UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

ANALISIS COMPARATIVO DE LA PRIVACIDAD DE LOS DATOS EXCLUSIVAMENTE EN LA TRANSMISION HACIA LAS PLATAFORMAS DE IOT MÁS UTILIZADAS

Trabajo de titulación previo a la obtención del
Título de Ingeniera de Sistemas

AUTORA: Chango Tonato Jenny Gabriela

TUTOR: Manuel Rafael Jaya Duche

Quito- Ecuador,

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Chango Tonato Jenny Gabriela con documento de identificación N° 1717830705; manifiesto que:

Soy la autora y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir y publicar de manera total o parcial el presente trabajo de titulación.

Quito, 08 de marzo de 2022

Atentamente,

Chango Tonato Jenny Gabriela
1717830705

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

Yo, Chango Tonato Jenny Gabriela con documento de identificación N. 1717830705, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del Artículo Académico: "Análisis Comparativo de la Privacidad de los Datos Exclusivamente en la Transmisión Hacia las Plataformas de IOT más Utilizadas", el cual ha sido desarrollado para optar por el título de: Ingeniera de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedido anteriormente.

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

Quito, 08 de marzo de 2022

Atentamente,

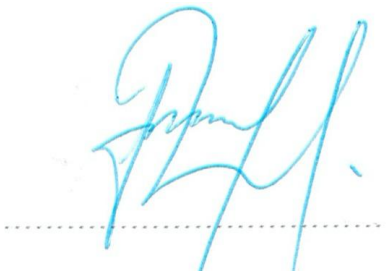
Chango Tonato Jenny Gabriela
1717830705

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Manuel Rafael Jaya Duche con documento de identificación N° 1710631035, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANALISIS COMPARATIVO DE LA PRIVACIDAD DE LOS DATOS EXCLUSIVAMENTE EN LA TRANSMISION HACIA LAS PLATAFORMAS DE IOT MÁS UTILIZADAS, realizado por Jenny Gabriela Chango Tonato con documento de identificación N° 1717830705, obteniendo como resultado final el trabajo de titulación bajo la opción Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 08 de marzo de 2022

Atentamente,



Ing. Manuel Rafael Jaya Duche, Mgtr
1710631035

DEDICATORIA

Dedico este trabajo a la vida, a mi familia y amigos ya que ellos siempre han estado a mi lado en tiempos buenos y malos y gracias a una segunda oportunidad de vivir estoy terminando este artículo a pesar de todas las cosas que han pasado.

Siempre hay algo bonito que viene solo debemos esperar y construirlo poco a poco.

Jenny Gabriela Chango Tonato

AGRADECIMIENTO

Agradezco a mi profesor de tesis por toda la paciencia empleada en el desarrollo de este artículo que a pesar de todos los obstáculos siempre estuvo ahí pendiente de la evolución del mismo, a la Universidad Politécnica Salesiana, institución que nos aportó conocimientos en mi formación personal y académica, a un amigo muy especial que sin su ayuda nunca hubiese podido ingresar a terminar la carrera que siempre quise, a mi madre y mi tío por la paciencia y el soporte y sobre todo a mi hija por ser el motivo de todo.

Jenny Gabriela Chango Tonato

ANALISIS COMPARATIVO DE LA SEGURIDAD DE LOS DATOS AL TRASMITIRSE HACIA PLATAFORMAS IOT.

COMPARATIVE ANALYSIS OF DATA SECURITY WHEN TRASMITTED TO IOT PLATAFORMS.

(Gabriela Chango 1, Rafael Jaya 2)

Resumen

La presente investigación tiene por objetivo la comparación de las seguridades de los datos transmitidos desde dispositivos IoT como el ESP32 hasta las distintas plataformas como Blynk, Firebase, Thinger.io y ThingSpeak.
Para este propósito, se utilizaron herramientas de software como EtterCap de WiFislax para realizar los ataques y Wireshark para capturar el tráfico simultáneamente al realizar los ataques a cada una de las conexiones desde el hardware ESP32 con sus respectivos sensores de temperatura y humedad DHT22, se efectuaron los ataques entre el ESP32 y el router inalámbrico.
Se tuvo como resultados que la conexión más segura es la de los dispositivos conectados a Firebase y la que presenta vulnerabilidades fue la conexión hacia ThingSpeak.
En conclusión, de la investigación arroja que la conexión más segura hacia las 4 plataformas es Firebase y la más insegura fue la de ThingSpeak.

Palabras clave: Seguridad, Hacking ético, EtterCap, Saas, IoT, Confiabilidad, Integridad, WiFislax, Wireshark, ESP32.

Abstract

The present research aims to compare the security of data transmitted from IoT devices such as ESP32 to different platforms such as Blynk, Firebase, Thinger.io and ThingSpeak.
For this purpose, software tools such as EtterCap from WiFislax were used to carry out the attacks and Wireshark to capture the traffic simultaneously when carrying out the attacks on each of the connections from the ESP32 hardware with their respective DHT22 temperature and humidity sensors. Attacks between the ESP32 and the wireless router.
The results were that the most secure connection is that of the devices to Firebase and the one that presents vulnerabilities was the connection to ThingSpeak.
In conclusion, the research shows that the most secure connection to the 4 platforms is Firebase and the most insecure was that of ThingSpeak.

Keywords: Segura, Hacking ético, Protocolo de comunicación, Saas, IoT, Confiabilidad, Departamento TI, ESP32

[1] Estudiante de Ingeniería en Sistemas Mención Gestión – Universidad Politécnica Salesiana, Egresado – UPS – **sede** Quito. Autor para correspondencia: jchangot1@est.ups.edu.ec.
2 Docente de la Carrera de Ingeniería en Sistemas y Ciencias de la Computación – Universidad Politécnica Salesiana, Magister – UPS – **sede** Quito. Autor para correspondencia: mjaya@est.ups.edu.ec.

