

**Caso Práctico Seguridad en IoT.  
German Rivera Martínez.**

## **1- Árbol Jerárquico del Sistema.**

El diagrama representa el árbol jerárquico de un sistema de hogar conectado, donde se utilizan diferentes dispositivos IoT conectados a un broker MQTT. Cada dispositivo en el hogar está conectado a través de tópicos específicos que permiten la comunicación y la automatización en conjunto con un panel principal.

### **Jerarquía del Sistema**

- **/hogar**
  - /hogar/salon
    - /hogar/salon/termostato
    - /hogar/salon/sensor\_movimiento
    - /hogar/salon/luces
  - **/hogar/cocina**
    - /hogar/cocina/sensor\_ventana
    - /hogar/cocina/luces
  - **/hogar/habitacion**
    - /hogar/habitacion/boton\_inalambrico
    - /hogar/habitacion/persianas
    - /hogar/habitacion/luces
- **/hogar/panel\_principal**

## 2- Inicio Actualizando el sistema e instalar Mosquitto con los comandos:

```
sudo apt-get update
```

```
sudo apt-get install mosquitto mosquitto-clients
```

```
(kali@kali)-[~]  
$ sudo apt-get update  
Hit:1 http://http.kali.org/kali kali-rolling InRelease  
Reading package lists... Done  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
mosquitto is already the newest version (2.0.18-1.1).  
mosquitto-clients is already the newest version (2.0.18-1.1).  
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

## 3- Iniciar y habilitar el servicio Mosquitto

Acá verificamos el estado del servicio, lo habilitamos para que se inicie automáticamente y volvemos a verificar para su correcto funcionamiento.

```
(kali@kali)-[~]  
$ sudo systemctl status mosquitto  
  
o mosquitto.service - Mosquitto MQTT Broker  
   Loaded: loaded (/usr/lib/systemd/system/mosquitto.service; disabled; preset: disabled)  
   Active: inactive (dead)  
     Docs: man:mosquitto.conf(5)  
           man:mosquitto(8)  
  
(kali@kali)-[~]  
$ sudo systemctl enable mosquitto  
  
Synchronizing state of mosquitto.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable mosquitto  
Created symlink '/etc/systemd/system/multi-user.target.wants/mosquitto.service' → '/usr/lib/systemd/system/mosquitto.service'.  
  
(kali@kali)-[~]  
$ sudo systemctl start mosquitto  
  
(kali@kali)-[~]  
$ sudo systemctl status mosquitto  
  
● mosquitto.service - Mosquitto MQTT Broker  
   Loaded: loaded (/usr/lib/systemd/system/mosquitto.service; enabled; preset: disabled)  
   Active: active (running) since Thu 2024-08-22 01:48:20 EDT; 42s ago  
 Invocation: 129f2997b02a493a9849aead0a922b83  
     Docs: man:mosquitto.conf(5)  
           man:mosquitto(8)  
  Process: 14456 ExecStartPre=/bin/mkdir -m 740 -p /var/log/mosquitto (code=exited, status=0/SUCCESS)  
  Process: 14458 ExecStartPre=/bin/chown mosquitto:mosquitto /var/log/mosquitto (code=exited, status=0/SUCCESS)  
  Process: 14460 ExecStartPre=/bin/mkdir -m 740 -p /run/mosquitto (code=exited, status=0/SUCCESS)  
  Process: 14462 ExecStartPre=/bin/chown mosquitto:mosquitto /run/mosquitto (code=exited, status=0/SUCCESS)  
 Main PID: 14464 (mosquitto)  
    Tasks: 1 (limit: 2269)  
  Memory: 1.9M (peak: 2.1M)  
     CPU: 79ms  
    CGroup: /system.slice/mosquitto.service  
            └─14464 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf  
  
Aug 22 01:48:20 kali systemd[1]: Starting mosquitto.service - Mosquitto MQTT Broker ...  
Aug 22 01:48:20 kali systemd[1]: Started mosquitto.service - Mosquitto MQTT Broker.
```

#### 4- Creación de usuarios para el bróker.

```
sudo mosquitto_passwd -c /etc/mosquitto/passwd panel_principal
```

Este comando nos crea un archivo de contraseñas y añadimos el usuario panel\_principal, quien tendrá acceso privilegiado a todos los topics.

