UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE COMPUTACIÓN

ANÁLISIS DE VULNERABILIDADES DE INTERNET DE LAS COSAS EN CASOS DE ESTUDIO DE INTRUSIÓN Y DETECCIÓN EN EL LABORATORIO DE SISTEMAS EMBEBIDOS, UPS Q-SUR

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

AUTORES:
MARÍA JOSÉ JÁCOME SÁNCHEZ
HENRY SALVADOR BÁEZ BRAVO

TUTOR:
MANUEL RAFAEL JAYA DUCHE

Quito - Ecuador
2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

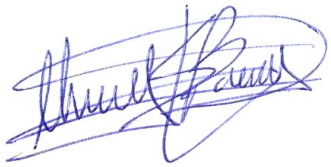
Nosotros, María José Jácome Sánchez con documento de identificación N° 1716853245 y Henry Salvador Báez Bravo con documento de identificación N° 1726526351; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 11 de marzo del año 2022

Atentamente,

.....
María José Jácome Sánchez
1716853245



.....
Henry Salvador Báez Bravo
1726526351

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

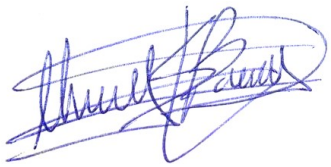
Nosotros, María José Jácome Sánchez con documento de identificación No.1716853245 y Henry Salvador Báez Bravo con documento de identificación No. 1726526351, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Articulo Académico: "Análisis de vulnerabilidades de internet de las cosas en casos de estudio de intrusión y detección en el laboratorio de sistemas embebidos, UPS Q-SUR", el cual ha sido desarrollado para optar por el título de: Ingeniero en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 11 de marzo del año 2022

Atentamente,

.....
María José Jácome Sánchez
1716853245



.....
Henry Salvador Baéz Bravo
1726526351

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Manuel Rafael Jaya Duche con documento de identificación N° 1710631035, docente de la Universidad Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS DE VULNERABILIDADES DE INTERNET DE LAS COSAS EN CASOS DE ESTUDIO DE INTRUSIÓN Y DETECCIÓN EN EL LABORATORIO DE SISTEMAS EMBEBIDOS, UPS Q-SUR, realizado por María José Jácome con documento de identificación N° 1716853245 y por Henry Salvador Báez Bravo con documento de identificación N° 1726526351, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 11 de marzo del año 2022

Atentamente,

Ing. Manuel Rafael Jaya Duche, MSc.
1710631035

Análisis de vulnerabilidades de internet de las cosas en casos de estudio de intrusión y detección en el laboratorio de sistemas embebidos, UPS Q-SUR

1st María José Jácome Sánchez
mjacomes1@est.ups.edu.ec

2nd Henry Salvador Báez Bravo
hbaezb@est.ups.edu.ec

3st Manuel Rafael Jaya Duche
mjaya@ups.edu.ec

***Resumen*—El presente trabajo de investigación tiene por objetivo analizar las vulnerabilidades de internet de las cosas en el laboratorio de Sistemas Embebidos UPS Q-SUR. Se inicia armando y configurando 3 tipos de redes de acuerdo a su cobertura como son: WPAN, WLAN y WWAN con módulos IoT como BT, ESP8266 y Lora TTGO ESP32 respectivamente, a estos módulos se conectan sensores (DHT11, MQ2, PIR). Sobre las redes WWAN y WPAN se efectúa un ataque desde módulos sniffer externos como nRF52840 y CatWAN USB Stick respectivamente y en la red WLAN se realizó un ataque ARP poisoning con la herramienta Ettercap. Una vez efectuados los respectivos ataques, se monitorizó y se capturó los paquetes por medio de Wireshark para evidenciar si los datos se encuentran encriptados o no, determinando así la existencia de vulnerabilidades dentro de cada red analizada. En la red WLAN se encontró una vulnerabilidad y en las otras redes se hallaron paquetes cifrados. De los resultados obtenidos, se pueden decir que ciertas redes presentan vulnerabilidades y otras poseen un cifrado robusto.**

***Palabras Clave*—Seguridad, Hacking ético, EtterCap, Saas, IoT, Confiabilidad, Integridad, WiFislax, Wireshark, ESP32, HC-05, LoRaWan.**

***Abstract*—The objective of this research work is to analyze the vulnerabilities of the internet of things for detection and intrusion in the UPS Q-SUR embedded systems laboratory. For which, it was divided into 3 types of networks according to their coverage, such as: WPAN with IoT Bluethoot modules, WLAN with ESP8266 module and WWAN with Lora TTGO ESP32 modules, which configure each of the networks through which it is transmitted. the data from the sensors (DHT11, MQ2, PIR). An attack is carried out on the WWAN and WPAN network from external sniffer modules such as nRF52840 and CatWAN USB Stick, respectively, and an ARP poisoning attack is carried out on the WLAN with the ettercap tool. Once the respective attacks have been carried out, the packets are monitored and captured by means of Wireshark to show if the data is encrypted or plain data, thus determining if there are vulnerabilities within each analyzed network. With the attack carried out on the network between ESP8266 and the gateway, a vulnerability was found when sending the data to the ThinkSpeak platform, evidencing plain ion.**

***Keywords*—Security, Ethical Hacking, EtterCap, Saas, IoT, Reliability, Integrity, WiFislax, Wireshark, ESP32, HC-05, LoRaWan.**

I. Introducción

Según [1], hoy en día se encuentran bastantes dispositivos en el mercado de IoT, en donde su crecimiento fue proporcional al aumento de vulnerabilidades y peligros por protocolos utilizados, mediante [2] , conduce a un aumento de los ataques cibernéticos que representan un riesgo para las entidades y personas que utilizan esta tecnología aumentando la posibilidad de incidentes de seguridad, pero para [3], la temática de la seguridad tomo inicio al ser examinado en serio al impacto de la gran cantidad de ataques satisfactorios a objetos que se entran en la categoría de IoT como por ejemplo a través de enrutadores u otros dispositivos integrados por medio de puertos.

