UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TELECOMUNICACIONES

Tema:

SOLUCIONES DE SEGURIDAD EN SISTEMAS IOT DE HOGARES INTELIGENTES PARA MITIGAR RIESGOS Y VULNERABILIDADES MEDIANTE LA REALIZACIÓN DE PRUEBAS DE PENETRACIÓN

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniera en Telecomunicaciones

ÁREA: Comunicaciones

LÍNEA DE INVESTIGACIÓN: Tecnología de la información y sistemas de control

AUTOR: María Isabel Araujo Robalino

TUTOR: Ing. Julio Enrique Cuji Rodríguez, Mg.

Ambato - Ecuador

febrero – 2024

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: SOLUCIONES DE SEGURIDAD EN SISTEMAS IOT DE HOGARES INTELIGENTES PARA MITIGAR RIESGOS Y VULNERABILIDADES MEDIANTE LA REALIZACIÓN DE PRUEBAS DE PENETRACIÓN, desarrollado bajo la modalidad Proyecto de Investigación por la señorita María Isabel Araujo Robalino, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, febrero 2024

Ing. Julio Enrique Cuji Rodríguez, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: SOLUCIONES DE SEGURIDAD EN SISTEMAS IOT DE HOGARES INTELIGENTES PARA MITIGAR RIESGOS Y VULNERABILIDADES MEDIANTE LA REALIZACIÓN DE PRUEBAS DE PENETRACIÓN es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero 2024

María Isabel Araujo Robalino

C.C. 1803510864

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, febrero 2024

María Isabel Araujo Robalino

C.C. 1803510864

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por la señorita María Isabel Araujo Robalino, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado SOLUCIONES DE SEGURIDAD EN SISTEMAS IOT DE HOGARES INTELIGENTES PARA MITIGAR RIESGOS Y VULNERABILIDADES MEDIANTE LA REALIZACIÓN DE PRUEBAS DE PENETRACIÓN , nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, febrero 2024

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
JOSE VICENTE MORALES LOZADA

Dr. PhD. Vicente Morales Lozada
PROFESOR CALIFICADOR

Firmado electrónicamente por:
GEOVANNI DANILO BRITO MONCAYO

Ing. Geovanni Brito Moncayo, Mg.
PROFESOR CALIFICADOR

DEDICATORIA

A mi familia, especialmente a mi madre, sin cuyo apoyo incondicional este logro no habría sido posible.

A mis amigos, quienes hicieron que cada paso de este trayecto fuese más llevadero.

A mi abuelito, a quien le hubiera gustado estar presente en este momento.

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a mis amigos y familiares, cuya orientación y aliento fueron fundamentales para cumplir con este objetivo.

A mis estimados docentes por sus valiosas enseñanzas y su guía a lo largo de mi trayecto universitario. En especial, a la Ing. Andrea Sánchez y al Ing. Julio Cuji, quienes con su tiempo, paciencia y guía me permitieron culminar exitosamente con esta investigación.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

El Internet de las Cosas (IoT) está revolucionando la intercomunicación entre los dispositivos de hogares inteligentes. No obstante, la seguridad de estos sistemas enfrenta desafíos de seguridad a medida que se incorporan más dispositivos, por lo que es necesario soluciones eficaces que permitan la protección de datos sensibles y la integridad de la información.

El sistema IoT diseñado para esta investigación está compuesto por una variedad de dispositivos comunes en hogares inteligentes, tales como luces, interruptores, enchufes, cámaras de seguridad, sensores de movimiento y un asistente de voz "Alexa". La ejecución de pruebas de penetración en este sistema utiliza el modelo STRIDE, que analiza seis categorías de amenazas: suplantación de identidad, manipulación de datos, repudio, divulgación de información, denegación de servicios y elevación de privilegios; para identificar riesgos y vulnerabilidades específicos.

A partir de estos resultados, se establecen medidas para garantizar la seguridad del sistema, que incluyen limitar el acceso a dispositivos autorizados, asignar direcciones IP estáticas y contraseñas seguras en la configuración del router. Además, se incorporan herramientas en la máquina para monitorear y controlar el tráfico de datos, proporcionando al usuario la capacidad de supervisar el estado de su red.

La evaluación de la efectividad de estas medidas revela una mitigación de vulnerabilidades de un 64,052 % en el sistema IoT total, destacando así la eficacia de las medidas de seguridad aplicadas. Este alto porcentaje de mitigación evidencia la robustez del sistema en la protección contra posibles ataques y garantiza un entorno más seguro para los dispositivos IoT.

Palabras clave: Internet de las Cosas, vulnerabilidades, pruebas de penetración, medidas de seguridad.

ABSTRACT

The Internet of Things (IoT) is revolutionizing the intercommunication between smart home devices. However, the security of these systems faces security challenges as more devices are incorporated, so effective solutions are needed to protect sensitive data and information integrity.

The IoT system designed for this research is made up of a variety of devices common in smart homes, such as lights, switches, plugs, security cameras, motion sensors, and an "Alexa" voice assistant. Penetration testing on this system uses the Stride model, which analyzes six categories of threats: spoofing, data tampering, repudiation, information disclosure, denial of service, and elevation of privilege; to identify specific risks and vulnerabilities.

