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
sudo apt-get install mosquitto mosquitto-clients

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

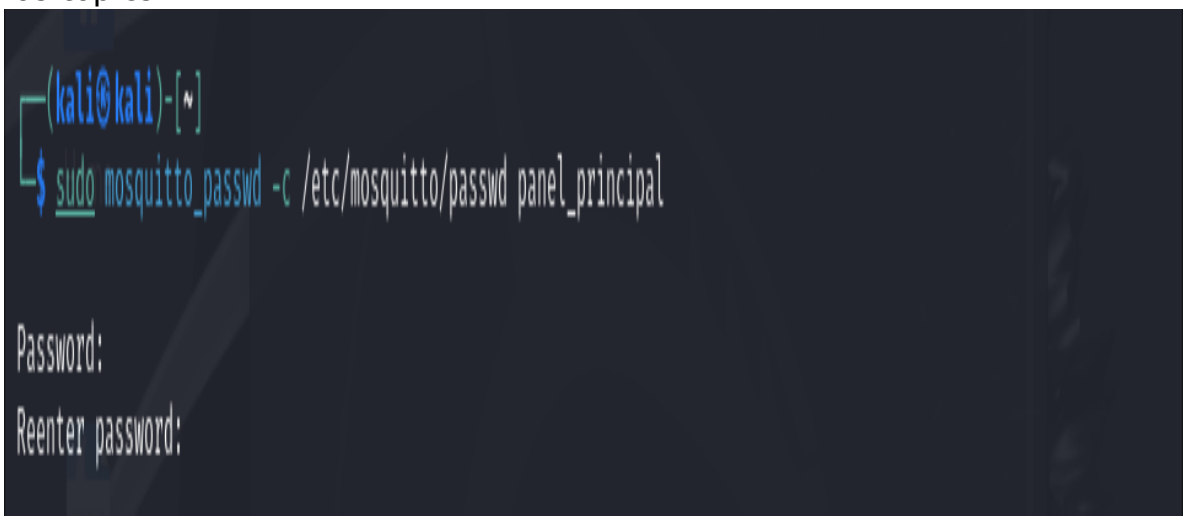
Acá verificamos el estado del servicio, lo habilitamos para que se inicie automáticamente y
volvemos a verificar para su correcto funcionamiento.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status mosquitto

○ 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: 129f2997b02a493a9849aeed0a922b83
       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.
```

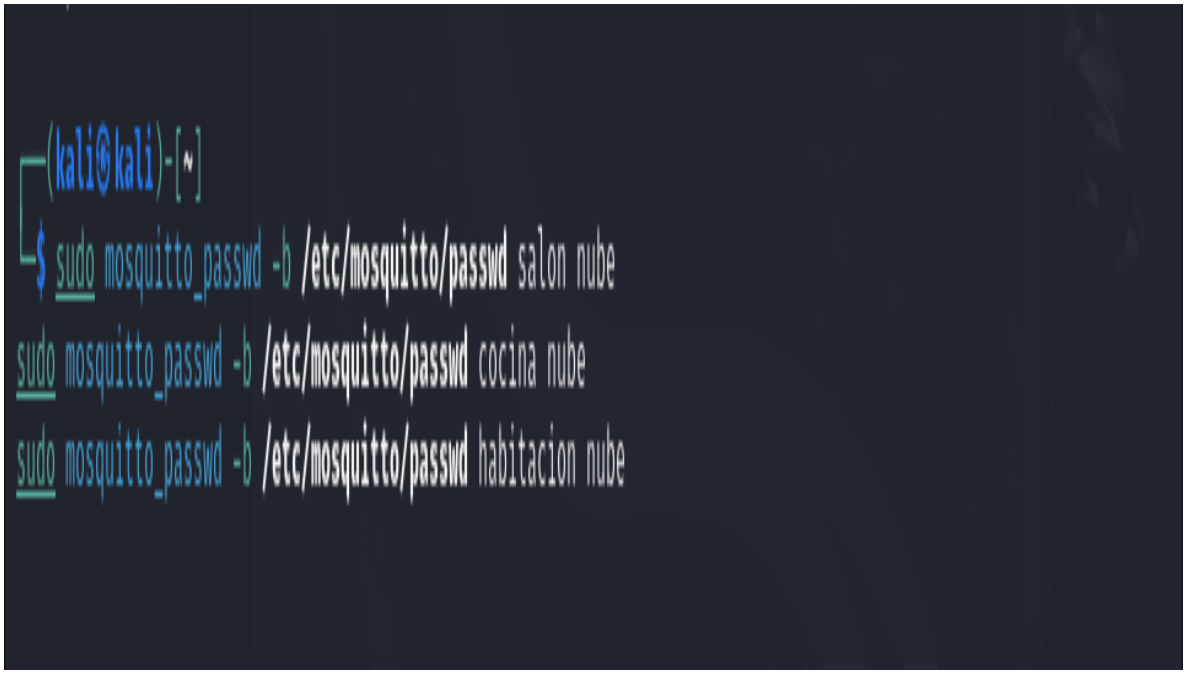
4- Creación de usuarios para el bróker.