1. Introducción

Dentro de la evolución de la tecnología se puede observar una rama denominada seguridad de los datos sobre los dispositivos conectados, cuyas reglas deben ser estrictas para resistir ataques cibernéticos y así garantizar la transparencia, privacidad y protección de la información. "Encontrar las vulnerabilidades en las redes de dispositivos IoT y analizar los mecanismos existentes en ambientes IoT, permitirá identificar un mecanismo de seguridad adecuado y el que mitigue de mejor manera la inseguridad y el uso malicioso de información" ayudando a los desarrolladores a mitigar los posibles futuros fallos en la seguridad de las plataformas [1].

Las plataformas IOT son "Un conjunto de servicios computacionales que administra la operación de los dispositivos remotos, gestiona las comunicaciones y mecanismos de seguridad, procesa los datos obtenidos y remite la información a múltiples aplicaciones o servicios computacionales" [2]. Estos son gestionados con normas de seguridad dentro de sus frameworks, "Garantizar seguridad y privacidad de los datos generados por el internet de las cosas es un reto a los que deben apuntar las personas que generan soluciones de seguridad" [2], para lo cual el análisis de referente a la seguridad plataformas más utilizadas es información valiosa para los usuarios nuevos y sus datos.

Por otro lado, el que una plataforma de este tipo despliegue inseguridades puede causar un gran impacto social y hará que los usuarios desconfíen de la seguridad que van a tener sus datos ya que el framework encargado de este no es lo suficientemente confiable, esto solo es comprobable realizando ataques cibernéticos sobre las plataformas utilizadas en el análisis de transmisión de datos como Blink, Thinger.io, Firebase y ThingSpeak, como referencia, se usarán estándares de seguridad Nist, Sans e ISO 27000.

Así mismo, "La disponibilidad es una de las características más importantes para los usuarios de sistemas IoT" [2]. Dentro de la disponibilidad de los datos se debe temer e cuenta que estos mismos no pueden ser alterados y robados.

Según, El concepto de M2M "Machine To Machine hace referencia al intercambio de información o comunicación ya sea inalámbrica o cableada, de datos entre dos máquinas remotas. Este intercambio se realiza de manera telemática utilizando ya sea redes privadas, comunicaciones sin hilos y otros sistemas que permiten la comunicación entre las máquinas" [3].

Para [4], "El problema primario de seguridad con la tecnología M2M es que los dispositivos están escuchando, y por lo tanto, son susceptibles de ataque", comentó Tom Sharon, director de tecnología de Clear2there, un proveedor de conectividad M2M con sede en Oklahoma City. Ahora tiene un puerto abierto. Tiene una vulnerabilidad. Los dispositivos no pueden realmente estar seguros de quién está tratando de hablar con ellos y controlarlos".

En resumen, existe la ciberseguridad para controlar estos sucesos, pero, la superficie de exposición es cada vez más grande, las amenazas mayores y más sofisticados en los desafíos de forma digital.

Durante los últimos años en el mundo se ha tenido cambios y avances en relación a las personas y la tecnología por lo que se afirma que [5], "la pandemia ha acelerados los procesos de transformación digital en las compañías". Y se puede estar seguro que no solo en compañías, también sobre nuevos emprendimientos, así como en la educación.

Así como la sociedad no ha tenido una relación muy cercana con la tecnología desconocen de ciertos detalles que involucran parte de la seguridad y uno de estos es que no "solo generan elevados costos económicos, sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas" [6], para evitar está perdida de confianza es que

se hacen pruebas y ataques para de esta manera brindarle confianza al usuario y seguridad a sus datos.

La presente investigación propone comparar las seguridades que poseen en cuanto a la transmisión de datos las diferentes plataformas de IoT, las aplicaciones son software capaz de conectar todo en un *sistema IoT como, por ejemplo: Hardware, Conectividad, Software, interfaz de usuario y a toda esta conexión se le puede dar el nombre de Cadena de Valor de IoT, así, para* [7]*, "E*l alcance total de la IoT no está definido con precisión; sin embargo, es evidentemente que cada sector tiene sus propios tipos de dispositivos de IoT"

Como se recalcó anteriormente un análisis comparativo de seguridad sobre plataformas IoT, tendrá como objetivo principal ayudar a los desarrolladores a mitigar posibles fallos en seguridad que pueden ocurrir dentro de la trasmisión de datos de dispositivos finales IoT y las posibles plataformas, para esto, se armarán escenarios de prueba con el SoC ESP32, el cual estará conectado a sensores como temperatura y humedad (DHT22), sobre este conjunto de hardware, se llevará a cabo ataques he intrusiones con EtterCap, tratando de vulnerar su seguridad, con Wireshark, se capturarán datos que serán analizados y documentados, identificando las posibles vulnerabilidades a las que están expuestas estas plataformas con respecto a los dispositivos conectados..

2. Materiales y Metodos

En esta sección, se da a conocer los materiales que se utilizó para las diferentes pruebas así como los métodos usados en cada escenario.

2.1. Materiales

Para realizar los escenarios de pruebas y así observar las debilidades de los frameworks de seguridad que manejan las plataformas se necesitarán materiales tanto en hardware como en software, así se tiene:

2.1.1. Hardware

- DHT22 (Sensor de humedad y temperatura)
- ESP32
- Router inalámbrico

2.1.2. Software

- Wireshark
- WiFislax
- EtterCap

2.2. Metodos

Se armó una red entre un ESP32 y el sensor DHT22, la maquina atacante, la máquina que captura el tráfico conectados al router inalámbrico por donde sale hacia la red y se conecta con las diferentes plataformas [11], una vez armada esta red, se procedió a realizar las respectivas pruebas sobre 4 escenarios, luego, se realizaron ataques de ARP Poisoning con EtterCap cuando se esté enviando información desde el ESP32 hasta las plataformas y al mismo tiempo, se estuvo monitorizando y capturando tráfico con el Wireshark para analizar las posibles vulnerabilidades.

