The Unknown Message CTF

Official Writeup.

Author / THM : kave3nirmal141

Overview.

- Lumen-9, a deep-space reconnaissance satellite, went silent during a routine pass. The room provides recovered artifacts (**comm, telemetry, blackbox, and an image**). The player's mission is to reconstruct the final timeline, extract fragmented data, and reveal the hidden message in the final image.

Files Provided.

1. ***Comm.txt***
2. ***Telemetry.log***
3. ***Blackbox.dd***

Tools Used.

- **echo, rev, base64, kali linux & sharp eyes.**

IMPORTANT NOTE!!!

Real World vs This CTF

Satellite systems are far more complex in reality, so a few elements were simplified for this CTF:

- **Comm.txt** : Real Radio Frequency links and space-packet protocols are shown as readable IP/port logs.
- **Telemetry.log** : Normally binary and encoded — provided here as plain text.
- **Blackbox.dd** : Actual spacecraft storage replaced with a standard .dd image.
- **Image file**: Used for steganography instead of real mission imaging formats.

These changes keep the investigation realistic in concept while making analysis practical.

CTF Walkthrough.

Task 1 Uplink Channel Analysis

1. Which uplink channel (port) did Lumen-9 use to transmit its final data to Vega Outpost on Earth?

comm.txt

```
1 1758166200|192.0.2.10|203.0.113.42|50000|5600|SYN
2 1758166202|203.0.113.42|192.0.2.10|5600|50000|SYN-ACK
3 1758166203|192.0.2.10|203.0.113.42|50000|5600|ACK
4 1758166220|192.0.2.10|203.0.113.42|50000|5600|HELLO frame_id=440
5 1758166230|192.0.2.10|203.0.113.42|50000|5600|TEMP:17.5;PWR:29.0
6 1758166240|192.0.2.10|198.51.100.5|50001|5600|NOISE_PACKET_A
7 1758166250|192.0.2.10|203.0.113.42|50001|5600|LOG:frame_id=441
8 1758166260|192.0.2.10|203.0.113.42|50001|5600|BEACON seq=441 link_status=OK
9 1758166270|192.0.2.10|203.0.113.42|50001|5600|SENSOR:CAM_OK
10 1758166280|192.0.2.10|203.0.113.42|50001|5600|NOISE_PACKET_B
11 1758166290|192.0.2.10|203.0.113.42|50002|5600|ROUTE:VegaOutpost
12 1758166300|192.0.2.10|203.0.113.42|50002|5600|TELEMETRY_OK frame_id=442
13 1758166310|192.0.2.10|203.0.113.42|50002|5600|BASE64_FRAG_1=TkVCVUxBLU
14 1758166320|203.0.113.42|192.0.2.10|5600|50002|ACK
15 1758166330|192.0.2.10|203.0.113.42|50003|5600|NOISE_PACKET_C
16 1758166340|192.0.2.10|203.0.113.42|50003|5600|LOG:frame_id=443
17 1758166350|192.0.2.10|198.51.100.5|50003|5600|FINAL_FRAME_PART
18 1758166360|192.0.2.10|203.0.113.42|50003|5600|BASE64_FRAG_2=RPT1ItT1BFT
19 1758166370|203.0.113.42|192.0.2.10|5600|50003|ACK
20 1758166380|192.0.2.10|203.0.113.42|50004|5600|BEACON seq=444 link_status=OK
21 1758166390|192.0.2.10|203.0.113.42|50004|5600|NOISE_PACKET_D
22 1758166400|192.0.2.10|203.0.113.42|50004|5600|ORBIT_ADJ ok
23 1758166410|192.0.2.10|203.0.113.42|50005|5600|STATUS_OK
24 1758166420|192.0.2.10|203.0.113.42|50005|5600|SENSOR:THERM_OK
25 1758166430|192.0.2.10|203.0.113.42|50005|5600|PING
26 1758166440|192.0.2.10|203.0.113.42|50006|5600|FINAL_FRAME
27 1758166450|192.0.2.10|203.0.113.42|50006|5600|NOISE_PACKET_E
28 1758166460|192.0.2.10|203.0.113.42|50006|5600|LOG_ROTATE
29 1758166470|192.0.2.10|203.0.113.42|50007|5600|CHECKSUM_OK
30 1758166480|192.0.2.10|203.0.113.42|50007|5600|TELEMETRY_OK frame_id=451
31 1758166490|192.0.2.10|198.51.100.5|50008|5600|NOISE_PACKET_F
32 1758166500|192.0.2.10|203.0.113.42|50008|5600|BASE64_FRAG_3_HINT=see_telemetry
33 1758166510|192.0.2.10|203.0.113.42|50009|5600|FINAL_FRAME_HDR
```

