|  |
| --- |
| Manual de Usuario |
| IoT Shield: Sistema Distribuido de Dispositivos Embebidos para la Prevención y Detección de Ataques en Dispositivos IoT mediante Modelos de Aprendizaje Automático (No Supervisado) |

David Quesada Calderón

10-10-2023

Contenido

[1. Introducción 2](#_Toc148366871)

[2. Instrucciones de uso 2](#_Toc148366872)

[Paso #1: Inicializa las instancias del servidor MQTT (broker). 2](#_Toc148366873)

[Paso #2: Carga del código en los dispositivos IoT. 2](#_Toc148366874)

[Paso #3: Carga del archivo UF2 a los Sistemas Embebidos. 3](#_Toc148366875)

[Paso #4: Ejecución del sistema de distribución. 3](#_Toc148366876)

[Paso #5: Realización de los ataques cibernéticos. 4](#_Toc148366877)

# 1. Introducción

El siguiente documento proporciona instrucciones detalladas sobre cómo utilizar el sistema IoT Shield. Se detallan los pasos para la inicialización de las instancias del servidor MQTT, la carga de código en los dispositivos IoT, la carga del archivo UF2 a los Sistemas Embebidos, la ejecución del sistema de distribución y la realización de ataques cibernéticos.

Es un sistema automático que detecta trafico inusual en la red y notifica a través del correo electrónico. La responsabilidad del usuario radica en tomar medidas correctivas en respuesta a estas notificaciones.

# 2. Instrucciones de uso

Las siguientes instrucciones describen los pasos necesarios para la correcta ejecución del sistema.

### Paso #1: Inicializa las instancias del servidor MQTT (broker).

Para inicializar las instancias 1 y 2, sigue estos pasos:

1. Abre el símbolo del sistema con privilegios de administrador.
2. Utiliza el comando "cd" para navegar hasta el directorio donde está instalado Mosquitto.
3. Ejecuta el siguiente comando para iniciar Mosquitto con la configuración del primer servidor: "mosquitto -c instance1\mosquitto.conf".
4. Repite los pasos 1 y 2 y, luego, ejecuta el siguiente comando para iniciar Mosquitto con la configuración del segundo servidor: "mosquitto -c instance2\mosquitto.conf".

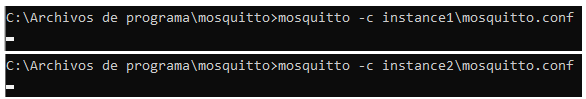


Figura 1: Instancias 1 y 2 en ejecución.

### Paso #2: Carga del código en los dispositivos IoT.

En la carpeta "iot\_code" se encuentran cuatro proyectos correspondientes a cada uno de los cuatro dispositivos IoT. Sigue los siguientes pasos para cargarlos:

1. Conecta el ESP32 al equipo.
2. Abre la carpeta del primer proyecto y abra al archivo ".ino" con Arduino IDE.
3. Verifica que las configuraciones de puerto y placa sean las correctas.
4. Haz clic en "cargar".
5. Repite los pasos del 1 al 4 para los demás proyectos en cada dispositivo.



Figura 2: Carga en Arduino IDE.

### Paso #3: Carga del archivo UF2 a los Sistemas Embebidos.

Para utilizar la inferencia en la Raspberry Pi Pico W, sigue estos pasos:

1. Mantén presionado el botón BOOTSEL mientras conecta la Raspberry Pi Pico W al equipo. Esto hará que aparezca un volumen de disco llamado RPI-RP2. Luego, suelta el botón.
2. Copia el archivo "device\_1.uf2" en el dispositivo. Una vez completada la copia, el volumen se desmontará automáticamente.
3. Repite los pasos 1 y 2 para el dispositivo 2, pero utiliza el archivo "device\_2.uf2".

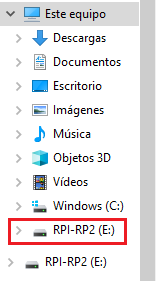
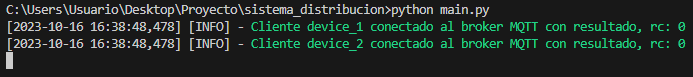


Figura 3: Volumen RPI-RP2.

### Paso #4: Ejecución del sistema de distribución.

Para utilizar el sistema de distribución, sigue estos pasos:

1. Abre el símbolo del sistema con privilegios de administrador.
2. Ejecuta el comando "python main.py" para iniciar el sistema de distribución. A partir de este punto, el sistema estará completamente operativo y podrá observar los mensajes relacionados con el comportamiento de la red.
3. Continúa con el paso #5 para llevar a cabo los ataques cibernéticos.

Figura 4: Sistema de distribución en ejecución.

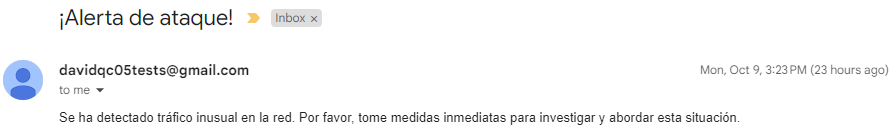


Figura 5: Mensaje de notificación de trafico inusual en la red.

### Paso #5: Realización de los ataques cibernéticos.

Dentro de la carpeta "ataques\_ciberneticos", se encuentra los archivos para llevar a cabo los ataques. Para ejecutar estos ataques, se requiere el uso de un equipo diferente al utilizado para el sistema de distribución. Sigue estos pasos:

1. Abre el archivo "comandos.txt". Este archivo contiene los comandos necesarios para ejecutar diferentes tipos de ataques. Copia el comando correspondiente al ataque que deseas realizar.
2. Abre el símbolo del sistema.
3. Pega el comando copiado y presiona la tecla "Enter" para ejecutar el ataque.



Figura 6: Ataque de fuerza bruta en ejecución.