProperty (12)
Object Identifier: analog-input, 7
- Context Tag: 0, Length/Value/Type: 4
... 1... = Tag Class: Context Specific Tag
0000 .... = Context Tag Number: 0
Length Value Type: 4
0000 0000 00... = Object Type: analog-input (0)
... ..00 0000 0000 0000 0000 0111 = Instance Number: 7
- Property Identifier: object-name (77)
- Context Tag: 1, Length/Value/Type: 1
... 1... = Tag Class: Context Specific Tag
0001 .... = Context Tag Number: 1
Length Value Type: 1
Property Identifier: object-name (77)
- [3]
... 1... = Tag Class: Context Specific Tag
0011 .... = Context Tag Number: 3
... ..110 = Named Tag: Opening Tag (0)
- Object Name
Object Name: Sensor_12345
- Application Tag: Character String, Length/Value/Type: 13
... 0... = Tag Class: Application Tag
0111 .... = Application Tag Number: Character String (7)
... ..101 = Named Tag: Extended Value (5)
Length Value Type: 13
String Character Set: ANSI X3.4 / UTF-8 (since 2010) (0)
- [3]
... 1... = Tag Class: Context Specific Tag
0011 .... = Context Tag Number: 3
... ..111 = Named Tag: Closing Tag (7)
0000 00 0d 56 e0 33 bc 00 01 e3 db 6e c0 08 00 45 00 .. V 3 ... n ... E
0010 00 3d 00 01 00 00 40 11 14 73 9a 9f 28 37 0a 9f .. = ... @ ... s ... (7 ...
0020 28 c8 ba c0 ba c0 00 29 ca f6 81 0a 00 21 01 00 (.....) ..... !...
0030 30 01 0c 0c 00 00 00 07 19 4d 3e 75 0d 00 53 05 0..... M>u .. Se
0040 6e 73 6f 72 5f 31 32 33 34 35 3f nsor_12345?

```

Object Name (bacapp.object_name), 12 bytes

Packets: 3017 - Displayed: 280 (9.3%) - Marked: 4 (0.1%) - Profile: Default

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}