Para [4], los ataques no guiados forzosamente ejecutados autónomamente por botnets y otros factores, además de las APT (Amenazas persistentes avanzadas) con sofisticados ataques dirigidos contra el usuario y la infraestructura, sin embargo, para [5], los problemas más importante se encuentran en la escasez de seguridad de la información, esto conduce necesariamente al acceso no autorizado a la red o a los distintos dispositivos, en el proceso de transmisión de datos y la encriptación de los mismos que puede desatar amenazas considerables en la mayoría para los usuarios que utilizan.

La noción de IoT se considera indefinidamente nueva; sus inicios datan ciertamente entre 2008 y el 2009, donde fue definido por CISCO Grupo de Soluciones Empresariales de Internet (IBSG) como la era en que la cantidad de objetos inertes estaban conectados a una red a una cantidad exorbitante sobrepasando a la cantidad de usuarios conectados [6]. Para [7] la elevada popularidad de la tecnología IoT se ve posibilitada por los objetos físicos que se conectan a internet por medio de distintos métodos o tecnologías inalámbricas clasificándose por el alcance corto y largo en las cuales se encuentran ZigBee, RFID, redes de sensores y tecnologías basadas en localización.

A la elevada cantidad de capacidades que brinda IoT, muchas entidades han resuelto problemáticas con soluciones innovadoras en el mercado, a su vez como resultado se han creado infraestructura de control y administración de IoT, pero no garantiza la posibilidad de tener vulnerabilidades causadas por su diseño, [8]. Según [9] el riesgo que más resalta son las brechas de seguridad, el robo y alteración de la información sensible o confidencial; por consiguiente, se requiere nueva metodología para mitigar o minimizar estos fallos. Las innovadoras tecnologías representan una cantidad grande de posibles aplicaciones debido a la capacidad dentro de IoT para capturar, procesar y transmitir información, aun cuando existe un porcentaje alto de ventajas para Tecnologías de IoT, la seguridad a nivel de dispositivo es un margen

primordial especialmente para las redes inalámbricas [10].

El aspecto más importante a considerarse en el IoT es la seguridad. Según un estudio realizado por un investigador de ISM en 2016, un gran porcentaje de los dispositivos IoT tienen problemas de privacidad, lo que los hace vulnerables a la piratería a través de redes de radiofrecuencia o IP, y es relativamente fácil clonar y administrar dispositivos de forma remota, generando así pérdidas económicas fuertes como por ejemplo las desventajas en el transporte privado y público; modificando rutas por fines antisociales, en el área de la salud, alterando los resultados, causando fallas en casos clínicos de suma importancia, por todo esto, los usuarios regresan a herramientas más antiguas que brindan mayor confiabilidad dejando de lado la innovación y la tecnología [11].

La falta de conocimiento e interés en el tema de vulnerabilidades son las principales causas para abordar el tema de estudio propuesto. El objetivo principal del desarrollo del estudio es dar a conocer a los lectores el análisis de las diferentes vulnerabilidades de dispositivos IoT, ya que en el laboratorio se realizan investigaciones y pruebas sobre seguridades de dispositivos de comunicación y esta investigación contribuirá de mejor manera al hallazgo de vulnerabilidades en dispositivos IoT.

El presente trabajo está organizado con la introducción, Materiales y métodos, Resultados y Discusión y finalmente las conclusiones.

II. Materiales y Métodos

A. Materiales

En el siguiente apartado, se muestran las herramientas utilizadas tanto en hardware como en software.

1) Hadware:

- 2 Lora TTGO ESP32
- 3 sensores DHT11
- 3 sensores MQ2
- 3 sensores PIR
- 2 Bluetooth BLE
- 1 ESP8266
- 2 ARDUINOS UNO
- CatWAN USB Stick LoRa y LoRaWAN 915Mhz
- Sniffer nRF52840

2) Software:

- IDE de Arduino
- PuTTY
- Wireshark
- Python
- EtterCap
- WiFislax

B. Metodología

En el siguiente apartado, se muestran los procedimientos que se siguieron para la presente investigación.

1) Escenario 1. Red con módulo bluetooth HC-05 (WPAN): En la figura 1, se evidencia un diagrama lógico del módulo Bluetooth HC-05 implementada en una red, se conectó un módulo Bluetooth que es el encargado de receptar los datos de los sensores, conectado así al otro modulo Bluetooth de un dispositivo telefónico que funciona como gateway transportando así los datos de los sensores a la plataforma.