Obviamente para realizar las pruebas con cada uno de estos escenarios, se tuvo que configurar y programar al ESP32 para que se conecte con cada una de las plataformas como se muestra a continuación.

2.2.1. Conexión ESP32 con las plataformas

Se requiere programar al dispositivo ESP32 a conectarse usando parámetros como como nombre de usuario, nombre de dispositivo y una credencial o generación de token, también, se procede a la instalación de librerías de acuerdo a la plataforma que se va a analizar, como se muestra en la en la figura 1 que corresponden a la conexión para Thinger.io.

```
#define USERNAME "GabyCh"
#define DEVICE_ID "Esp32Gaby"
#define DEVICE_CREDENTIAL "JDuHB#nD0ptTAAQK"
```

Figura 1. Código para comunicación del ESP32 al Thinger.io.

2.2.2 Conexión del ESP32 al Router inalámbrico.

Como se puede observar en la figura 2, para dicha conexión se requieren el nombre de la red inalámbrica, su contraseña y en la figura 3, se envían estos parámetros con métodos en este casi thing.add_wifi () y también se necesita la IP que le asigna por DHCP el router para con este dato atacar al enlace ESP32- Gateway (router) con el EtterCap.

```
#define SSID "BITCH."
#define SSID_PASSWORD "Estrellita.2021"
```

Figura 2. Captura credenciales Wifi.

```
// add WiFi credentials
thing.add_wifi(SSID, SSID_PASSWORD);
Serial.println(WiFi.localIP());
```

Figura 3. Captura método para impresión IP con credenciales wifi.

En la figura 4, se muestra el circuito armado del ESP32 con el sensor DHT22.

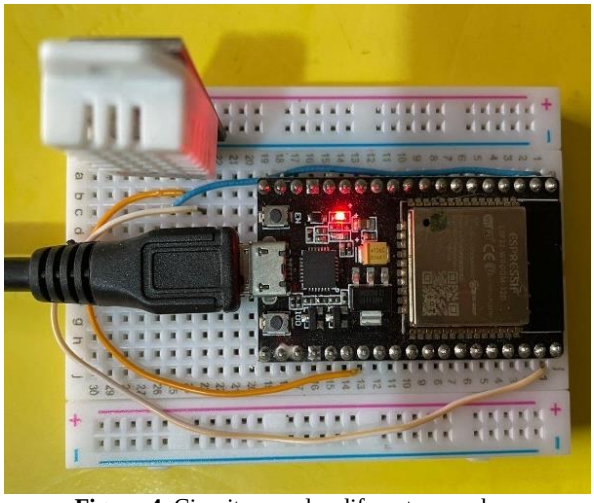


Figura 4. Circuito para las diferentes pruebas.

2.2.3. Análisis y envío de datos del ESP32.

En este apartado, se presenta un modelo compuesto por un circuito que consta de la comunicación entre el ESP32 y sensor DHT22 para él envió de datos de temperatura y humedad a la plataforma Thinger.io como modelo referencial de las otras conexiones.

Para la comunicación del ESP32, se crea un script usando como IDE el de Arduino en donde se programa las funciones que permite la conexión inalámbrica como se muestra en la Figura 5.

```
#define THINGER_SERIAL_DEBUG

#include <ThingerESP32.h>
//#include "arduino_secrets.h"
#include "DHT.h"
#define DHTPIN 4
#define DHTTYPE DHT22   // DHT 22  (AM2302), AM2321
DHT dht(DHTPIN, DHTTYPE);

#define USERNAME "GabyCh"
#define DEVICE_ID "Esp32Gaby"
#define DEVICE_CREDENTIAL "JDuHB#nD0ptTAAQK"



#define SSID "BITCH."
#define SSID_PASSWORD "Estrellita.2021"


ThingerESP32 thing(USERNAME, DEVICE_ID, DEVICE_CREDENTIAL);

void setup() {
  // open serial for monitoring
  Serial.begin(115200);
  dht.begin();
  // set builtin led as output
//  pinMode(LED_BUILTIN, OUTPUT);

  // add WiFi credentials
  thing.add_wifi(SSID, SSID_PASSWORD);
  Serial.println(WiFi.localIP());
  // digital pin control example (i.e. turning on/off a light, a relay, configuring a parameter, etc)
 // thing["led"] << digitalPin(LED_BUILTIN);

  // resource output example (i.e. reading a sensor value)
  thing["humedad"] >> outputValue(dht.readHumidity());
  thing["temperatura"] >> outputValue(dht.readTemperature());


  // more details at http://docs.thinger.io/arduino/
}

void loop() {
  delay(1000);
  thing.handle();
}
```

Figura 5. Script para conexión hacia plataforma Thinger.

2.2.4. Herramientas para la monitorización y captura de datos de datos.

2.2.4.1 Wireshark para la monitorización de red y análisis de paquetes.

Wireshark es un analizador de paquetes en tiempo real, y desde esa monitorización se puede observar la trasmisión de datos desde el ESP32 hacia las plataformas a las cuales se va a realizar ataques para hallar vulnerabilidades de la información enviada en tiempo real y de esta manera analizar si los datos se transmiten cifrados o no.

En la Figura 5, se muestra la aplicación Wireshark en acción.

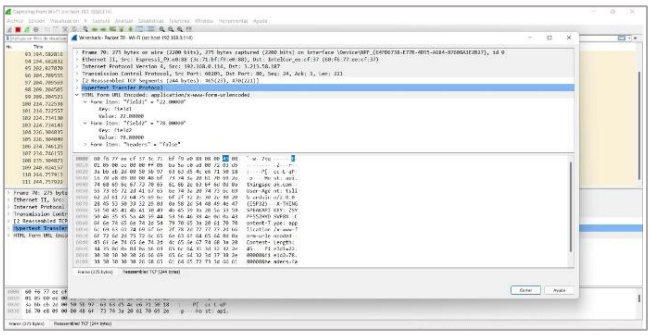


Figura 5. Análisis de trasmisión de datos.