```
(kali@kali)-[~]  
$ sudo mosquitto_passwd -c /etc/mosquitto/passwd panel_principal  
  
Password:  
Reenter password:
```

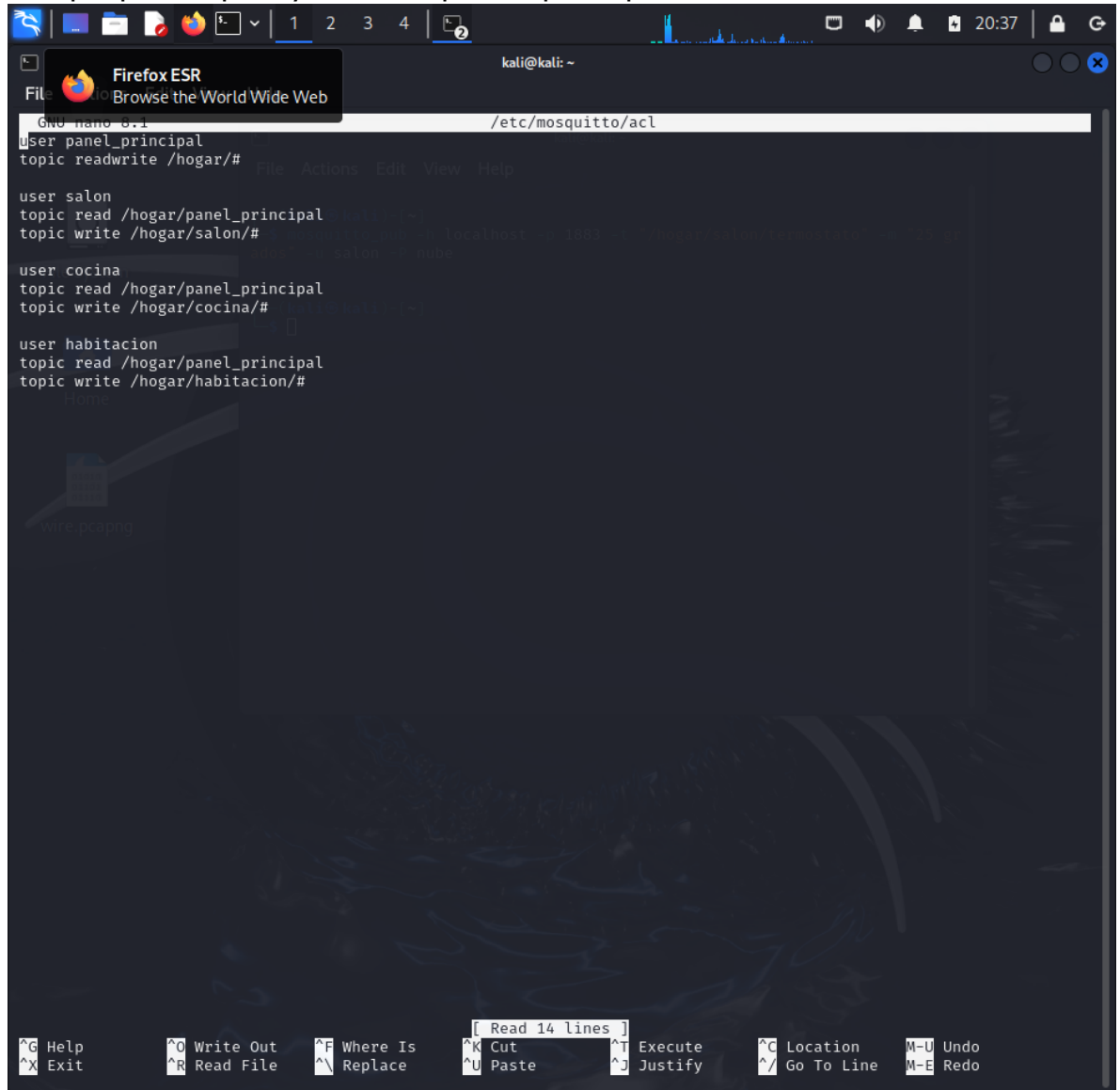
#### 5- Añado más usuarios para las distintas áreas del hogar, permitiendo que cada dispositivo tenga credenciales únicas.