Based on these results, measures are established to ensure the security of the system, including limiting access to authorized devices, assigning static IP addresses, and strong passwords in the router's configuration. In addition, specific tools are incorporated in the machine to monitor and control data traffic, allowing users to supervise their network’s status.

The evaluation of the effectiveness of these measures reveals a mitigation of vulnerabilities of up to 64,052% in the total system. This highlights the effectiveness of the security measures applied. This high percentage of mitigation evidences the robustness of the system in protecting against possible attacks and guarantees a more secure environment for the system's IoT devices.

Keywords: Internet of Things, vulnerabilities, penetration testing, security measures.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

SOLUCIONES DE SEGURIDAD EN SISTEMAS IOT DE HOGARES INTELIGENTES PARA MITIGAR RIESGOS Y VULNERABILIDADES MEDIANTE LA REALIZACIÓN DE PRUEBAS DE PENETRACIÓN

1.1.1 Planteamiento del problema

En Ecuador, las redes de datos que incluyen dispositivos IoT se utilizan en diferentes instituciones y sectores, tanto privados como públicos y en hogares, para intercomunicarse y facilitar las actividades diarias. El impacto tecnológico de diferentes servicios en el país, como el servicio móvil avanzado, la telefonía fija y móvil, y fundamentalmente el servicio de acceso a internet, han tenido un aumento del 41% en el país, para el año 2022. Además, se tiene en cuenta que la población ecuatoriana cada vez más emplea sistemas conectados a los servicios de internet para realizar diferentes actividades cotidianas [1].

En Tungurahua, el número de abonados que cuentan con acceso a internet es de 91.506 aproximadamente, según datos obtenidos por ARCOTEL, a finales del año 2022, lo que permite un aumento considerable de los dispositivos IoT conectados a estas redes. Esto indica que el número de personas que hacen uso de tecnologías con acceso a internet sigue en aumento constante, como son teléfonos inteligentes, tablets, computadoras, luces inteligentes, sensores, cámaras, entre otros dispositivos inteligentes[2].

En la ciudad de Ambato, se ha dado un gran crecimiento en el desarrollo tecnológico de diferentes servicios. Esto ha creado una mayor demanda en redes de datos y conectividad IoT en diversos sectores, como son el comercio, la industria, la salud y el hogar. Sin embargo, la seguridad en entornos IoT aún presenta dificultades en la privacidad de datos. Es necesario realizar un análisis detallado de los riesgos y vulnerabilidades existentes en la seguridad de las redes que incluyen dispositivos IoT, con la finalidad de mejorar la seguridad en estos sistemas [3].

El Internet de las cosas (IoT) ha cambiado la forma en que los dispositivos se conectan y comunican entre sí, permitiendo que cada vez más usuarios decidan hacer uso de estos en el hogar. De esta manera, la seguridad en los sistemas IoT para hogares inteligentes es un tema importante a tratar a medida que más dispositivos conectados se integran. Sin embargo, la falta de seguridad, las vulnerabilidades en el diseño y desarrollo, la privacidad de datos y las deficiencias en las actualizaciones de seguridad de los sistemas IoT plantean una gran cantidad de desafíos. Por lo tanto, es necesario desarrollar soluciones efectivas para garantizar la seguridad en los hogares inteligentes basados en IoT [4].

La falta de conocimiento en seguridad informática por parte de los usuarios de dispositivos IoT ha generado diversos riesgos en la privacidad de sus datos. Esto puede resultar en una configuración insegura de los dispositivos, contraseñas débiles o falta de actualizaciones de seguridad importantes para el sistema. Por otra parte, la presencia de vulnerabilidades en el diseño y desarrollo de estos dispositivos facilita el acceso de los atacantes. La funcionalidad de los dispositivos IoT suele recibir más atención que la seguridad durante el proceso de diseño y desarrollo, debido a recursos limitados o falta de pruebas adecuadas [5].

En conclusión, la seguridad en los sistemas IoT para hogares inteligentes presenta diversas dificultades que requieren atención y soluciones efectivas. A través de una constante mejora de la seguridad se puede aprovechar plenamente los beneficios de los sistemas IoT en hogares inteligentes sin comprometer la privacidad y la seguridad de los usuarios.

1.2 Antecedentes investigativos

La investigación se basa en una amplia revisión de repositorios universitarios nacionales e internacionales, así como en bases de datos de artículos científicos. A través de esta revisión bibliográfica, se adquirió información relevante acerca de las vulnerabilidades encontradas en los principales dispositivos IoT que forman parte de los hogares inteligentes.

Geovanny Manuel García Villafuerte, en el año 2023, realiza un "ANÁLISIS DE VULNERABILIDADES EN SISTEMAS DE AUTOMATIZACIÓN EN EL HOGAR" en Guayaquil. Esta investigación demuestra cómo se consigue vulnerar la seguridad de la red en el hogar al utilizar medidas de seguridad débiles y propone soluciones efectivas para proteger la integridad de la información y los dispositivos conectados. Se destaca la importancia de implementar medidas de seguridad sólidas, como el uso de contraseñas seguras, la actualización regular del software y firmware de los dispositivos, la configuración del protocolo de cifrado WPA2, y la aplicación de firewalls que ayuden a proteger la red [6].