2.2.4.2 WiFislax - Ettercap

Ettercap se utiliza para el ataque ARP del objetivo, estableciendo la puerta de enlace predeterminada del equipo victima a la dirección IP del equipo atacante [14].

De esta manera el equipo atacante estará situado entre el router y el objetivo, logrando así escuchar todo el tráfico de red que genera este último. En la Figura 6, se muestra la aplicación EtterCap en donde se ha seleccionado la IP del Gateway y la IP que le ha asignado el router al ESP32 [15].

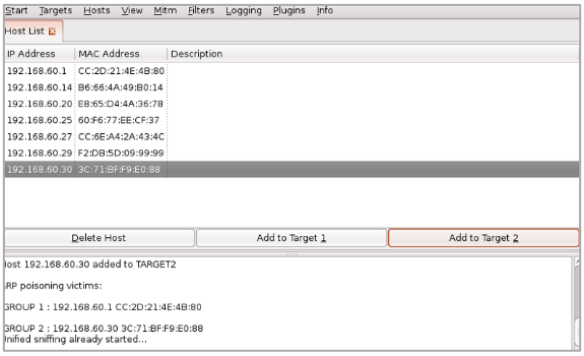


Figura 6. Captura Ettercap de los objetivos dentro de la red.

2.2.5. Ataques e intrusiones.

Los tipos de ataques que se efectúan para obtener los resultados son:

2.2.5.1 Man in the midle

"Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas" [8].

2.2.5.2 ARP Poisoning

"De los ataques Man in the Middle más conocidos y más peligrosos que se puede encontrar en las redes cableadas e inalámbricas" [9].

3. Resultados

Según [16], se realiza ataques a las plataformas y captura de datos con las herramientas antes mencionadas a 4 escenarios así se tienen: ESP32-BLYNK, ESP32-FIREBASE, ESP32-THINGERIO y ESP32-THINGSPEAK, cuyos resultados obtenidos se muestran en los siguientes apartados.

3.1. Conexión 1: ESP32 con plataforma Blynk.

En la Figura 7, se muestra la conexión establecida entre el ESP32 y el servidor de Blynk, así como la asignación de la IP dada por el router al dispositivo, también se puede observar él envió de los datos de temperatura y humedad.

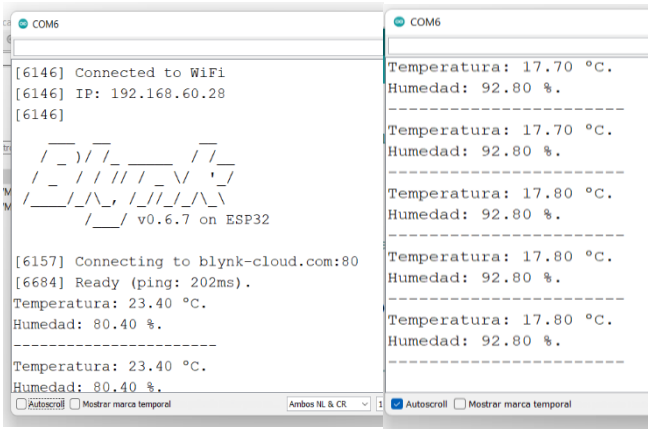


Figura .7 Conexión a la plataforma Blynk.

En la Figura 8, se puede observar la obtención de los datos en un dashboard del blynk instaladas en un Smartphone.

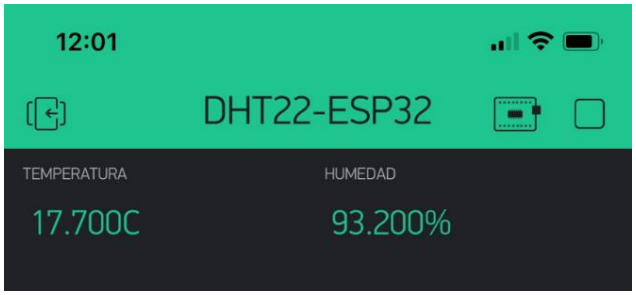


Figura 8. Información datos temperatura y humedad en dashboard Blynk.

3.1.1. Ataque a la conexión ESP32-Blynk.

Dentro de WiFislax se utiliza al Ettercap para realizar los ataques, el ataque utilizado será ARP Poisonig entre el Gateway (192.168.60.1) y el asignado al ESP32 (192.168.60.28) con dirección MAC= 3C:71: BF: F9:E0:88.

En la figura 9, se muestra la asignación de las víctimas a ser atacadas desde el router y el ESP32.

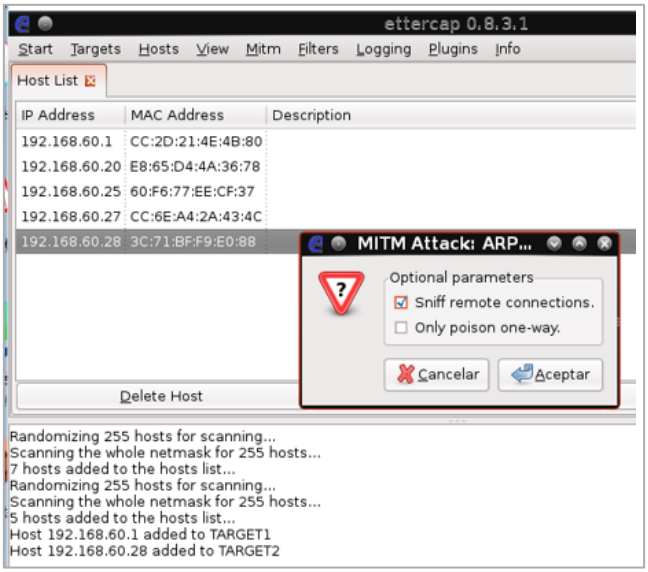


Figura 9. Captura EtterCap de los objetivos dentro de la red

En la figura 10, se puede observar que una vez efectuado el ataque con EtterCap ya puede observar simultáneamente con Wireshark la captura de paquetes, en este caso solo se puede observar paquetes ARP y TCP y no se pueden observar datos planos de la temperatura y humedad debido a que están cifrados. También se puede observar las direcciones fuente (ESP: 192.168.60.28) y destino, es decir, el servidor de Blynk (45.55.96.146).