```
(kali@kali)-[~]  
$ sudo mosquitto_passwd -b /etc/mosquitto/passwd salon nube  
sudo mosquitto_passwd -b /etc/mosquitto/passwd cocina nube  
sudo mosquitto_passwd -b /etc/mosquitto/passwd habitacion nube
```

## 6- Configuración ACL.

Acá creamos y configuramos el archivo ACL

Estas reglas ACL son las que controlan qué usuarios pueden leer y escribir en los diferentes topics. El panel\_principal tiene acceso completo, mientras que los otros usuarios solo pueden escribir en sus propios topics y leer del panel\_principal.



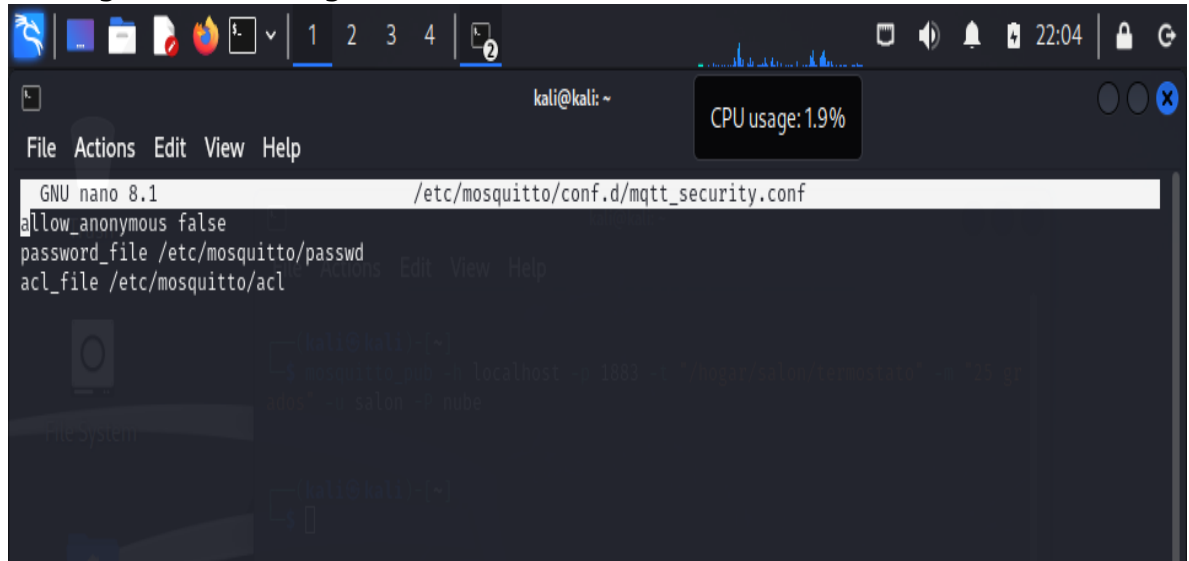
```
GNU nano 2.9.3 /etc/mosquitto/acl
user panel_principal
topic readwrite /hogar/#