- **BEACON seq=441**: *Beacon Signals sent at fixed intervals so Earth receivers can track and measure signal strength*.

- Since BEACON Signals Are Sent To Earth You Must Look At From Which channel (port) it sent. That's Your Answer For No.1

- The Yellow Line Highlights The IP's of Lumen-9 & Vega Outpost.

Answer: 5* port.**

Task 2 The Fragmented Signal

2. What is the password use to protect satellite's final image.

comm.txt

```
1758166200|192.0.2.10|203.0.113.42|50000|5600|SYN
1758166202|203.0.113.42|192.0.2.10|5600|50000|SYN-ACK
1758166203|192.0.2.10|203.0.113.42|50000|5600|ACK
1758166220|192.0.2.10|203.0.113.42|50000|5600|HELLO frame_id=440
1758166230|192.0.2.10|203.0.113.42|50000|5600|TEMP:17.5;PWR:29.0
1758166240|192.0.2.10|198.51.100.5|50001|5600|NOISE_PACKET_A
1758166250|192.0.2.10|203.0.113.42|50001|5600|LOG:frame_id=441
1758166260|192.0.2.10|203.0.113.42|50001|5600|BEACON seq=441 link_status=OK
1758166270|192.0.2.10|203.0.113.42|50001|5600|SENSOR:CAM_OK
1758166280|192.0.2.10|203.0.113.42|50001|5600|NOISE_PACKET_B
1758166290|192.0.2.10|203.0.113.42|50002|5600|ROUTE:VegaOutpost
1758166300|192.0.2.10|203.0.113.42|50002|5600|TELEMETRY_OK frame_id=442
1758166310|192.0.2.10|203.0.113.42|50002|5600|BASE64_FRAG_1=[redacted]
1758166320|203.0.113.42|192.0.2.10|5600|50002|ACK
1758166330|192.0.2.10|203.0.113.42|50003|5600|NOISE_PACKET_C
1758166340|192.0.2.10|203.0.113.42|50003|5600|LOG:frame_id=443
1758166350|192.0.2.10|198.51.100.5|50003|5600|FINAL_FRAME_PART
1758166360|192.0.2.10|203.0.113.42|50003|5600|BASE64_FRAG_2=[redacted]
1758166370|203.0.113.42|192.0.2.10|5600|50003|ACK
1758166380|192.0.2.10|203.0.113.42|50004|5600|BEACON seq=444 link_status=OK
1758166390|192.0.2.10|203.0.113.42|50004|5600|NOISE_PACKET_D
1758166400|192.0.2.10|203.0.113.42|50004|5600|ORBIT_ADJ ok
1758166410|192.0.2.10|203.0.113.42|50005|5600|STATUS_OK
1758166420|192.0.2.10|203.0.113.42|50005|5600|SENSOR:THERM_OK
1758166430|192.0.2.10|203.0.113.42|50005|5600|PING
1758166440|192.0.2.10|203.0.113.42|50006|5600|FINAL_FRAME
1758166450|192.0.2.10|203.0.113.42|50006|5600|NOISE_PACKET_E
1758166460|192.0.2.10|203.0.113.42|50006|5600|LOG_ROTATE
1758166470|192.0.2.10|203.0.113.42|50007|5600|CHECKSUM_OK
1758166480|192.0.2.10|203.0.113.42|50007|5600|TELEMETRY_OK frame_id=451
1758166490|192.0.2.10|198.51.100.5|50008|5600|NOISE_PACKET_F
1758166500|192.0.2.10|203.0.113.42|50008|5600|BASE64_FRAG_3_HINT=see_telemetry
1758166510|192.0.2.10|203.0.113.42|50009|5600|FINAL_FRAME_HDR
```