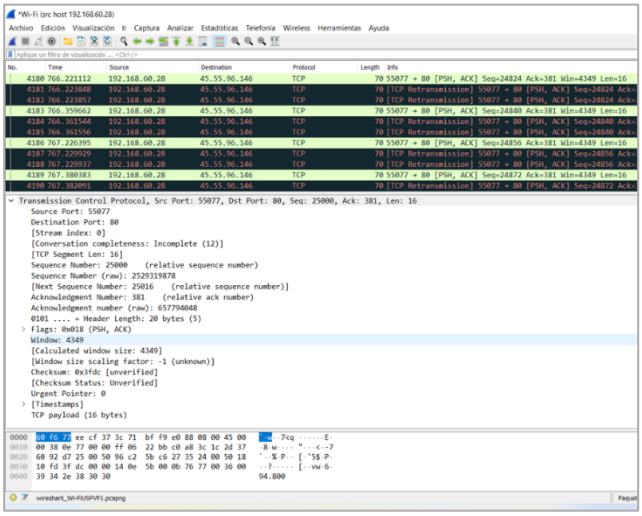


Figura .10 Lista de Paquetes dentro del analizador.

3.2. Conexión 2: ESP32 con plataforma Firebase.

En la Figura 11, se muestra la conexión establecida entre el ESP32 y el servidor de Firebase, así como la asignación de la IP dada por el router al dispositivo, también se puede observar él envió de datos de temperatura y humedad.

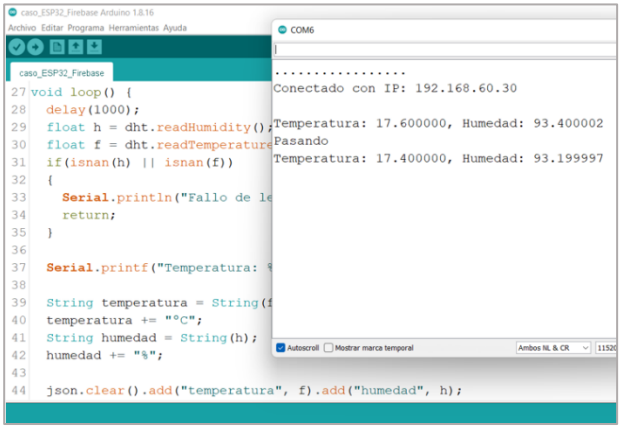


Figura 11. Conexión a la plataforma Firebase.

En la Figura 12, se puede observar la obtención de los datos en la base en tiempo real en el servidor de Firebase.

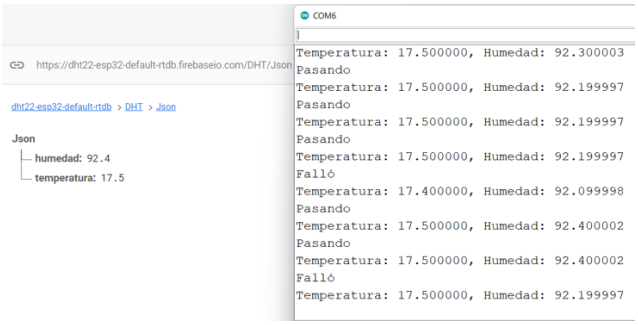


Figura 12. Información datos temperatura y humedad en Firebase.

3.2.1. Ataque a la conexión ESP32-Firebase

Dentro de WiFislax se utiliza al Ettercap, el ataque utilizado será ARP Poisonig entre el Gateway (192.168.60.1) y el asignado al ESP32 (192.168.60.30) con dirección MAC= 3C:71: BF: F9:E0:88.

En la figura 13, se muestra la asignación de las víctimas a ser atacadas desde el router y el ESP32

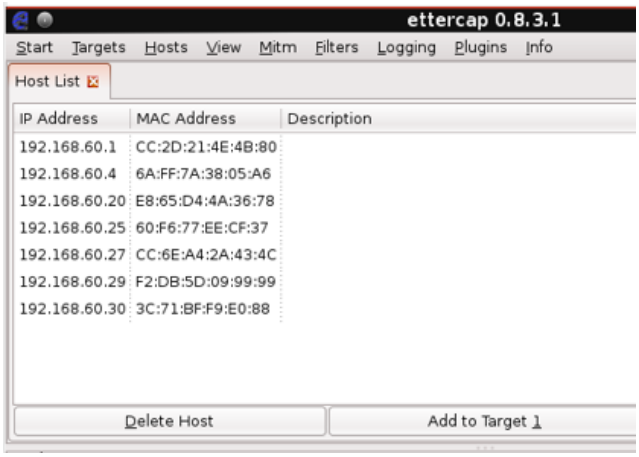


Figura 13. Captura EtterCap de los objetivos dentro de la red

En la figura 14, se puede ver que una vez efectuado el ataque con EtterCap ya puede observar simultáneamente con Wireshark la captura de paquetes, en este caso solo se puede obtener paquetes ARP, TCP y TLS v1.2 y no se pueden observar datos planos de la temperatura y humedad debido a que están cifrados e incluso se utiliza TLS para su seguridad. También se puede ver las direcciones fuente (ESP: 192.168.60.30) y destino, es decir, el servidor de Firebase (35.201.97.85).