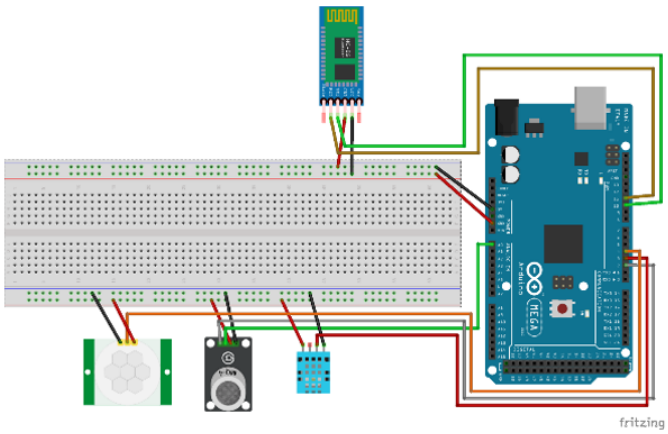


Fig. 1: Diagrama lógico del HC-05.

En la figura 2, se considera la conexión de la plataforma, se necesita la librería *(Blynk print Serial)*, y algunos datos que proporciona la plataforma que es una clave de acceso y la conexión respectivamente para enlazar según [12] .

```
#define BLYNK_PRINT Serial
char auth[] = "fLMWJmDM0OwtVRu9Km70e7zIedY7W_NF";
#include <BlynkSimpleSerialBLE.h>
#include <SoftwareSerial.h>
SoftwareSerial SerialBLE(10, 11);
```

Fig. 2: Código para comunicación del HC-05 y plataforma Blynk

2) Escenario 2. Red con ESP8266 (WLAN): La tecnología de comunicación Wi-Fi y la plataforma como servidor, todos los sensores están conectados a través de una red entre el nodeMCU y el Router inalámbrico que es la puerta de enlace. En la figura 3, se evidencia un diagrama lógico del ESP8266 implementada en una red WLAN representada por tres distintos sensores que representan varios entornos donde se pueden implementar, a través del código C++ del IDE de Arduino para manejar el SoC.

En la figura 4, se presenta las líneas de código para la conexión con la plataforma, se necesita la librería ThingSpeak.h, y algunos datos que proporciona la plataforma como es el APIKey, el canal ID, el nombre de usuario y la contraseña según [13] .

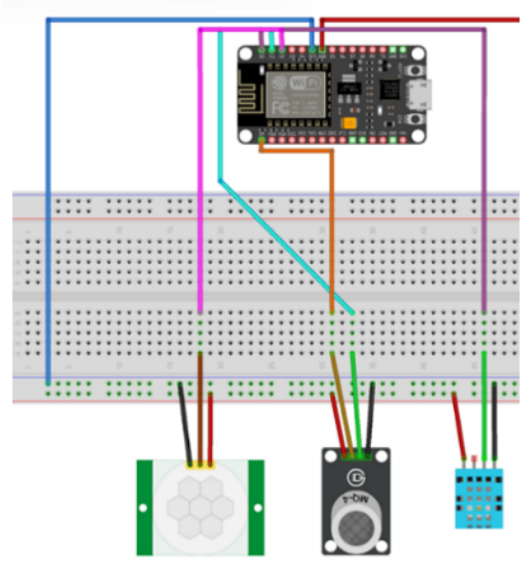


Fig. 3: Diagrama lógico de ESP8266.

```
#include "ThingSpeak.h"
unsigned long channelID = 1641087;
const char* WriteAPIKey = "81OFWLU3JPQ07IIU";
const char* ssid = "NETLIFE- CBaez";
const char* password = "sjh1708944549";
```

Fig. 4: Código para comunicación del ESP8266 al ThingSpeak.

3) Escenario 3. WWAN Red con módulos LoraWan: En la figura 5 , se puede evidenciar un diagrama lógico del módulo Lora TTGO que es el encargado de receptar los datos de los sensores, conectado así al otro modulo Lora TTGO que funciona como gateway transportando así los datos de los sensores a la plataforma.

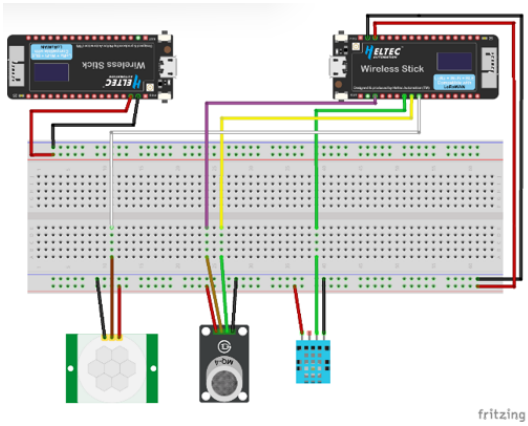


Fig. 5: Diagrama lógico de Lora TTGO.

Para conectarse a la plataforma, se basó en [14] y la librería de Lora TTGO (LoRa.h), y ciertos datos como nombre de usuario, nombre de dispositivo y credenciales, ver figura 6.

```
//Conexion con Thinger
#include <ThingerESP32.h>

#define USERNAME "majojacome"
#define DEVICE_ID "ESP32_Lora"
#define DEVICE_CREDENTIAL "k%04E#bBVIeH36SK"

#define SSID "Majito"
#define SSID_PASSWORD "majo1997"

ThingerESP32 thing(USERNAME, DEVICE_ID, DEVICE_CREDENTIAL);
```

Fig. 6: Código para comunicación del Lora al Thinger.io.

C. Implementación

En este proyecto, existen tres escenarios, cada escenario contiene 3 sensores conectados respetivamente a los dispositivos de los módulos, que son los receptores de cada uno de los enlaces creados. En cada uno de los enlaces se envía un bloque de Strings de los valores de cada uno de los sensores respectivamente (Temperatura, humedad, gas y movimiento), finalmente se procede a utilizar hardware externo, y sus respectivos controladores y con wireshark se husmeará los paquetes transmitidos para verificar si tiene o no vulnerabilidades previo ataques, dependiendo de las tecnologías de red en prueba.