En el año 2023, Aaesha Aldahmani, Bassem Ouni, Thierry Lestable y Merouane Debbah realizan una investigación acerca de "CYBER-SECURITY OF EMBEDDED IOTS IN SMART HOMES: CHALLENGES, REQUIREMENTS, COUNTERMEASURES, AND TRENDS" para Technology Innovation Institute. En esta investigación se detalla los problemas de seguridad y privacidad a los cuales los usuarios de dispositivos IoT se enfrentan en el hogar. Los hogares inteligentes son vulnerables a diversos tipos de ataques, por lo que se realiza un análisis de los objetos, el diseño y los estándares utilizados en dispositivos IoT. Así, los investigadores analizaron los riesgos más graves relacionados con la privacidad y la seguridad en un hogar inteligente. Además, establecieron un estudio sobre los principales componentes de un hogar inteligente que deben ser protegidos [7].

Akashdeep Bhardwaj, Keshav Kaushik, Mohammed Alshehri, Ahmed Abo-Bakr Mohamed e Ismail Keshta, en el año 2023, realizan la investigación "ISF: SECURITY ANALYSIS AND ASSESSMENT OF SMART HOME IOT-BASED FIRMWARE" para la Association for Computing Machinery. En este estudio explican los peligros de seguridad de datos asociados a la implementación de tecnología IoT en ciudades y hogares inteligentes. Esta investigación estudia el firmware de los dispositivos IoT, revelando datos sensibles y credenciales de usuario y contraseñas codificadas que pueden ser utilizadas en futuros ataques y violaciones de dispositivos IoT. Los investigadores proponen una base sobre cómo analizar los conjuntos de datos en tiempo real producidos por los motores de búsqueda de IoT utilizando palabras clave según diferentes tipos de dispositivos, ubicaciones y fabricantes [8].

Erini Sofia Anthi, en el año 2022, realiza un estudio basado en “DETECTING AND DEFENDING AGAINST CYBER ATTACKS IN A SMART HOME INTERNET OF THINGS ECOSYSTEM” para Cardiff University: School of Computer Science & Informatics. Esta investigación plantea el diseño de un prototipo IoT hub, un punto central que permite la conectividad y la gestión de múltiples dispositivos IoT, que demuestra cómo las tecnologías de conectividad, API y seguridad pueden ser implementadas en entornos de hogares inteligentes. Este IoT hub permite a los usuarios controlar y acceder de manera remota y segura a una variedad de dispositivos IoT dentro de su hogar. Además, presenta un sistema de Detección de Intrusiones (IDS) de IoT que utiliza aprendizaje automático supervisado para clasificar y detectar dispositivos y ataques en la red de manera muy precisa. En conjunto, estas tecnologías y enfoques contribuyen significativamente a mejorar la seguridad de los dispositivos IoT en un entorno de hogar inteligente [9].

En el año 2022, Rohit Akhilesh, Oliver Bill, Naveen Chilamkurti y Mohammad Jabed Morshed Chowdhury, realizan un artículo titulado “AUTOMATED PENETRATION TESTING FRAMEWORK FOR SMART-HOME-BASED IOT DEVICES” para la revista Future Internet. En esta investigación se desarrolló un marco de pruebas de penetración automatizado para dispositivos IoT en hogares inteligentes, con el objetivo de identificar vulnerabilidades comunes. Se seleccionaron cinco dispositivos comunes, entre los cuales se encuentran los Tp-Link Smart Bulb, el Tp-Link Smart Camera y el Google Home Mini, y se aplicaron pruebas automatizadas para descubrir vulnerabilidades, utilizando el Sistema de Puntuación de Vulnerabilidad Común (CVSS) para evaluar su gravedad. A través de este sistema se encontró que el Tp-Link Smart Bulb y el Tp-Link Smart Camera eran los dispositivos más vulnerables, mientras que el Google Home Mini era el más seguro, al mostrar un nivel más alto de seguridad en su diseño y configuración. Por lo tanto, estos hallazgos muestran la necesidad de abordar y corregir las vulnerabilidades más comunes en dispositivos IoT para garantizar la protección y seguridad de los hogares inteligentes [10].

1.3 Fundamentación teórica

1.3.1 Industria 4.0

El término industria 4.0 se refiere a un modelo de organización y control de la cadena de valor a través del ciclo de vida del producto y a lo largo de los sistemas de fabricación apoyado por las tecnologías de la información, es habitual referirse a este concepto con términos como “Fábrica Inteligente” o "Internet industrial", por lo que se trata de la aplicación a la industria del modelo "Internet de las cosas" (IoT) [11].

La industria 4.0 representa un enfoque a la innovación de nuevos productos y procesos, a través de fábricas inteligentes, totalmente integradas en redes de trabajo que propician nuevas formas de colaboración e infraestructuras sociales. Esta tecnología se relaciona con la digitalización de los sistemas de información y producción para las actividades de gestión; los sistemas de automatización para la adquisición de datos de las máquinas y líneas de producción; el monitoreo de datos y control de procesos, entre otros [12].

a. Fundamentos tecnológicos de la Industria 4.0

La Industria 4.0 se basa en nueve pilares tecnológicos. Estas innovaciones conectan los mundos físico y digital y habilitan sistemas inteligentes y autónomos. Las empresas y cadenas de suministro ya utilizan algunas de estas tecnologías avanzadas, pero todo el potencial de la Industria 4.0 cobra vida cuando se utilizan juntas [11]. En la Figura 1, se observa un esquema general de las tecnologías pertenecientes a la Industria 4.0.