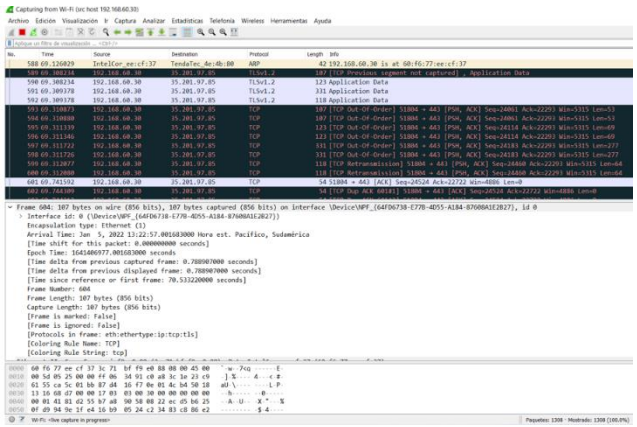


Figura 14. Lista de Paquetes dentro del analizador

3.3. Conexión 3: ESP32 con plataforma Thinger.io.

En la Figura 15, se muestra la conexión establecida entre el ESP32 y el servidor de Thinger.io, así como la asignación de la IP dada por el router al dispositivo, también se puede observar el envío de datos de temperatura y humedad.

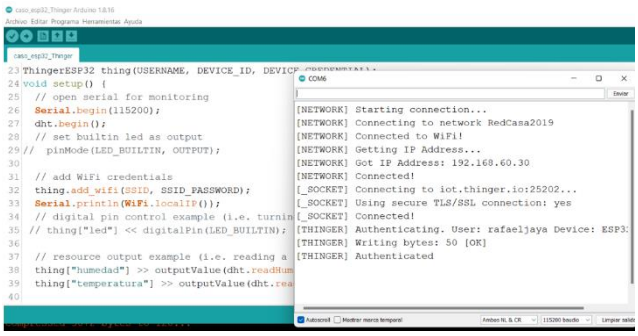


Figura 15. Conexión a la plataforma Thinger.io.

En la Figura 16, se puede observar la obtención de los datos en el dashboard de Thinger en tiempo real en el servidor de Thinger.io.

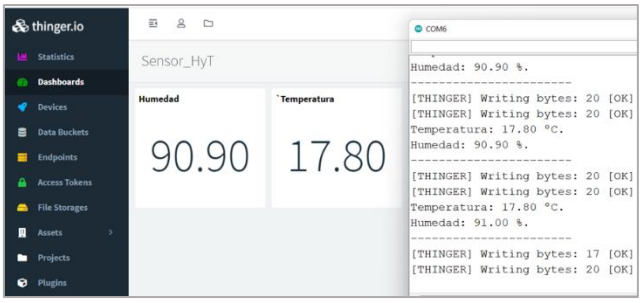


Figura 16. Información datos temperatura y humedad en Thinger.io.

3.3.1 Ataque a la conexión ESP32-Thinger.io

Dentro de WiFislax se utiliza al Ettercap para realizar los ataques, el ataque utilizado será ARP Poisonig entre el Gateway (192.168.60.1) y el asignado al ESP32 (192.168.60.30) con dirección MAC= 3C:71: BF: F9:E0:88.

En la figura 17, se muestra la asignación de las víctimas a ser atacas como son el router y el ESP32.

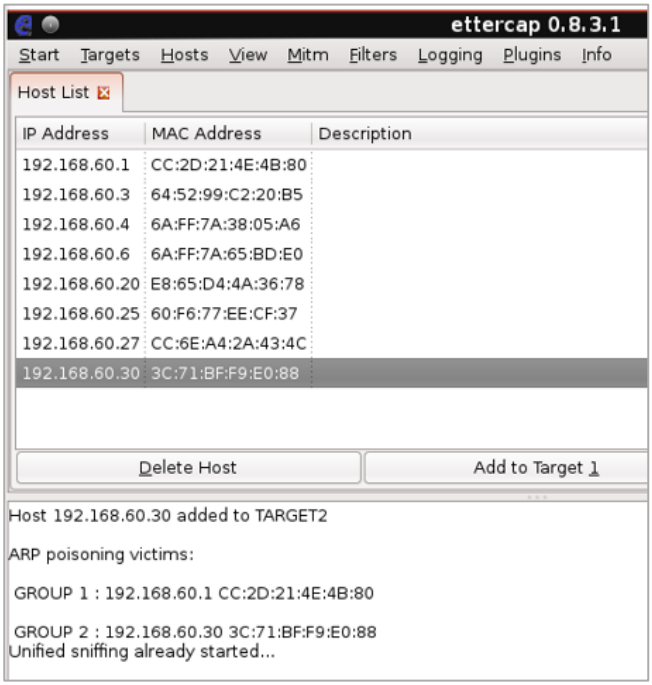


Figura 17. Captura Ettercap de los objetivos dentro de la red

En la figura 18, se puede ver que una vez efectuado el ataque con EtterCap ya puede observar simultáneamente con Wireshark la captura de paquetes, en este caso solo se puede obtener paquetes ARP, TCP y TLS v1.2 y no se pueden observar datos planos de la temperatura y humedad debido a que están cifrados e incluso se utiliza TLS para su seguridad. También se puede observar las direcciones fuente (ESP: 192.168.60.30) y destino, es decir, el servidor de Thinger.io (18.232.145.118).

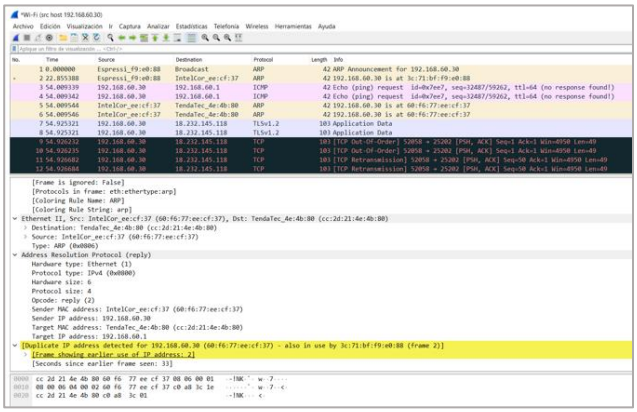


Figura 18. Lista de Paquetes dentro del analizador

3.4. Conexión 4: ESP32 con plataforma ThingSpeak

En la Figura 19, se muestra la conexión establecida entre el ESP32 y el servidor de ThingSpeak, así como la asignación de la IP dada por el router al dispositivo, también se puede observar él envió de datos de temperatura y humedad [12] y [13].

