|  |
| --- |
| Configuración y dependencias |
| 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 1](#_Toc148367036)

[2. Componentes de Hardware 2](#_Toc148367037)

[3. Configuración e instalación en la computadora 2](#_Toc148367038)

[3.1. Instalación del servidor MQTT (broker) 2](#_Toc148367039)

[3.1.1. Configuración de Mosquitto 2](#_Toc148367040)

[3.2. Instalación del analizador de tráfico de red 2](#_Toc148367041)

[3.3. Instalación de dependencias del sistema de distribución y del sistema de generación de ataques cibernéticos. 3](#_Toc148367042)

[3.4. Instalación del entorno de desarrollo Arduino 3](#_Toc148367043)

[3.4.1. Configuración del entorno de desarrollo Arduino 3](#_Toc148367044)

# 1. Introducción

Este documento proporciona una guía detallada para la configuración e instalación de cada componente que forma parte de IoT Shield. Además, se presentan los componentes de hardware requeridos para utilizar sus funcionalidades.

# 2. Componentes de Hardware

Los componentes de hardware necesarios para ejecutar el sistema IoT Shield son los siguientes:

* 2 Raspberry Pi Pico W
* 4 ESP32
* Cables de alimentación para los dispositivos
* 2 Computadoras con sistema operativo Windows 10

# 3. Configuración e instalación en la computadora

## 3.1. Instalación del servidor MQTT (broker)

Para comenzar, es necesario instalar un servidor MQTT, y para este propósito, se utiliza el software Eclipse Mosquitto, el cual se puede descargar desde el siguiente enlace: <https://mosquitto.org/download/>.

### 3.1.1. Configuración de Mosquitto

Después de la instalación del broker, se deben configurar dos instancias del mismo. Para ello, se deben crear dos carpetas con los nombres "instance1" e "instance2" en la ubicación donde Mosquitto ha sido instalado. Luego, se debe crear un archivo de configuración en cada una de estas carpetas, al que se le asignará el nombre "mosquitto.conf".

En cada uno de los archivos de configuración creados, se deben incluir las siguientes líneas:

* listener PUERTO 0.0.0.0
* allow\_anonymous false
* password\_file RUTA

El valor de PUERTO se ajusta a 1883 para el primer archivo y a 1884 para el segundo. En cuanto al valor de RUTA, se debe especificar la ubicación donde se encuentra el archivo de credenciales, por ejemplo, "C:\Program Files\mosquitto\creds.txt".

El archivo llamado "creds.txt" contiene las credenciales requeridas por Mosquitto. Para este proyecto, se ha empleado el nombre de usuario "user1\_david" y la contraseña "pass2\_david". Sigue estos pasos para crear el archivo:

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 crear el archivo "creds.txt" con las credenciales: "echo user1\_david:pass1\_david > creds.txt".
4. Utiliza el siguiente comando para cifrar las contraseñas: "mosquitto\_passwd -U creds.txt".

## 3.2. Instalación del analizador de tráfico de red

Para llevar a cabo la captura del tráfico de red, se utiliza el software Wireshark junto con Tshark. Tshark se instala automáticamente al instalar Wireshark. Puede descargar Wireshark desde el siguiente enlace: <https://www.wireshark.org/>.

## 3.3. Instalación de dependencias del sistema de distribución y del sistema de generación de ataques cibernéticos.

Los sistemas de distribución y generación de ataques cibernéticos están desarrollados en Python y sus respectivos códigos se encuentran en las carpetas "sistema\_distribucion" y "ataques\_ciberneticos".

Para asegurar su funcionamiento óptimo, es necesario instalar las dependencias adecuadas. Cada sistema tiene su propio archivo "requirements.txt" que contiene las bibliotecas necesarias. Para instalar estas dependencias, se debe ejecutar el comando "pip install -r requirements.txt" en la carpeta correspondiente a cada sistema.

**Nota:** Los ataques cibernéticos deben llevarse a cabo desde una computadora diferente a la que se está utilizando para ejecutar el sistema de distribución.

## 3.4. Instalación del entorno de desarrollo Arduino

Para llevar a cabo la carga del código en los dispositivos IoT, es necesario instalar el software Arduino IDE. Puede descargarlo desde el siguiente enlace: <https://www.arduino.cc/en/software>. El código destinado a los dispositivos IoT está ubicado en la carpeta "codigo\_iot/esp32\_code".

### 3.4.1. Configuración del entorno de desarrollo Arduino

Una vez que haya completado la instalación, deberá configurar el entorno para admitir el uso de placas ESP32. Siga estos pasos:

1. Abra Arduino IDE.
2. Vaya a la opción "Archivo" y haga clic en "Preferencias".
3. En la sección de "URLs adicionales de gestor de placas", agregue la siguiente URL: <https://dl.espressif.com/dl/package_esp32_index.json>.

Posteriormente, instale la biblioteca de ESP32 siguiendo estos pasos:

1. Vaya a la pestaña "Herramientas".
2. Seleccione la opción "Placa" y luego haga clic en "Gestor de placas".
3. En el campo de búsqueda, busque "esp32 de Espressif Systems" y haga clic en "Instalar".