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.



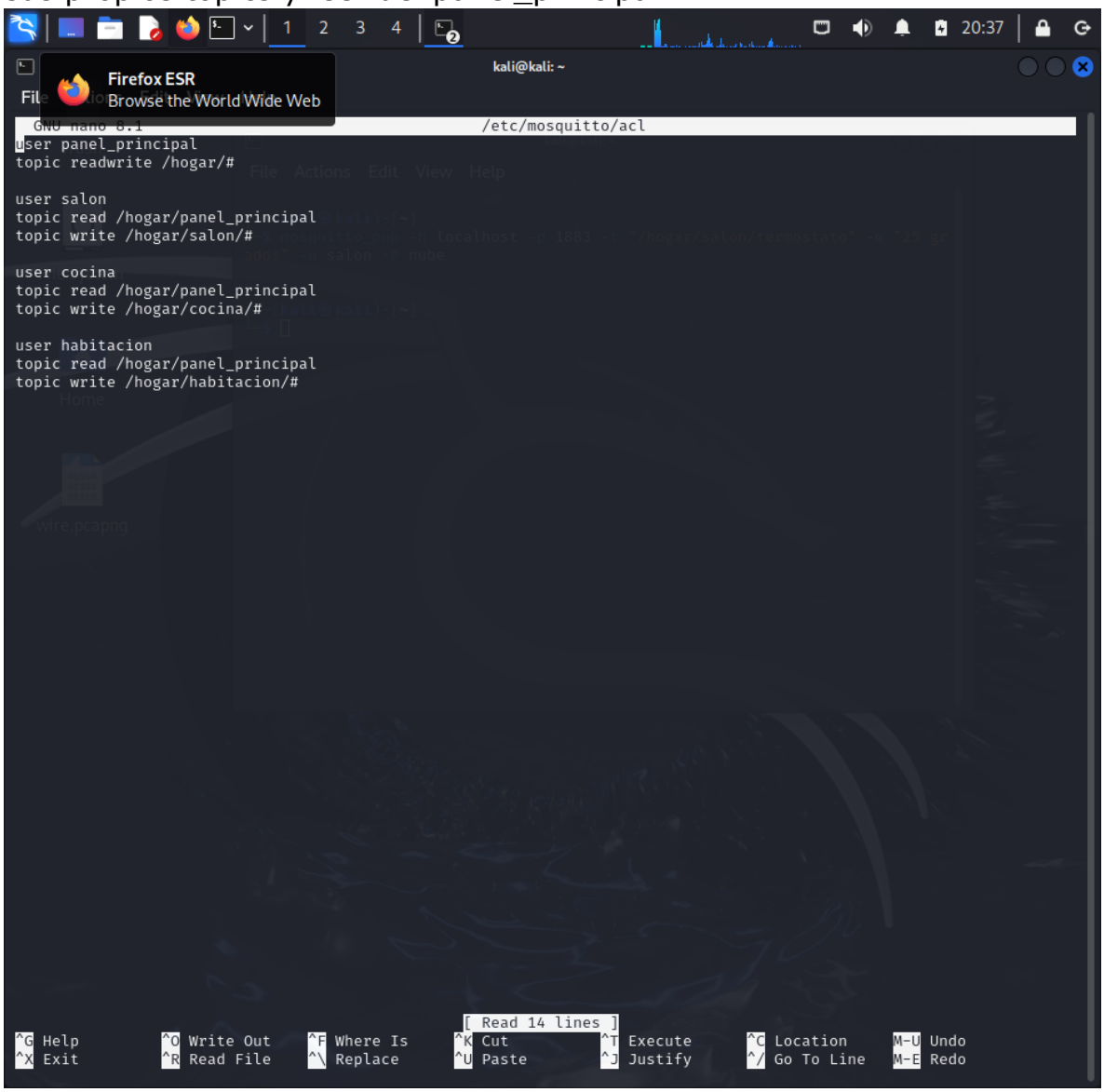
5- Añado más usuarios para las distintas áreas del hogar, permitiendo que cada dispositivo tenga credenciales únicas.