1) Implementación del Sniffer : La configuración usada en la investigación fue implementada en 3 escenarios (WLAN, WWAN, y WPAN) como se muestra en la figura 7 . Donde hay una típica red entre un nodo, Gateway y el sniffer, la información transmitida entre el nodo y el Gateway es vista por el sniffer colocada dentro de la misma red, que se basó en [8].

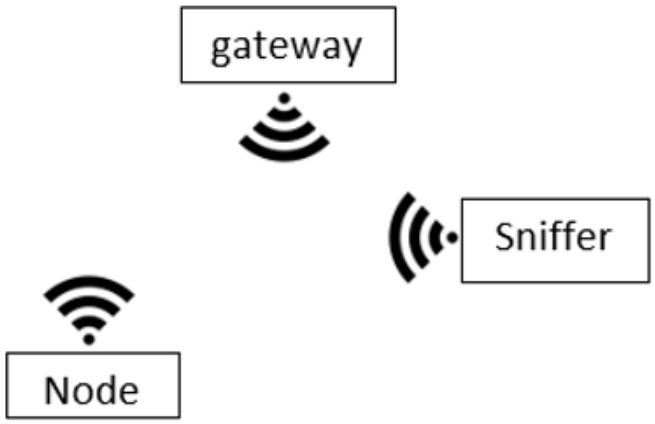


Fig. 7: Configuración de los escenarios con Sniffer.

III. Resultados y Discusión

A. Herramientas y monitorización de datos y capturas de tráfico de datos.

1) Wireshark como monitorización de tráfico de datos : Wireshark es un analizador de tráfico de datos en tiempo real,

y desde esa monitorización se puede observar la transmisión de Lora TTGO a Lora TTGO la cual se realizó ataques para hallar vulnerabilidades de la información enviada en tiempo real y de esta manera se analizó si los datos se transmiten cifrados o no, esto es según [15].

En la Figura, 8 se muestra la aplicación Wireshark en acción.

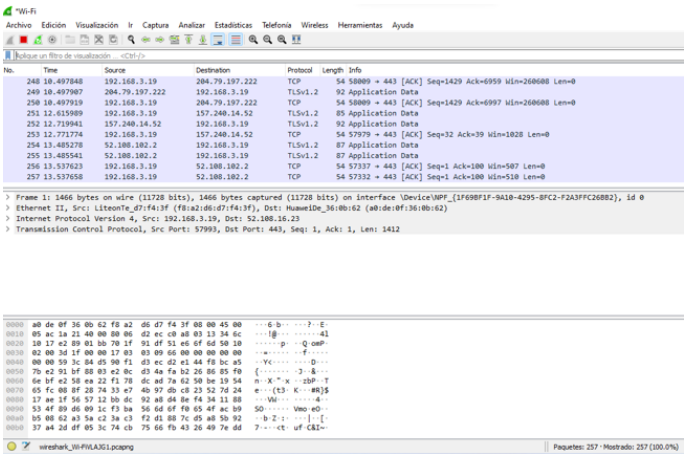


Fig. 8: Análisis de tráfico de datos.

2) WiFislax - Ettercap : El Ettercap se utilizó para el ataque ARP, el objetivo es establecer la puerta de enlace predeterminada del equipo y la dirección IP del equipo atacante, esto es según [16].

De esta manera el equipo atacante estará situada entre el router, tratando así de escuchar todo el tráfico de la red que genera el objetivo. En la figura 9 , se muestra la aplicación Ettercap en donde se ha seleccionado la ip del Gataway y la ip que le ha asignado el router al ESP8266. [17]

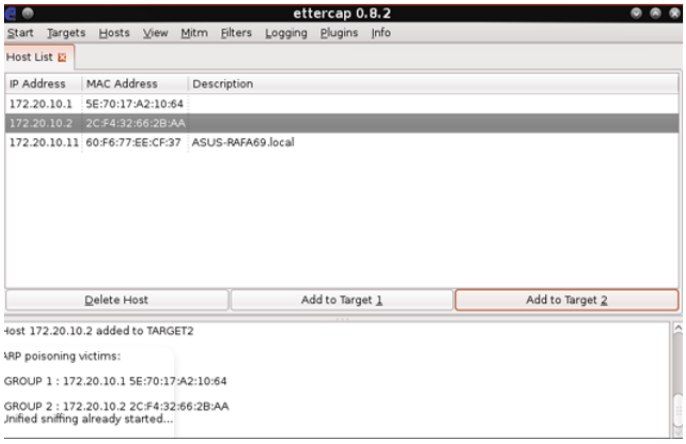


Fig. 9: Captura Ettercap de las direcciones ip asignadas.

3) Conexión 1: Bluetooth con la plataforma Blink : En la figura 10, se muestra el diagrama físico acerca de la estructura de los sensores y la obtención de datos en base a las secciones de código restructuradas mediante [18] [19] [20]. En la figura 11, se evidencia el envío de datos de los sensores al servidor Blynk

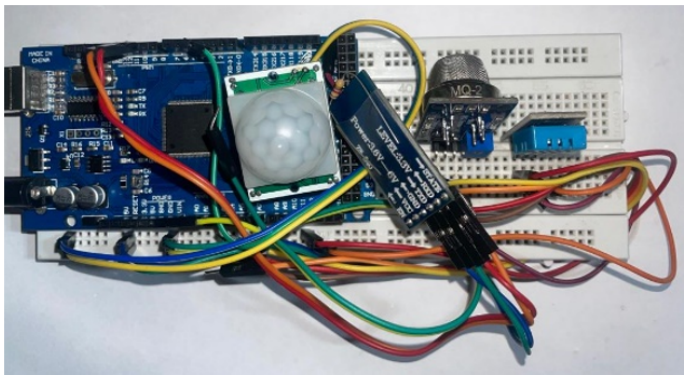


Fig. 10: Diagrama físico del Bluetooth.