Figura 1. Tecnologías de la Industria 4.0

En la Tabla 1, se describen las principales características de cada una de las tecnologías que componen la Industria 4.0.

Tabla 1. Tecnologías que forman parte de la industria 4.0 [12], [11].

Tecnología	Descripción
El Big Data y las analíticas de la IA	Big Data analiza grandes volúmenes de datos para obtener información valiosa, mientras que las analíticas de la IA utilizan algoritmos de inteligencia artificial para extraer patrones y conocimientos de estos datos.
Integración horizontal y vertical	La integración horizontal es la colaboración entre empresas del mismo nivel en la cadena de suministro, y la integración vertical es el control de una empresa sobre varias etapas de producción.
Computación en la nube	Los usuarios pueden acceder a servidores, bases de datos y otros servicios alojados en centros de datos remotos a través de la nube.
Realidad aumentada (AR)	La realidad aumentada, combina elementos virtuales con el entorno real, a través de ciertos dispositivos.
Internet de las cosas industrial (IIoT)	Es la interconexión de dispositivos y sistemas para recopilar y compartir datos, permitiendo el monitoreo y control de datos.
Fabricación aditiva/Impresión 3D	Es la reproducción del mundo físico en un modelo virtual que puede incluir máquinas, productos y personas.
Robots autónomos	Son robots que pueden operar sin intervención humana, tomando decisiones y adaptándose a su entorno de manera independiente.
Simulación/gemelos digitales	Es una simulación virtual de una máquina, producto, proceso o sistema del mundo real basado en datos de sensores de IoT.
Ciberseguridad	Es la práctica de proteger sistemas informáticos y redes de ataques, robo de datos y amenazas cibernéticas para garantizar la integridad, confidencialidad y disponibilidad de la información.

b. Sistema ciberfísico

Un sistema ciberfísico (CPS, por sus siglas en inglés) es un sistema en el cual los componentes físicos y los componentes computacionales están estrechamente integrados y se comunican entre sí para lograr una funcionalidad conjunta. Estos sistemas combinan el mundo físico con el mundo digital, permitiendo la interacción y la colaboración entre objetos físicos y sistemas informáticos Estos sistemas se caracterizan por su capacidad para monitorear, controlar y responder a eventos y condiciones del mundo real utilizando sensores, actuadores y software, además de la capacidad de comunicarse a través de redes de información [13].

1.3.2 Internet de las cosas

El “Internet de las Cosas” (IoT) hace referencia, como se ha indicado previamente, a una tecnología basada en la conexión de objetos cotidianos a Internet que intercambian, agregan y procesan información sobre su entorno físico para

proporcionar servicios de valor añadido a los usuarios finales. También reconoce eventos o cambios, y tales sistemas pueden reaccionar de forma autónoma y adecuada. Su finalidad es, por tanto, brindar una infraestructura que supere la barrera entre los objetos en el mundo físico y su representación en los sistemas de información Permite la conexión y la comunicación de dispositivos, y ofrece numerosos beneficios, como la optimización de recursos, la eficiencia energética, la seguridad mejorada, la toma de decisiones basada en datos y la mejora de la calidad de vida. Sin embargo, también plantea desafíos en términos de privacidad, seguridad y gestión de grandes volúmenes de datos generados [5], [14].

a. Dispositivos IoT

Los dispositivos IoT hacen referencia a cualquier tipo de dispositivo u objeto que se integra en una red de comunicación, con el propósito de intercambiar información y garantizar el rendimiento de una aplicación específica. Estos componentes tienen la capacidad de realizar su identificación de manera única, conocer su ubicación y los registros de ubicaciones previas, comunicar su estado a un servidor para actualizar sus características y funcionamiento, y comprender su entorno, de manera que se puedan aprovechar todos sus recursos. Los dispositivos IoT se caracterizan por la presencia de ciertos componentes específicos que incluyen sensores, actuadores, procesadores y transceptores integrados. [15].

b. Sistema IoT para un Hogar Inteligente

Un hogar inteligente (smart home) es un hogar que contiene dispositivos u objetos inteligentes que recolectan y generan información sobre su uso y entorno. Estos se pueden controlar, ajustar a nuestras preferencias, así como configurarlos para que funcionen de manera autónoma. Se trata, por tanto, de dispositivos de uso doméstico que ofrecen nuevas posibilidades mediante la conexión a Internet y cuyo objetivo es mejorar los distintos aspectos de la calidad de vida de los hogares [16].

Los dispositivos de smart home pueden analizar y aprender de los hábitos de sus usuarios, las preferencias y las condiciones para autoajustarse cuando sea necesario. El hogar inteligente está equipado, por tanto, con múltiples dispositivos que pueden cooperar entre sí como un sistema homogéneo. De esta manera se permite a los

usuarios controlar remotamente los electrodomésticos y otros dispositivos, regular el consumo de energía y disminuir la carga de las actividades cotidianas del hogar [17]. En la Tabla 2, se muestran ejemplos de dispositivos IoT distribuidos en distintas categorías que se utilizan en un hogar inteligente.

Tabla 2. Dispositivos IoT para hogares inteligentes [17].