user salon
topic read /hogar/panel_principal
topic write /hogar/salon/#

user cocina
topic read /hogar/panel_principal
topic write /hogar/cocina/#

user habitacion
topic read /hogar/panel_principal
topic write /hogar/habitacion/#
```

- 7- **Configuración de Mosquitto** para que utiliza las ACL para así deshabilitar las conexiones anónimas esto deshabilitan las conexiones anónimas, utilizan el archivo de contraseñas y aplican las reglas ACL configuradas.



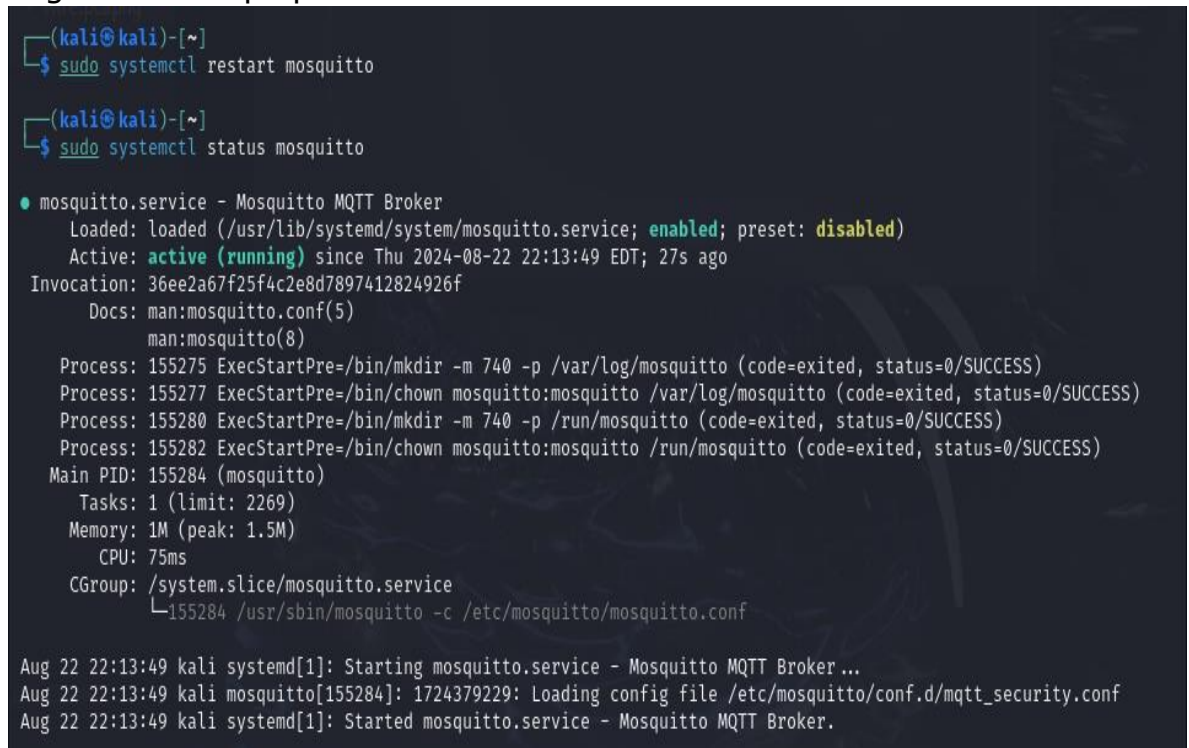
The screenshot shows a terminal window with the nano text editor open, editing the file `/etc/mosquitto/conf.d/mqtt_security.conf`. The configuration includes the following lines:

```
allow_anonymous false
password_file /etc/mosquitto/passwd
acl_file /etc/mosquitto/acl
```

The terminal window also shows the system's top bar with the time 22:04 and a CPU usage of 1.9%.

## 8- Reiniciar Mosquitto.

Lo reinicio para verificar que las nuevas configuraciones de seguridad se apliquen correctamente.



The screenshot shows a terminal window with the following commands and output:

```
(kali@kali)-[~]
$ sudo systemctl restart mosquitto

(kali@kali)-[~]
$ sudo systemctl status mosquitto
```

The output of the `status` command is as follows:

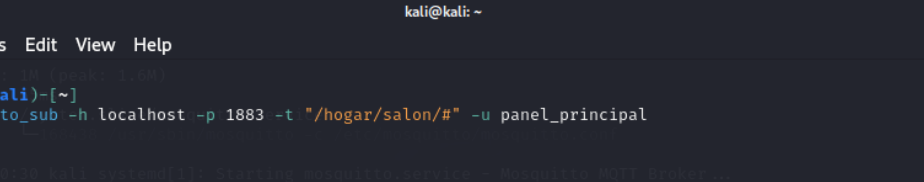
```
● mosquitto.service - Mosquitto MQTT Broker
   Loaded: loaded (/usr/lib/systemd/system/mosquitto.service; enabled; preset: disabled)
   Active: active (running) since Thu 2024-08-22 22:13:49 EDT; 27s ago
     Invocation: 36ee2a67f25f4c2e8d7897412824926f
       Docs: man:mosquitto.conf(5)
            man:mosquitto(8)
    Process: 155275 ExecStartPre=/bin/mkdir -m 740 -p /var/log/mosquitto (code=exited, status=0/SUCCESS)
    Process: 155277 ExecStartPre=/bin/chown mosquitto:mosquitto /var/log/mosquitto (code=exited, status=0/SUCCESS)
    Process: 155280 ExecStartPre=/bin/mkdir -m 740 -p /run/mosquitto (code=exited, status=0/SUCCESS)
    Process: 155282 ExecStartPre=/bin/chown mosquitto:mosquitto /run/mosquitto (code=exited, status=0/SUCCESS)
   Main PID: 155284 (mosquitto)
      Tasks: 1 (limit: 2269)
     Memory: 1M (peak: 1.5M)
        CPU: 75ms
     CGroup: /system.slice/mosquitto.service
            └─155284 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf
```

The bottom of the terminal shows the systemd logs for the service restart:

```
Aug 22 22:13:49 kali systemd[1]: Starting mosquitto.service - Mosquitto MQTT Broker ...
Aug 22 22:13:49 kali mosquitto[155284]: 1724379229: Loading config file /etc/mosquitto/conf.d/mqtt_security.conf
Aug 22 22:13:49 kali systemd[1]: Started mosquitto.service - Mosquitto MQTT Broker.
```

## 9- Simulación de los dispositivos.

Acá estoy simulando con el comando un dispositivo en el salón (termostato) que publica la temperatura "25 grados".



```

kali@kali: ~
File Actions Edit View Help
mosquitto: IM (peak: 1.6M)
(kali@kali)-[~]
$ mosquitto_sub -h localhost -p 1883 -t "/hogar/salon/#" -u panel_principal
-P nube

25 grados
22:48:30 kali: systemd[1]: Starting mosquitto.service - Mosquitto MQTT Broker...
22:48:30 kali: mosquitto[168428]: 1726388830: Loading config file /etc/mosquitto/conf.d/mqtt_security.conf
22:48:30 kali: systemd[1]: Started mosquitto.service - Mosquitto MQTT Broker.

kali@kali: ~
$ cat /etc/mosquitto/mosquitto.conf

kali@kali: ~
$ systemctl restart mosquitto
kali@kali: ~
$ systemctl status mosquitto

● mosquitto.service - Mosquitto MQTT Broker
   Loaded: loaded (/usr/lib/systemd/system/mosquitto.service; enabled; preset: disabled)
   Active: active (running) since Thu 2024-08-22 22:41:06 EDT; 38ms ago
   Invocation: 224018f10441c1b9b6a2f2ae22d5965

```

## 10- Generación de los certificados SSL/TLS.

Con estos comando creamos los certificados SSL/TLS:

```
sudo openssl genpkey -algorithm RSA -out
/etc/mosquitto/certs/mosquitto.key
sudo openssl req -new -key /etc/mosquitto/certs/mosquitto.key -
out /etc/mosquitto/certs/mosquitto.csr
sudo openssl x509 -req -in /etc/mosquitto/certs/mosquitto.csr -
signkey /etc/mosquitto/certs/mosquitto.key -out
/etc/mosquitto/certs/mosquitto.crt
```

[illegible]

## 11- Simulación de los dispositivos.

Dispositivo publicador:

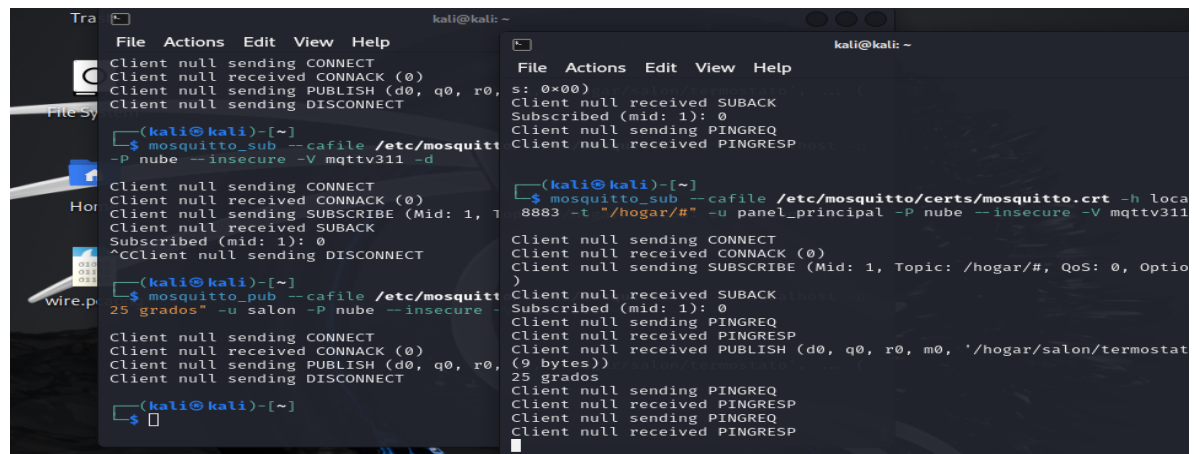
Acá explico el comando usado: **mosquitto\_pub --cafile /etc/mosquitto/certs/mosquitto.crt -h localhost -p 8883 -t "/hogar/salon/termostato" -m "25 grados" -u salon -P nube --insecure -V mqttv311 -d**

**Explicación:**

- **--cafile /etc/mosquitto/certs/mosquitto.crt:** Especifica el certificado del CA para la conexión segura.
- **-h localhost:** Indica que te estás conectando al broker MQTT local.
- **-p 8883:** Utiliza el puerto 8883, que es el estándar para conexiones MQTT seguras.
- **-t "/hogar/salon/termostato":** Publica el mensaje en el tema /hogar/salon/termostato.
- **-m "25 grados":** El mensaje que envía el dispositivo, en este caso "25 grados".
- **-u salon -P nube:** Credenciales del dispositivo.
- **--insecure:** Deshabilita la verificación del nombre del servidor, útil para pruebas.
- **-V mqttv311:** Usa la versión 3.1.1 del protocolo MQTT.
- **-d:** Activa el modo de depuración para ver detalles de la conexión y mensajes.

Simulación de dispositivo suscriptor.

Uso el comando: **mosquitto\_sub --cafile /etc/mosquitto/certs/mosquitto.crt -h localhost -p 8883 -t "/hogar/#" -u panel\_principal -P nube --insecure -V mqttv311 -d**



The image shows two terminal windows side-by-side on a Kali Linux system. The left window shows the execution of the `mosquitto_pub` command, which publishes a message "25 grados" to the topic `/hogar/salon/termostato`. The right window shows the execution of the `mosquitto_sub` command, which subscribes to the topic `/hogar/#` and receives the published message "25 grados". Both windows show detailed MQTT protocol logs, including CONNECT, SUBSCRIBE, PUBLISH, and DISCONNECT messages.

```
(kali@kali)-[~]
$ mosquitto_pub --cafile /etc/mosquitto/certs/mosquitto.crt -h localhost -p 8883 -t "/hogar/salon/termostato" -m "25 grados" -u salon -P nube --insecure -V mqttv311 -d

Client null sending CONNECT
Client null received CONNACK (0)
Client null sending PUBLISH (d0, q0, r0, m0, '/hogar/salon/termostato', 25 bytes)
Client null sending DISCONNECT

(kali@kali)-[~]
$ mosquitto_sub --cafile /etc/mosquitto/certs/mosquitto.crt -h localhost -p 8883 -t "/hogar/#" -u panel_principal -P nube --insecure -V mqttv311 -d

s: 0x000
Client null received SUBACK
Subscribed (mid: 1): 0
Client null sending PINGREQ
Client null received PINGRESP

(kali@kali)-[~]
$ mosquitto_sub --cafile /etc/mosquitto/certs/mosquitto.crt -h localhost -p 8883 -t "/hogar/#" -u panel_principal -P nube --insecure -V mqttv311 -d

Client null sending CONNECT
Client null received CONNACK (0)
Client null sending SUBSCRIBE (Mid: 1, Topic: /hogar/#, QoS: 0, Optio
)
Client null received SUBACK
Subscribed (mid: 1): 0
Client null sending PINGREQ
Client null received PINGRESP
Client null receiving PUBLISH (d0, q0, r0, m0, '/hogar/salon/termostato', 25 bytes)
25 grados
Client null sending PINGREQ
Client null received PINGRESP
Client null sending PINGREQ
Client null received PINGRESP
```