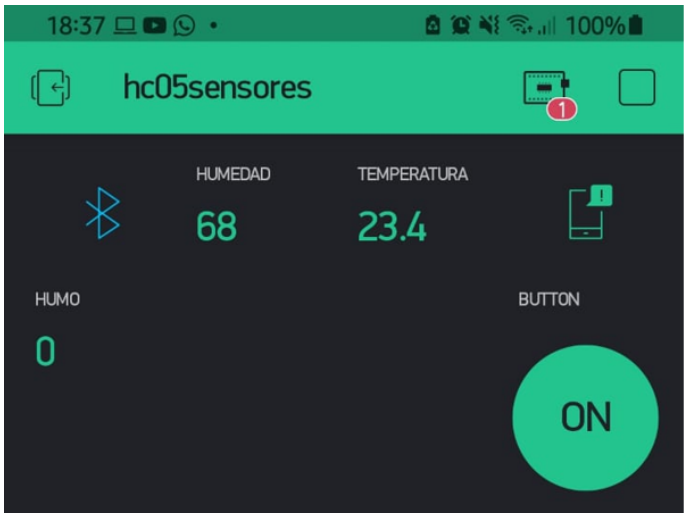


Fig. 11: Informacion de datos de los sensores en Blynk.

4) Conexión 2: ESP8266 con la plataforma ThingSpeak : En la figura 12, se muestra el diagrama físico acerca de la estructura de los sensores y la obtención de datos se basó en [21] [22].

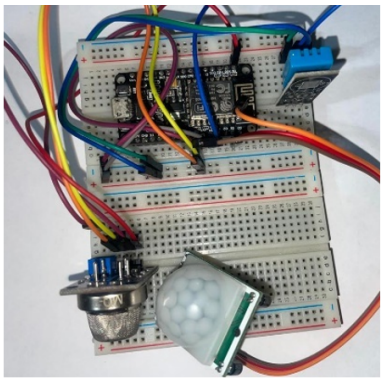


Fig. 12: Diagrama físico de ESP8266

En la figura 13, se puede evidenciar la obtención de los datos que envían los sensores al dashboard de ThingSpeak en tiempo real.

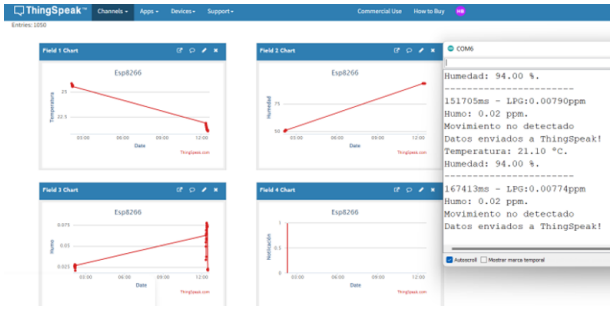


Fig. 13: Información de datos de los sensores en ThinkSpeak

5) Conexión 3: Lora TTGO con la plataforma Thinger.io : En la figura 14 , se muestra el diagrama físico de los sensores y la obtención de datos, aunque en pantalla se muestre solo los datos de temperatura y humedad, los otros datos de los sensores se basaron en [23] [24] [25] y se muestran en la plataforma de Thinger.io.

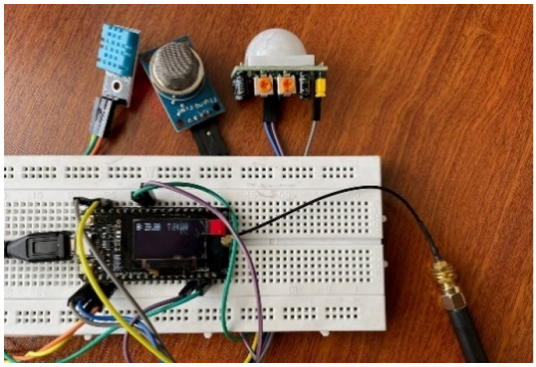


Fig. 14: Diagrama físico de Lora TTGO

En la 15, según [26] es el código de un String el cual abarca todos los datos de los sensores, mientras que en la figura 16, se puede evidenciar la obtención de los datos en el dashboard de Thinger.io en tiempo real.

[23] [24] [25] y se muestran en la plataforma de Thinger.io.

```
String LoRaMessage = String(h) + "&" + String(t)+ "&" + String(movim)+
"&" + String(gassensorAnalog)+ "&" + String(gassensorDigital) ;
```

Fig. 15: Vector de String que abarca los datos de los sensores

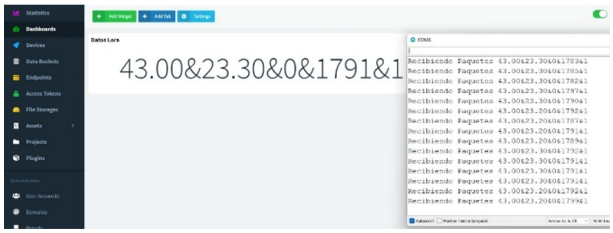


Fig. 16: Información de datos de los sensores en Thinger.io

6) Ataque a la Conexión HC-O5: En la figura 17 , se puede evidenciar datos capturados con la herramienta de Wireshark, que son simplemente las ondas de radios emanadas del módulo hc-05 a la plataforma Blynk, la cual se visualiza con una encriptación en hexadecimal, la configuración se basó mediante [26].