Categorías	Dispositivo IoT
Asistentes de voz.	Alexa Echo, Google Home, Apple Homepod
Electrodomésticos	Lavavajillas, frigoríficos, lavadoras, aspiradoras.
Ocio y entretenimiento	Smartphone, smart tv, chromecast, fire stick.
Accesorios wereables	Smartwatch, dispositivos fitness.
Sonido	Altavoces, auriculares.
Climatización	Termostato, humidificador, aire acondicionado, estaciones de meteorología.
Iluminación y ahorro de energía	Lámparas, bombillas, interruptores, enchufes, temporizadores.
Salud y atención sanitaria	Monitoreo del sueño, medición de signos vitales.
Seguridad y vigilancia	Cámaras WIFI, cámaras para bebés, alarmas.
Detectores y sensores	Detectores de humo, detectores de agua, sensores de movimiento, sensores para puertas y ventanas.

1.3.3 Ciberseguridad

Es el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, prácticas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y sus usuarios en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes características: disponibilidad, integridad y confidencialidad. La ciberseguridad es la protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información procesada, almacenada y transportad por los sistemas de información que se encuentran interconectados [18].

a. Seguridad en aplicaciones

La seguridad de las aplicaciones se refiere a las medidas de seguridad, a nivel de aplicación, cuyo propósito es impedir el robo o el secuestro de datos o códigos dentro de la aplicación. Son las consideraciones de seguridad que se deben tener en cuenta al desarrollar y diseñar aplicaciones. La seguridad de las aplicaciones puede incluir hardware, software y procesos que mitigan las vulnerabilidades de seguridad [19].

b. Seguridad en dispositivos móviles

La seguridad de dispositivos móviles es la protección total de datos en dispositivos portátiles y la red conectada a los dispositivos mediante estrategias, infraestructuras y softwares. Algunos dispositivos portátiles comunes de una red son los teléfonos inteligentes, las tablets y las computadoras personales. La seguridad en los dispositivos móviles incluye la protección de datos en el dispositivo local, en los endpoints conectados al dispositivo y en los equipos de redes [20].

1.3.4 Seguridad en infraestructura de redes

La seguridad en infraestructura de redes se suele aplicar a los entornos de tecnologías de la información empresariales. Se trata de un proceso para proteger la infraestructura de red subyacente mediante la instalación de medidas preventivas con el objetivo de denegar el acceso, la modificación, la eliminación y la apropiación no autorizados de recursos y datos [21]. En la Tabla 3, se presentan los enfoques principales para la aplicación de la seguridad de infraestructura de redes.

Tabla 3. Enfoques de aplicación en la seguridad de la infraestructura de red [21]

Enfoque de aplicación	Descripción
Segmentación y separación de redes y funciones	Es un mecanismo de seguridad que dividir la infraestructura de red en segmentos o zonas separadas, donde solo ciertos usuarios o sistemas pueden acceder a cada segmento.
Restricción de las comunicaciones laterales innecesarias	Es la limitación de la comunicación directa entre sistemas o usuarios en una red, permitiendo solo las comunicaciones necesarias para las operaciones.
Refuerzo de los dispositivos de red	Es fortalecer la seguridad en los dispositivos de red, como routers, switches y firewalls, mediante la aplicación de configuraciones seguras, actualizaciones de firmware y la implementación de autenticación y autorización adecuadas.
Gestión de red fuera de banda (OoB)	Es la administración los dispositivos de red a través de una red separada y dedicada, que está aislada de la red principal.

Además, es importante tener en cuenta que las redes seguras se centran en dos principios básicos: autenticación y autorización. Es decir, primero, se verifica la autenticidad de los usuarios y a continuación, se confirma sus autorizaciones de acceso a datos específicos [22].

a. Seguridad en redes de área local

La red área local es un tipo de red que conecta ordenadores y dispositivos en un área específica y delimitada, como por ejemplo una oficina o un edificio. Se logra mediante la implementación de medidas como contraseñas seguras, autenticación de usuarios autorizados, configuración adecuada de dispositivos de red como routers y puntos de acceso Wi-Fi, y el uso de tecnologías como VPN para conexiones remotas [19].

b. Seguridad en redes inalámbricas

La seguridad en las redes inalámbricas es fundamental para proteger la privacidad y los datos sensibles de los usuarios. La implementación de medidas de seguridad adecuadas protege la información que se transmite a través de la red Wi-Fi. Además, se deben utilizar contraseñas seguras para el acceso a la red y cambiarlas periódicamente. Asimismo, mantener el firmware actualizado y monitorear la red en busca de actividad sospechosa son prácticas de seguridad son también aspectos esenciales para mantener una red inalámbrica segura [20].