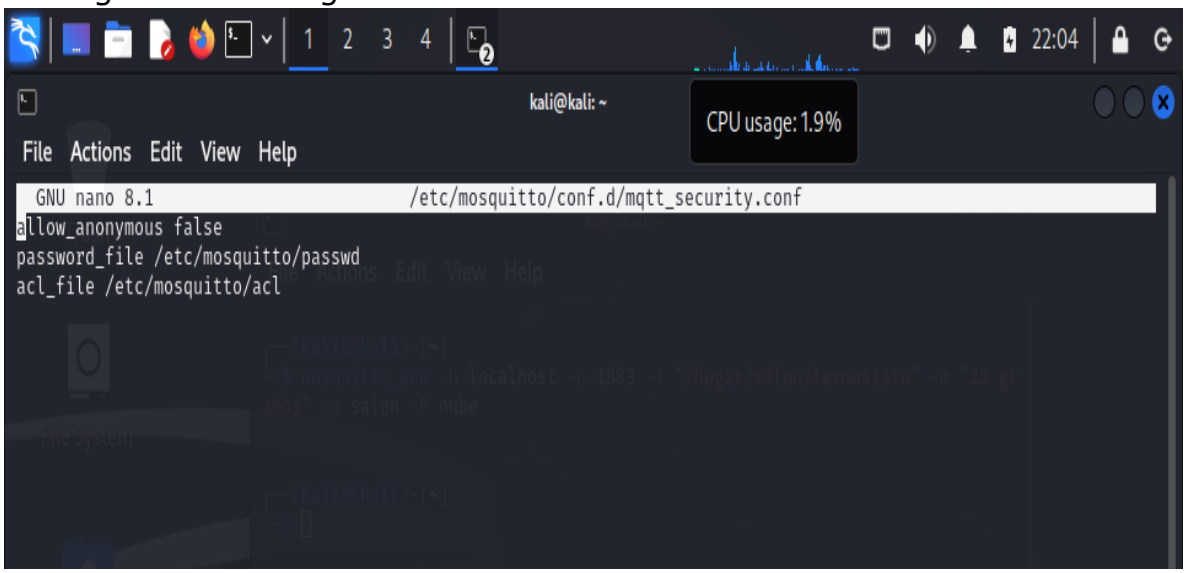
6- Configuración ACL.

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.

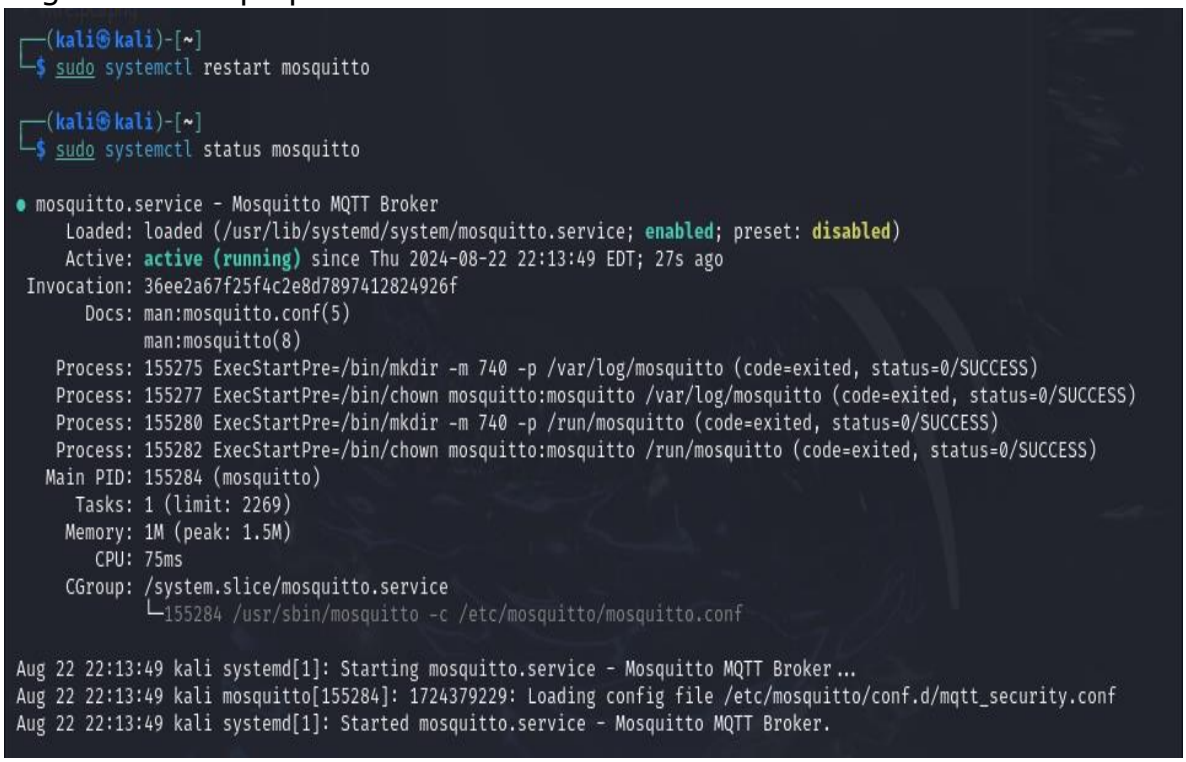


7- **Configuración de Mosquitto** para que utiliza las ACL para así deshabilitar las conexiones anónimas esto deshabilitan las conexiones anónimas, utilizan el archivo de contraseñas y aplican las reglas ACL configuradas.