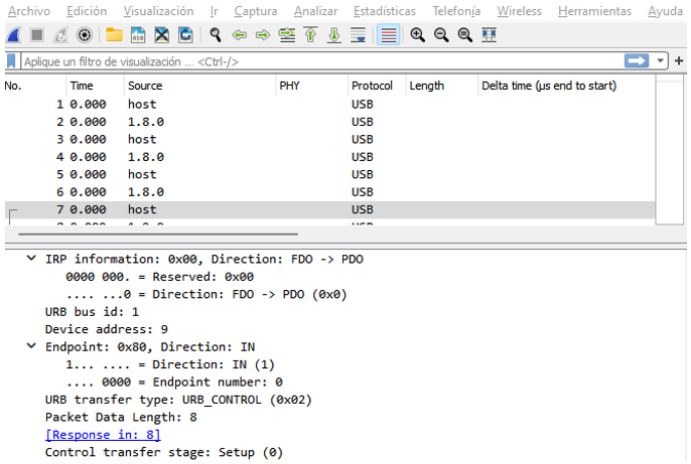


Fig. 17: Datos capturados y visualizados en wireshark.

En la figura 18, se puede observar mediante Wireshark la informacion detallada del nodo al momento del envío del mensaje a la plataforma y es capturado por el sniffer.

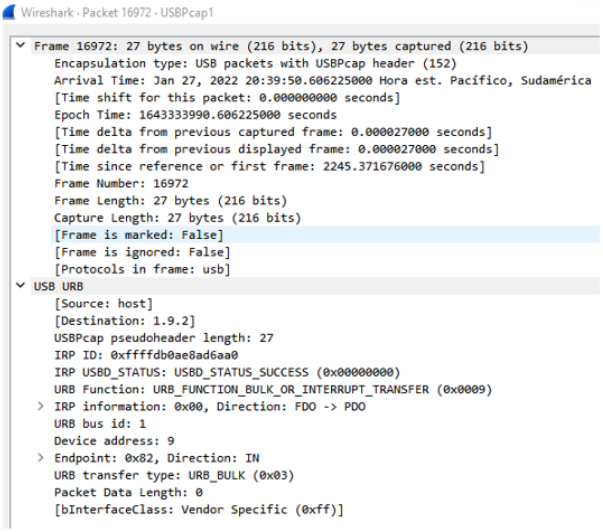


Fig. 18: Datos visualizados y capturados en wireshark con el sniffer.

7) Ataque a la Conexión ESP8266: En la figura 19 , se evidencia los datos capturados en la conexión del ESP8266 con el Router inalámbrico donde se puede visualizar el ataque poisoning desde Ettercap que envia paquetes ARP, DNS y HTML, todo eso se basó mediante [27].

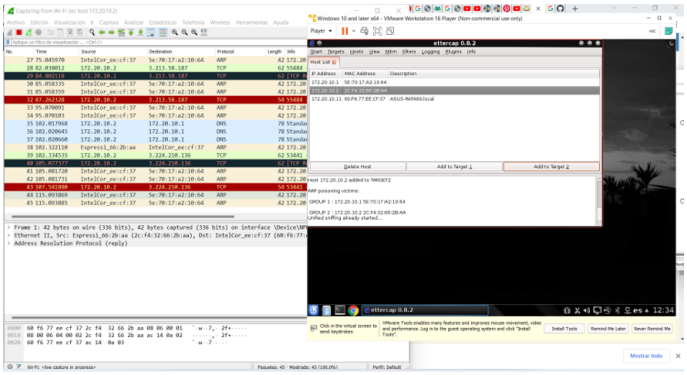


Fig. 19: Lista de Paquetes dentro del analizador.

En la figura 20 , se puede evidenciar que el mensaje capturado se envía a través de otro protocolo al analizador de tráfico, los datos que muestra Wireshark tienen más información que los datos que muestra directamente el ESP8266. Como resultado, se agregan ciertas cabeceras antes de que se muestren los datos capturados.

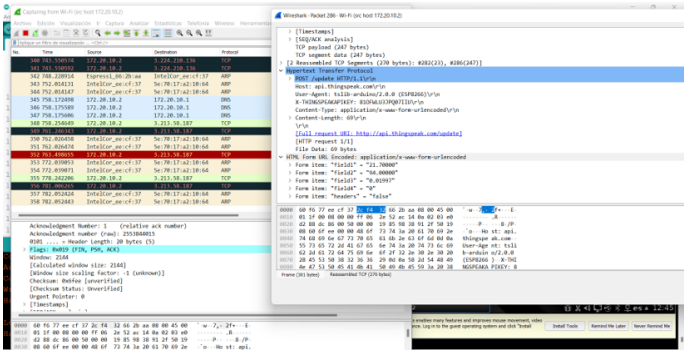


Fig. 20: Lista de Paquetes dentro del analizador.

8) Ataque a la Conexión Lora TTGO: En la figura 21 , según [8] , se evidencia los datos capturados en formato hexadecimal (aún sin cifrar) que pertenecen a los nodos, que se pueden ver en el área resaltada de verde, mientras que los datos capturados en formato hexadecimal (aún sin cifrar) se pueden ver en la sección inferior, que se organiza en bloques que se envían a un frame.