1.3.5 Seguridad en redes IoT

La seguridad de la Internet de las cosas implica proteger los dispositivos de Internet y las redes a las que están conectados de las amenazas en línea y las filtraciones de datos. Esto se logra al identificar, monitorear y abordar posibles vulnerabilidades de seguridad en todos los dispositivos. A medida que aumenta el número de dispositivos conectados, los ciberdelincuentes tienen más oportunidades para poner en peligro la seguridad de los datos Las consecuencias de las brechas de seguridad de la IoT pueden ser muy dañinas. Esto porque el IoT afecta a sistemas tanto virtuales como físicos [21].

a. Riesgos y vulnerabilidades en sistemas IoT

El aumento en la implementación de dispositivos IoT ha generado desafíos para la ciberseguridad debido a la falta de mecanismos que permitan una autenticación adecuada de los datos. Según, The Role of Artificial Intelligence in Cyber Security, el 70 % de los dispositivos IoT son vulnerables a brechas y ataques de seguridad [23]. Además, la mayoría de los dispositivos IoT presentan limitaciones en cuanto al almacenamiento de datos, lo que motiva la necesidad de utilizar soluciones de

almacenamiento en la nube. Sin embargo, muchos fabricantes no consideran la clasificación de los datos transmitidos al diseñar los dispositivos IoT, lo que deja vulnerable al dispositivo [24]. En la Figura 2, se muestra el diseño de un diagrama de amenazas en dispositivos IoT, en el cual se observan los conceptos clave relacionados.

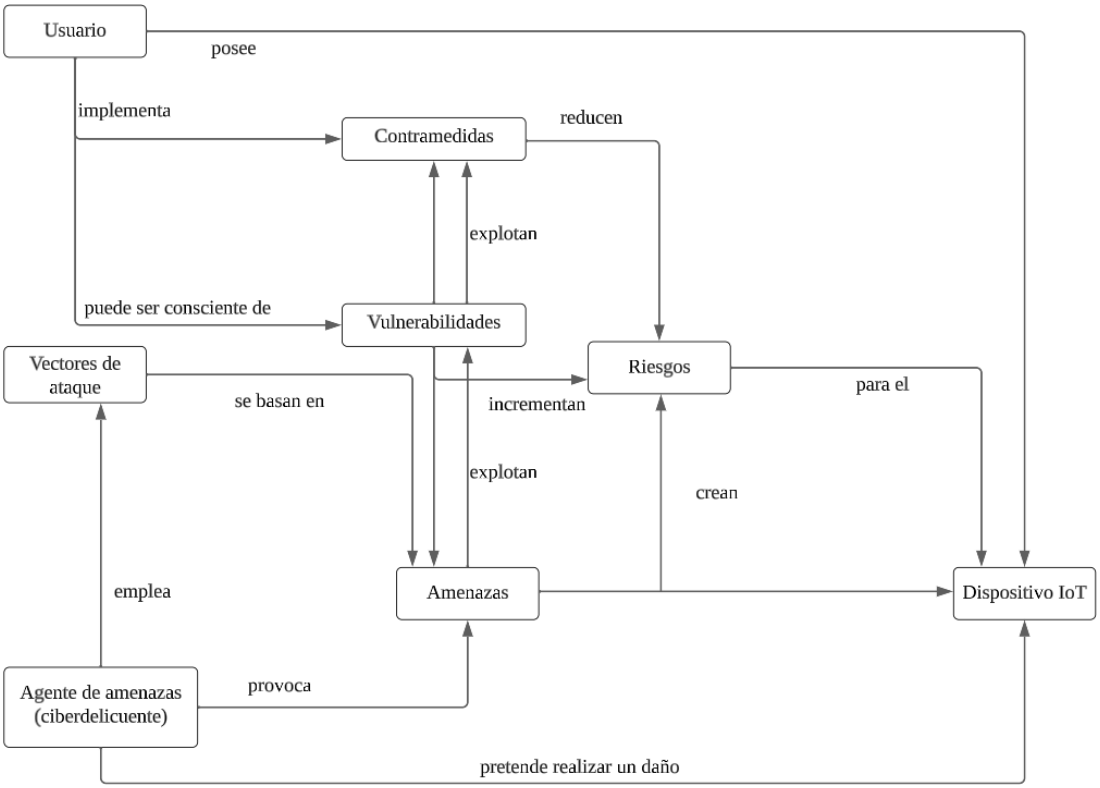


Figura 2. Diagrama de amenazas en dispositivos IoT [24].

La seguridad en los dispositivos IoT es fundamental para los usuarios de hogares inteligentes, los cuales esperan que los dispositivos IoT implementados en su hogar sean seguros y funcionen de manera confiable. Los agentes de amenazas o ciberdelincuentes intentan explotar las vulnerabilidades a través de diversos vectores de ataque. Las amenazas se convierten en riesgos, y las contramedidas se implementan para reducir estos riesgos y proteger los dispositivos IoT [24]. La gestión de la seguridad en dispositivos IoT implica la identificación de vulnerabilidades, la evaluación de riesgos y la implementación de contramedidas efectivas para garantizar la seguridad y la privacidad del usuario. Para ello es necesario identificar posibles debilidades en hardware, software y configuración, evaluar los riesgos asociados y aplicar medidas de seguridad adecuadas a los requerimientos del sistema IoT [25].

- ***Análisis de la arquitectura de sistemas IoT.*** En general, la arquitectura de un sistema IoT, se puede dividir en cuatro capas: capa de aplicación, capa de procesamiento de datos o servicios, capa de red y capa perceptiva o de sensores. En esta arquitectura, cada capa funciona con diferentes tecnologías, y por lo tanto, han surgido riesgos y vulnerabilidades relacionados con la seguridad en cada capa [26]. En la Figura 3, se presentan gráficamente los componentes que conforman cada una de las capas de la arquitectura en los sistemas IoT.