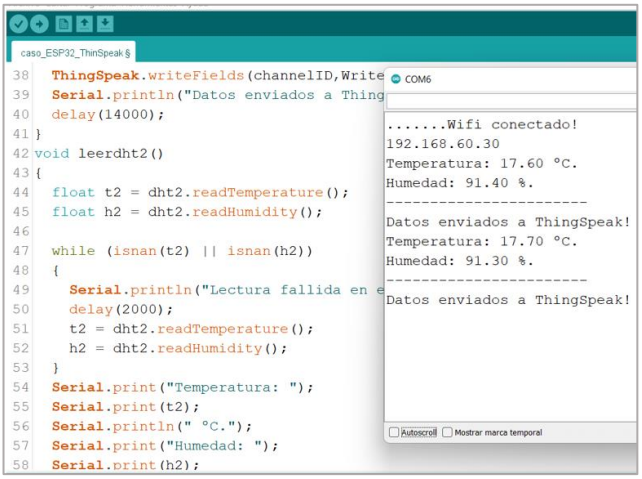


Figura 19. Conexión a la plataforma ThingSpeak.

En la Figura 20, se puede observar la obtención de los datos en el dashboard de

ThingSpeak en tiempo real en el servidor de ThingSpeak.

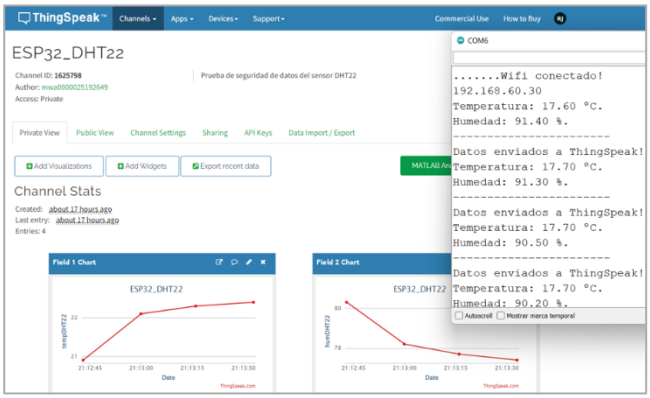


Figura 20.Captura de datos en tiempo real ThingSpeak

3.4.1. Ataque a la conexión ESP32-ThingSpeak

De las varias aplicaciones de WiFislax, se utiliza al Ettercap para realizar los ataques, el ataque utilizado será ARP Poisonig entre el Gateway (192.168.60.1) y el asignado al ESP32 (192.168.60.30) con dirección MAC= 3C:71: BF: F9:E0:88.

En la figura 21, Se muestra las victimas a ser atacadas.

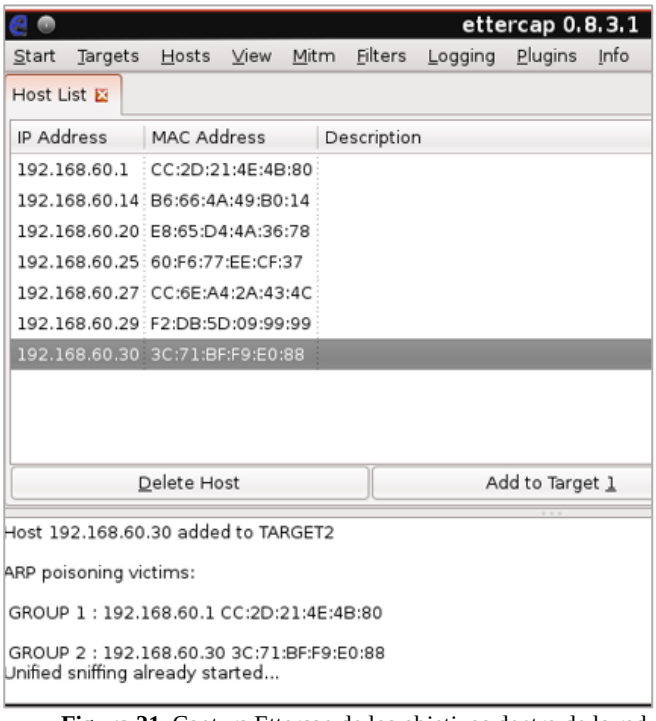


Figura 21. Captura Ettercap de los objetivos dentro de la red

En la figura 22, se puede ver que una vez efectuado el ataque con EtterCap, ya puede observar simultáneamente con Wireshark la captura de paquetes, en este caso solo se puede obtener paquetes ARP, TCP, UDP y HTML que es precisamente en este protocolo capturado donde se pueden observar datos planos de la temperatura y humedad en este caso T=17.8 y H=91.6 en los registros fiel1 y fiel2 respectivamente. También se puede observar las direcciones fuente (ESP: 192.168.60.30) y destino, es decir, el servidor de ThingSpeak (3.224.210.136).