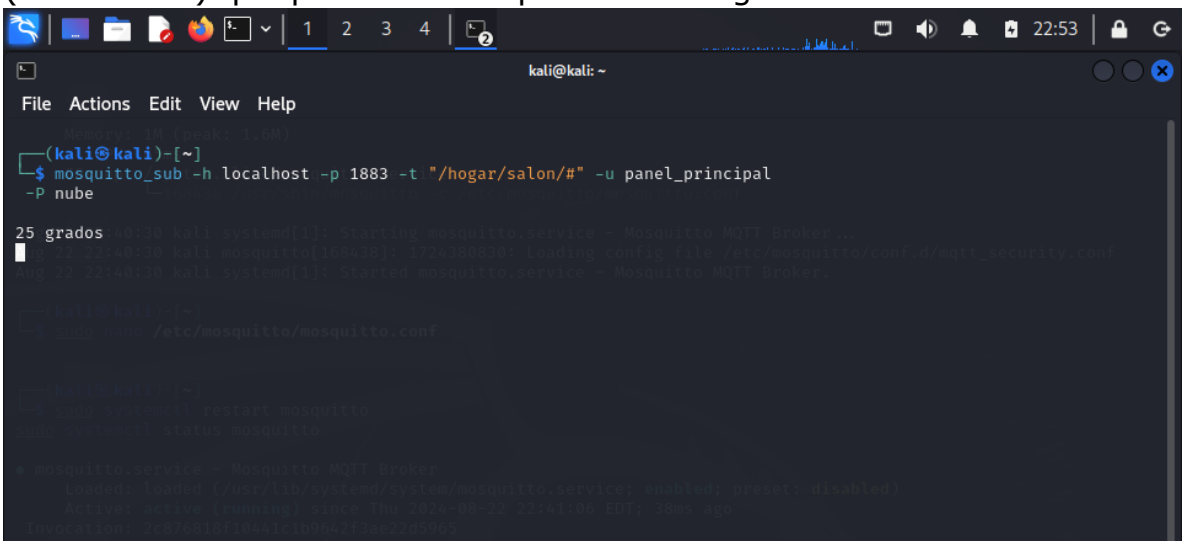
8- Reiniciar Mosquitto.

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



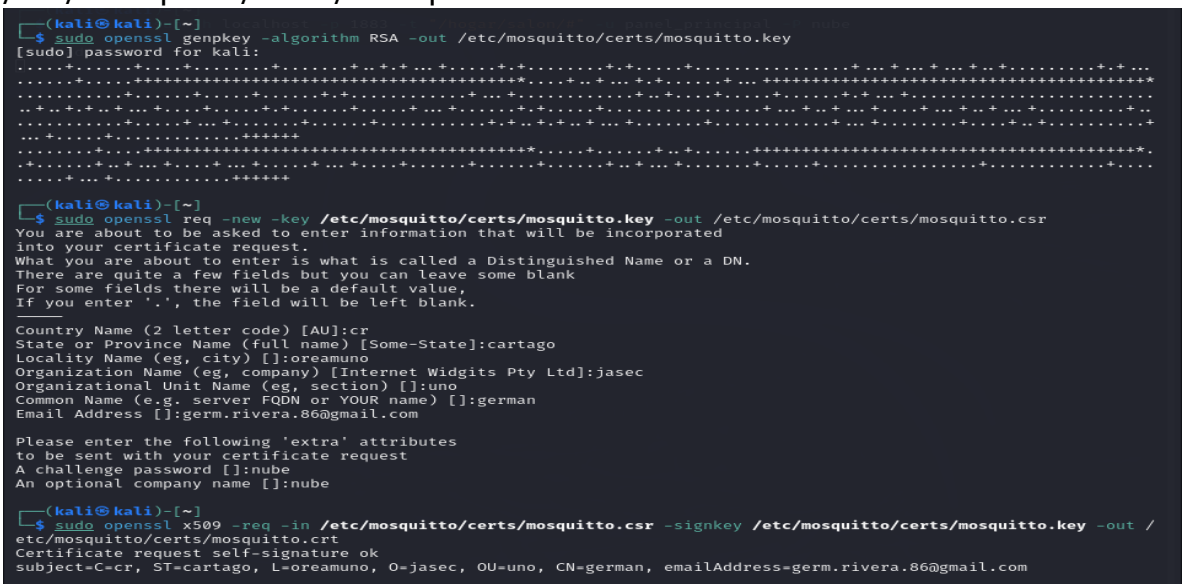
9- Simulación de los dispositivos.

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



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



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**