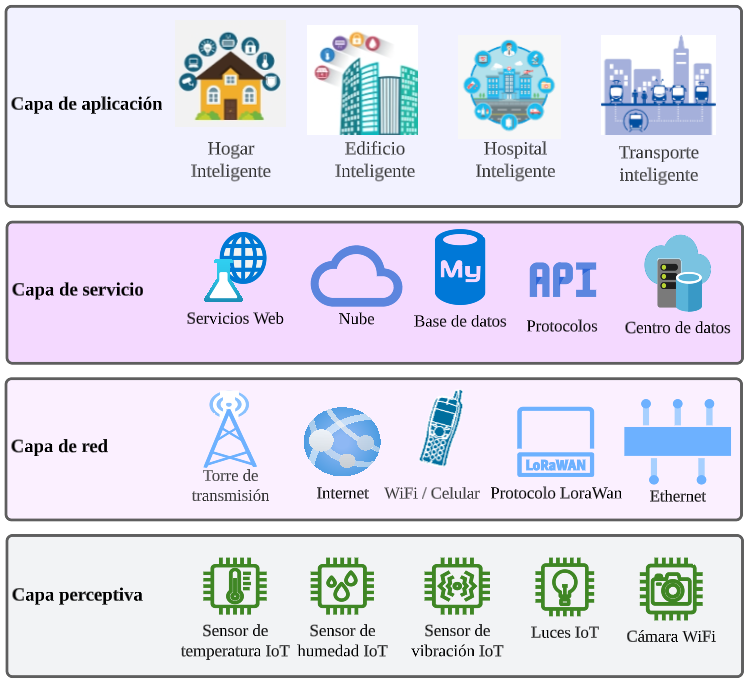


Figura 3. Capas de la arquitectura en los sistemas IoT [26].

- **Capa perceptiva:** La capa perceptiva corresponde a los sensores y demás dispositivos de hardware empleados en los sistemas IoT. Se encuentran diferentes tipos de sensores, como sensores de temperatura, sensores de humedad, sensores de vibración, sensores en cámaras, iluminación, detectores de humo, entre otros. Esta capa cumple un papel fundamental al recopilar datos del sistema a través de sensores y dispositivos físicos. Sin embargo, esta capa es especialmente vulnerable a amenazas de seguridad debido a su exposición a posibles ataques externos [26]. En la Tabla 4, se muestran los riesgos y vulnerabilidades encontrados en la capa perceptiva, con sus respectivas medidas de seguridad.

Tabla 4. Riesgos y vulnerabilidades en la capa perceptiva [24], [26].

Riesgos y vulnerabilidades	Descripción	Mecanismos de seguridad
Ataque de inyección de código malicioso	El atacante utiliza códigos maliciosos para insertarlos en la memoria de los nodos físicos, obteniendo acceso al dispositivo.	Filtrado y validación de datos de entrada, actualizaciones de firmware seguras y autenticadas.
Ataque de inyección de datos falsos	El atacante captura el nodo e inyecta datos falsos en el dispositivo, lo que genera que el sistema funcione incorrectamente.	Criptografía y autenticación de datos, filtros de datos y control de acceso.
Captura de nodos	El atacante intenta reemplazar un nodo existente con un nodo malicioso, el cual actúa como parte del sistema.	Encriptación de comunicaciones entre nodos, monitoreo los nodos.
Intervención y escucha	Los sistemas IoT poseen varios nodos desplegados por los cuales los usuarios no autorizados recopilan información confidencial.	Encriptación de datos en tránsito, autenticación mutua de dispositivos.
Ataques de canal lateral	Es la observación de información no pública que se filtra involuntariamente durante en un sistema o dispositivo.	Controles de acceso, cortafuegos, protección contra manipulación y autodestrucción.
Ataque de privación del sueño	El atacante agota la batería de un dispositivo IoT al tenerlo activo de manera continua, lo que genera problemas de funcionamiento.	Sistema de detección de intrusiones, red neuronal de Hopfield, función de sesgo radial.
Ataques de arranque	Es la explotación de vulnerabilidades y debilidades de seguridad en la fase inicial del procesamiento de los dispositivos IoT.	Medidas de autenticación y verificación de datos, control de acceso al firmware.
Ataque de interferencia en nodos WSNs	Se lleva a cabo por nodos maliciosos en la red, que interfieren, interrumpen o bloquean las señales, al enviar información inútil.	Protección física de los dispositivos, auditorías de seguridad física periódicas.
Puertos de depuración visibles	Los puertos de depuración se utilizan para conectar y analizar el registro de dispositivos y la información de errores.	Desactivación o aseguramiento de los puertos de depuración, restricción de acceso.
Componentes de terceros no verificados	Los dispositivos IoT suelen utilizar firmware de terceros, las vulnerabilidades de estos sistemas se heredarían al sistema.	Evaluación y verificación de la seguridad de los dispositivos.
Universal Plug-and-Play (UPnP)	Permite la conexión de cualquier dispositivo conectado al resto del mundo a través de Internet.	Deshabilitación de UPnP si no es esencial.
Baja seguridad física de los dispositivos	El monitoreo remoto de los dispositivos representa un riesgo, al recopilar datos en lugares públicos o al aire libre.	Políticas de privacidad, encriptación de datos.
Recopilación de objetos	Los dispositivos IoT no se supervisan físicamente en lugares remotos y un atacante podría insertar físicamente un nuevo dispositivo/objeto en la red.	Uso de etiquetas RFID seguras con autenticación y cifrado.
Clonación de etiquetas	El atacante copia la información de una etiqueta electrónica RFID o una tarjeta inteligente a una etiqueta clonada	Uso de etiquetas resistentes a manipulación y autenticación de etiquetas.
Ataque de manipulación de etiquetas	Los atacantes pueden falsificar una etiqueta en un sistema de RFID utilizando el método de manipulación de etiquetas.	Verificación de la autenticidad de hardware y firmware.
Troyanos en el Hardware	El atacante modifica maliciosamente el circuito integrado, al obtener acceso y recopilar información confidencial.	Medidas de autenticación y verificación de datos, control de acceso al firmware.