Se puede evidenciar que los datos mostrados en la figura 22, se basa en el mensaje capturado y enviado a través de otro protocolo al analizador de tráfico, con esto Wireshark tiene simplemente información sobre la trama LoRa y ciertas cabeceras que se agregan antes de que se muestren los datos capturados en sí.

En la figura 23, se observa la información recibida por wireshark cuando un nodo envía un mensaje y es capturado por el sniffer en forma más detallada.

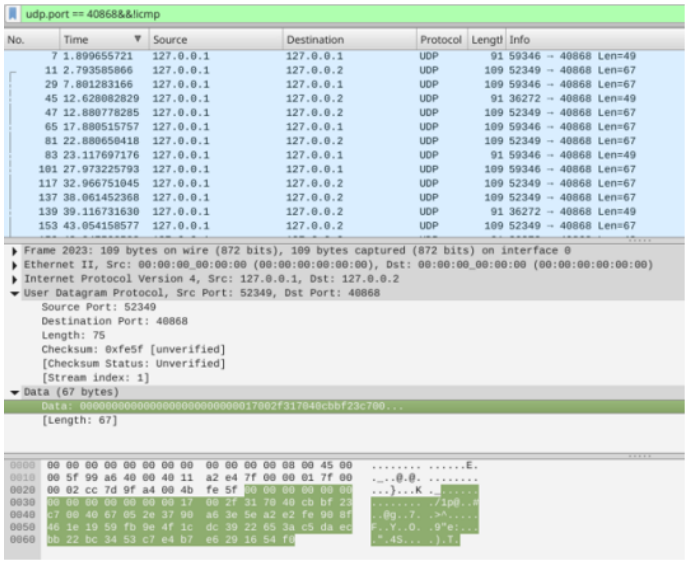


Fig. 21: Datos capturados visualizados en wireshark.

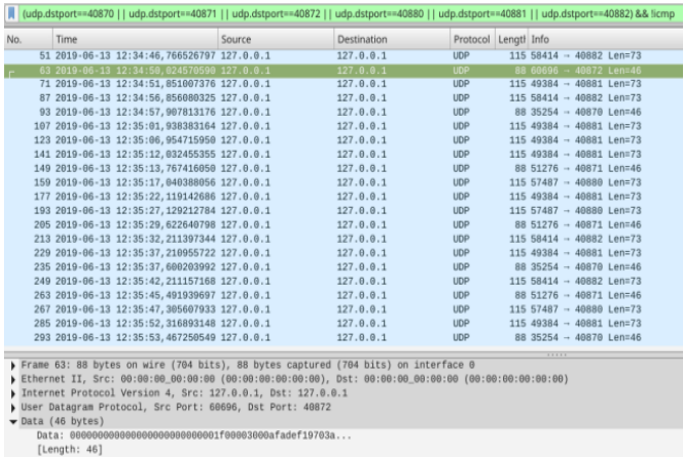


Fig. 22: Datos capturados y visualizados en wireshark

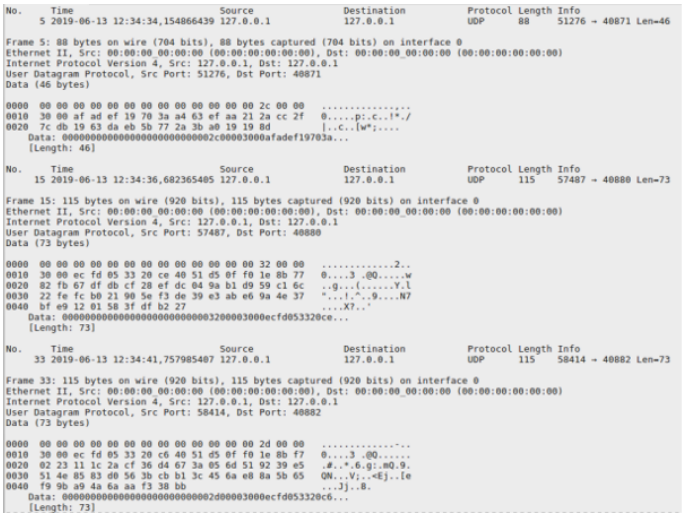


Fig. 23: Datos visualizados y capturados en wireshark con el sniffer.

B. DISCUSIÓN

Como se puede observar en los 3 escenarios, de las redes respectivamente atacadas, en el único escenario donde se halló vulnerabilidades fue en la red WLAN con la plataforma ThingSpeak donde se puede evidenciar el tráfico de datos planos sin cifrar de los sensores (DHT11, PIR, MQ2), estos datos fueron encontrados en los protocolos HTML. El escenario más seguro fue WWAN puesto que mediante el sniffer se observó paquetes fuertemente cifrados, según [28], se utiliza algoritmos AES para proporcionar autenticación e integridad de paquetes al servidor de red y cifrado de extremo a extremo al servidor de aplicaciones, tanto WWAN Y WPAN presentan cifrado en sus transmisiones, por ende, no se puede evidenciar sus datos mediante el sniffer tan solo de sus tramas de envió de datos.

IV. CONCLUSIONES

Con el sniffer implementando, fue posible capturar el proceso de transmisión de datos, identificando cada segmento de la trama LoRaWaN donde está fuertemente cifrado los datos. Como resultado, solo fue posible determinar la dirección del dispositivo de recepción de datos, demostrando que la transmisión de datos es la más segura posible.