telemetry.log

```
2025-09-18T03:34:00Z INFO  system:boot_time=129600 uptime=1200
2025-09-18T03:34:20Z DEBUG sensors:gyro=0.00011 mag=0.0020 accel=0.0008
2025-09-18T03:34:40Z INFO  nav:coarse_lock=OK
2025-09-18T03:34:55Z INFO  sensors:cam_status=READY cam_exposure=0.6 payload_id=img_0086
2025-09-18T03:35:10Z INFO  storage:cache_free=125000
2025-09-18T03:35:30Z INFO  system:task=health_report status=OK
2025-09-18T03:35:50Z DEBUG sensors:temp=17.4 power=28.9
2025-09-18T03:36:10Z INFO  nav:star_lock=OK
2025-09-18T03:36:30Z INFO  sensors:cam_status=CAPTURED payload_id=img_0087
2025-09-18T03:36:50Z INFO  storage:flush done
2025-09-18T03:37:10Z INFO  system:frame_id=440
2025-09-18T03:37:30Z WARN  comm:uplink_retry=1 last_rssi=-78
2025-09-18T03:37:50Z INFO  sensors:cam_status=READY payload_id=img_0088
2025-09-18T03:38:10Z INFO  health:all_good
2025-09-18T03:38:30Z INFO  nav:course_correction applied
2025-09-18T03:38:50Z DEBUG sensors:gyro=0.00014
2025-09-18T03:39:10Z INFO  sensors:cam_status=READY payload_id=img_0089
2025-09-18T03:39:30Z INFO  storage:write starting
2025-09-18T03:39:50Z INFO  system:frame_id=445
2025-09-18T03:40:10Z WARN  comm:link=degraded retries=2 last_rssi=-90
2025-09-18T03:40:30Z INFO  sensors:cam_status=READY payload_id=img_0090
2025-09-18T03:40:40Z INFO  storage:write_cache low free_blocks=124000
2025-09-18T03:40:50Z INFO  system:prepare_save payload=img_0091
2025-09-18T03:40:55Z INFO  telemetry:seq=450 payload_id=img_0091 BASE64_FRAG_3=[redacted]
2025-09-18T03:41:05Z WARN  comm:uplink_retry=3 last_ack_missing
2025-09-18T03:41:15Z INFO  system:save_status partial_write
2025-09-18T03:41:25Z ERROR storage:write_fail sector=4012
2025-09-18T03:41:35Z INFO  system:panic_check running
2025-09-18T03:41:45Z ERROR system:shutdown initiated cause=UNKNOWN
2025-09-18T03:41:55Z DEBUG postmortem:collecting fragments
2025-09-18T03:42:10Z INFO  recovery:package ready for tx
```