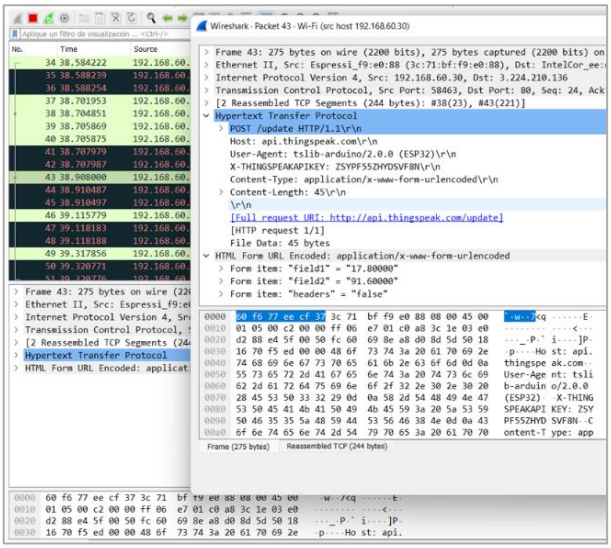


Figura 22. Lista de Paquetes dentro del analizador

3.5 Discusión

Como se pueden observar en los resultados de los 4 escenarios, de las 4 conexiones atacadas, la única que se halló vulnerabilidades fue en la conexión hacia ThingSpeak, donde se pudo capturar datos planos de temperatura y humedad, estos datos fueron hallados en los paquetes de HTML.

Por otro lado, la conexión más segura fue la de Firebase, puesto que se obtuvieron paquetes de ARP, TCP, y también paquetes TLS v1.2 que transmiten los datos cifrados porque según [10] "Actualmente, TLS 1.2 es el protocolo encargado de la mayoría de las encriptaciones que se producen en la web", por tanto, no se pudo capturar los datos transmitidos.

Finalmente, tanto Blynk como Thinger.io también presentan cifrados en sus transmisiones y, por ende, no se pudo evidenciar sus datos, de estos dos Thinger utiliza TLS y el Blynk solo se observaron paquetes TCP.

4. Conclusiones

De los 4 escenarios analizados con sus respectivos ataques, en la única que se halló vulnerabilidades fue en la conexión hacia ThingSpeak, donde se pudo observar la captura de datos planos de temperatura y humedad, estos datos fueron encontrados en los paquetes de HTML como se evidenció en las figuras. La conexión más segura fue la Firebase, puesto que, a más de los paquetes de ARP, TCP, se observó que también tiene paquetes TLS v1.2 que actualmente, es el protocolo encargado de la mayoría de las encriptaciones que se producen en la web, por tanto, no se pudo capturar los datos transmitidos. Finalmente, tanto Blynk como Thinger.io también presentan cifrados en sus transmisiones y, por ende, no se pudo evidenciar sus datos, de estos dos, Thinger utiliza TLS y en Blynk solo se pudo observar paquetes TCP.

5. Referencias

[1] General Juan Pablo Duarte y Diez. (2019). Las amenazas en el ciberespacio. 2019, de revista Científica Seguridad, Ciencia y Defensa http://201.159.222.35/bitstream/handle/22000/18891/Proyecto%20de%20Titulaci%c3%b3n%20Maestr%c3%ada%20Tic%c2%b4s%20Christian%20Cisneros.pdf?sequence=1&isAllowed=y

[2] Christian Rafael Cisneros Mera. (2021). Estudio de mecanismos de aseguramiento de la información para internet e las cosas IOT en Smart home. 2021, de Universidad Católica del Ecuador. http://201.159.222.35/bitstream/handle/22000/18891/Proyecto%20de%20Titulaci%c3%b3n%20Maestr%c3%ada%20Tic%c2%b4s%20Christian%20Cisneros.pdf?sequence=1&isAllowed=y

[3] Karen Scarfone. (2019). Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas. 2019, de National Institute of Standars and Technology ttps://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932207

[4] Carlos Andrés Mundt Briceño. (2018). Análisis Comparativo entre Algoritmos Simétricos orientados al IOT. 2018, de Universidad Andrés Bello http://repositorio.unab.cl/xmlui/bitstream/handle/ria/13569/a124724_Mundt_C_An%c3%a1lisis_Comparativo_Entre_Algoritmos_2018_Tesis.pdf?sequence=1&isAllowed=y

[5] José de la Prima Muñoz. (14/09/2021). Cyberseguridad Corporativa. 30 SIC, 146, 185.

[6] Javier Francisco Córdova Perdomo. (2021). Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la norma ISO 27001. 2021, de Universidad Peruana Unión https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/4789/Javier_Tesis_Maestro_2021.pdf?sequence=1&isAllowed=y

[7] S. Malenkovich, «kaspersky daily, » 10 04 2013. https://www.kaspersky.es/blog/que-es-un-ataqueman-in-the-middle/648/

[8] Roberto Garrido Pelaz. (2014). Auditoria de Sistemas y la seguridad en entornos mixtos. 2014, de Universidad Carlos III de Madrid Sitio web: https://e-archivo.uc3m.es/bitstream/handle/10016/22501/PFC_Roberto_Garrido_Pelaz_2014.pdf?sequence=1&isAllowed=y

[9] Sergio de Luz. (2021). Ataque ARP poisoning. 17 agosto 2021, de Redes Zone RZ https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/

[10] Linube. (2021). TLS a TLS 1.2. 2021, de Linube https://linube.com/blog/tls-1-2-protocolo-encriptar/#:~:text=Actualmente%2C%20TLS%201.2%20es%20el,los%20navegadores%20a%20TLS%201.2.

[11] A. F. Bravo Montoya, J. S. Rondón Sanabria y E. E. Gaona-García, «Desarrollo y prueba de un Sniffer en tiempo real de una red LoRawan usando GNU-Radio,» *TecnoLogicas,* vol. 22, nº 46, p. 10, 2019.

[12] Erfan, «Blynk community,» 2019. https://community.blynk.cc/t/mq2-gas-measurement/32387/2.

[13] G. Juan, «Instructables Circuits,» 2020. https://www.instructables.com/Nodemcu-Esp8266-PIR-Blynk/.

[14] S. d. Luz, «Aprende cómo utilizar Wireshark para capturar y analizar el tráfico de red,» RZ redes Zone, 13 Agosto 2021. https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/.

[15] S. d. Luz, «Aprende todo sobre el ataque ARP Poisoning y protégete,» RZ redes zone, 17 Agosto 2021. [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/.

[16] S. D. Luz, Redes Zone, 2021 Agosto 17. [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/.