Se demostró que hay la vulnerabilidad evidente en la conexión con la plataforma ThingSpeak, en la cual se captura los datos planos generados por los sensores en el protocolo HTML como se visualizó anteriormente en las graficas 19 y 20, su seguridad es ineficiente en la transmisión de datos en la cual se visualiza paquetes ARP y TCP.

En el escenario del módulo bluetooth no se visualizó vulnerabilidad, m en la conexión con la plataforma Blynk porque en base a los gráficos 17 y 18, la trama es enviada en codificación hexadecimal, por lo tanto, no se tuvo captura de los datos transmitidos y a su vez la plataforma Blynk maneja paquetes TCP en su recepción de datos se considera que el sniffer utilizado no pudo descifrar la codificación.

REFERENCES

[1] C. L. Rose Karen, Eldridge Scott, "La internet de las cosas una breve reseÑa," vol. 1, p. 83, 2015.

[2] "Cómo reducir la inseguridad en iot y las vulnerabilidades sin morir en el intento." [Online]. Available: https:https://es.linkedin.com/pulse/c%C3%B3mo-reducir-la-inseguridad-en-iot-y-las-sin-morir-el-zambrana

[3] L. J. Roman Rodrigo, Najera Pablo, "Securing the internet of things," *University of Malaga*, 2011.

[4] S. J. Cui Ang, "Reflections on the engineering and operation of a large-scale," *Department of Computer Science*, 2011.

[5] V. N. D. S. C. J. E. P. A. G. R. M. C. J. M. Q. L. C. M. M. A. Romero Castro Martha Irene, Figueroa Moran Grace Liliana, "IntroducciÓn a la seguridad informÁtica y el anÁlisis de vulnerabilidades," *Área de Innovación y Desarrollo*, 2018.

[6] "Un poco de historia sobre internet de las cosas." [Online]. Available: https://www.sorayapaniagua.com/2012/04/15/un-poco-de-historia-sobre-internet-de-las-cosas/

[7] "The internet of things how the next evolution of the internet is changing everything." [Online]. Available: https://www.slideshare.net/marklittlewood/io-t-cisco-definition

[8] G. G. E. E. Bravo Montoya Andrés F., Rondón Sanabria Jefersson S., "Desarrollo y prueba de un sniffer en tiempo real de una red lorawan usando gnu-radio," *TecnoLogicas*, p. 10, 2019.

[9] L. P. P. D. Aras Emekcan, Ramachandran Gowri Sankar, "Exploring the security vulnerabilities of lora," *IEEE International Conference on Cybernetics (CYBCON)*, p. 6, 2017.

[10] C. L. Rose Karen, Eldridge Scott, "La internet de las cosas una breve reseÑa," vol. 1, p. 83, 2015.

[11] V. C. M. Santiago, "Hacking Ético al iot mediante sdr," p. 144, 2018.

[12] "Blynk iot platform,vshymanskyy." [Online]. Available: https://github.com/blynkkk/blynk-library

[13] "Esp8266 nodemcu publish sensor readings to thingspeak (easiest way)." [Online]. Available: https://randomnerdtutorials.com/esp8266-nodemcu-thingspeak-publish-arduino/

[14] "Espressif esp32." [Online]. Available: https://docs.thinger.io/arduino/espressif-esp32

[15] "Aprende cómo utilizar wireshark para capturar y analizar el tráfico de red." [Online]. Available: https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/

[16] "Capturar credenciales." [Online]. Available: https://mundo-hackers.weebly.com/capturar-credenciales.html

[17] "Aprende todo sobre el ataque arp poisoning y protégete." [Online]. Available: https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/

[18] "Esp8266-01 pir and dht on thingspeak." [Online]. Available: https://www.hackster.io/mamic/esp8266-01-pir-and-dht-on-thingspeak-687c75

[19] "Gas level monitor on internet using esp8266 gas sensor." [Online]. Available: https://how2electronics.com/gas-level-monitor-esp8266-gas-sensor/

[20] "Dht11 humidity sensor with esp8266 and thingspeak." [Online]. Available: https://www.electronicshub.org/dht11-humidity-sensor-with-esp8266/

[21] "Mq2 gas measurement." [Online]. Available: https://community.blynk.cc/t/mq2-gas-measurement/32387

[22] "Nodemcu esp8266 + pir + blynk." [Online]. Available: https://www.instructables.com/Nodemcu-Esp8266-PIR-Blynk/

[23] "Tutorial sensores de gas mq2, mq3, mq7 y mq135." [Online]. Available: https://naylampmechatronics.com/blog/42_tutorial-sensores-de-gas-mq2-mq3-mq7-y-mq135.html

[24] "Lorawan – sensor humedad y temperatura. gateway y broker." [Online]. Available: http://blog.espol.edu.ec/girni/category/dispositivos-lora/lorawan-humedad-y-temperatura/

[25] "Esp32 with pir motion sensor using interrupts and timers." [Online]. Available: https://randomnerdtutorials.com/esp32-pir-motion-sensor-interrupts-timers/

[26] "How to install ble sniffer on nrf52840 dongle and run it." [Online]. Available: https://jimmywongiot.com/2020/07/08/how-to-install-nrf-sniffer-through-nrf52-dk-board/

[27] "Aprende todo sobre el ataque arp poisoning y protégete." [Online]. Available: https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/

[28] "What is lorawan® specification." [Online]. Available: https://lora-alliance.org/about-lorawan/