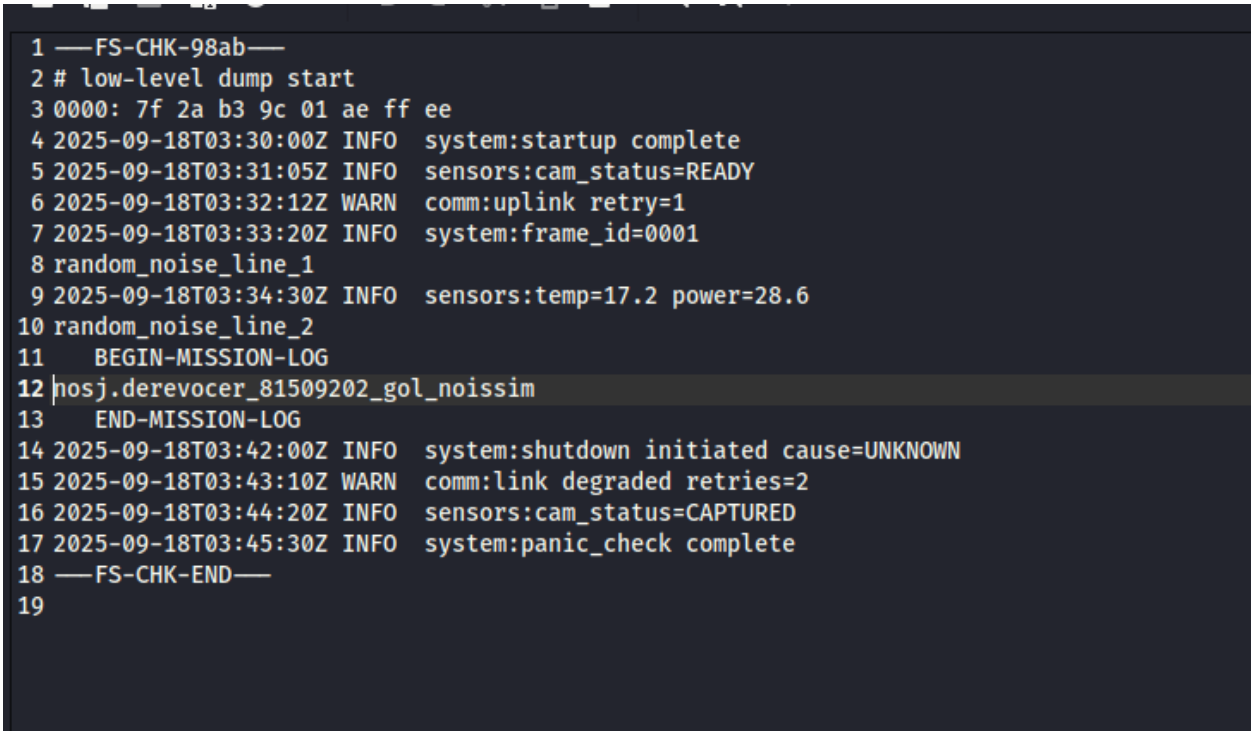
- The base64 fragments are through out the comm.txt and telemetry.txt. And its easy to locate them and **arange them in the correct order .**

- After Locating & arranging them decode them.

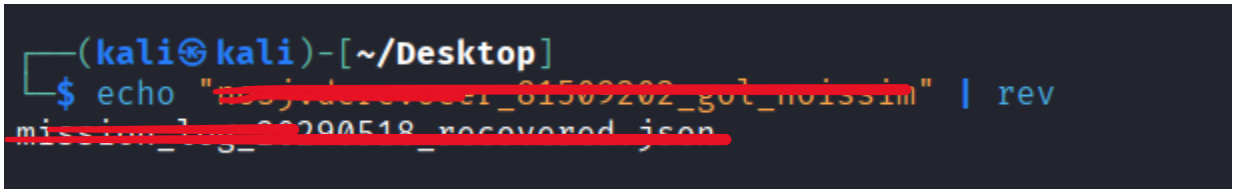
After you decode them you will get the password that protects the final image's **UNKNOWN** message.

Task 3 Blackbox Discovery

blackbox.dd



- Look for something scrambled and suspicious. Grab that and make sure to rev it.



- After reversing it you will get the **name of the hidden mission log.**

Task 4 The Unknown Message.

- Extract the hidden message from the ***Mysterious capture.jpg*** by using the password took from comm.txt and telemetry.log.

- After that the final message will be written on a .txt file in your current directory.

----------END----------