- **Capa de red:** La capa de red se encarga de la transferencia de datos desde los dispositivos o sensores ubicados en la capa perceptiva, a través de una red de comunicación, hasta la capa de procesamiento de datos o servicios, en donde se analizan estos datos para la toma de decisiones. En esta capa se presentan diversas vulnerabilidades que pueden comprometer la seguridad de la red y los dispositivos conectados. La integridad y la autenticación de los datos enviados a los dispositivos del sistema, es el principal problema de seguridad en esta capa [26]. En la Tabla 5, se muestran los riesgos y vulnerabilidades encontrados en la capa de red, con sus respectivas medidas de seguridad.

Tabla 5. Riesgos y vulnerabilidades en la capa de red [26], [27].

Riesgos y Vulnerabilidades	**Descripción**	**Mecanismos de seguridad**
Ataque de denegación de servicio (DoS)	El atacante genera un alto número de solicitudes no deseadas a los dispositivos, afectando sus servicios para el usuario.	Filtrado de tráfico no deseado, implementación de cortafuegos.
Ataques de enrutamiento	El atacante intenta alterar la forma en que los datos se transmiten a través de la red.	Implementación de protocolos de enrutamiento seguros, autenticación de dispositivos.
Intercepción de redes celulares	Los dispositivos utilizan comúnmente conexiones Wi-Fi o celulares, los atacantes pueden crear una estación base falsa y robar información del usuario.	Uso de cifrado, monitoreo constante para detectar interferencias.
Ataque de fuerza bruta	El atacante intenta acceder a un dispositivo a través de los puertos SSH o Telnet para violaciones de datos.	Políticas de contraseñas seguras y complejas.
Ataque de hombre en el medio (MITM)	El atacante se inserta en una comunicación entre dos partes, para interceptar o alterar información.	Uso de cifrado de extremo a extremo, autenticación mutua entre dispositivos.
Ataques de criptoanálisis	El atacante estudia el texto cifrado, los cifrados y los criptosistemas para encontrar la clave de cifrado que se está utilizando.	Uso de algoritmos de cifrado fuertes, actualización regular de las claves de cifrado.

- **Capa de servicio:** La capa de servicio o de procesamiento de datos sirve como una capa intermedia entre la capa de aplicación y la capa de red en el sistema IoT. Esta capa comúnmente se encuentra compuesta por sistemas de cómputo y almacenamiento de gran capacidad, que incluyen unidades de procesamiento, almacenamiento de datos, unidades de procesamiento de inteligencia artificial (IA), entre otros. La capa de procesamiento de datos cumple un papel importante en la gestión y el análisis de los datos recopilados por los

dispositivos conectados. La seguridad en la nube y la seguridad de la base de datos son dos desafíos clave para los usuarios [26]. En la Tabla 6, se muestran los riesgos y vulnerabilidades encontrados en la capa de servicio, con sus respectivas medidas de seguridad.

Tabla 6. Riesgos y vulnerabilidades en la capa de servicio [26], [27].

Riesgos y vulnerabilidades	**Descripción**	**Mecanismos de seguridad**
Inyección de malware en la nube	El atacante puede tomar control de la máquina, de esta manera accede a datos sensibles almacenados en la máquina.	Escaneo y verificación de los archivos cargados en la nube en busca de malware.
Ataque de inyección SQL	El atacante emplea un segmento de código SQL para obtener acceso a información sensible que se encuentra almacenada en la base de datos.	Firewalls de aplicaciones web.
Ataque de inundación en la nube	El atacante envía con regularidad muchas solicitudes a la nube, lo que genera un impacto en la disponibilidad de los servidores.	Uso de servicios de mitigación de DDoS
Ataques de suplantación o pishing	El atacante puede realizar ataques de phishing para engañar a los usuarios y obtener credenciales de acceso a servicios IoT legítimos.	Autenticación de dos factores para el acceso a servicios en la nube.

- **Capa de aplicación:** La capa de aplicación es donde los usuarios finales interactúan directamente con los dispositivos conectados, proporcionando una amplia variedad de aplicaciones y servicios para diversas industrias. Esta capa es importante en la recopilación y presentación de datos, así como en la gestión de interacciones con los dispositivos IoT. Sin embargo, esta interacción directa entre el usuario y los dispositivos también presenta problemas de seguridad en la experiencia del usuario y en la integridad de los datos. La exposición de datos sensibles y los problemas de privacidad son las principales vulnerabilidades de esta capa [26]. En la Tabla 7, se muestran los riesgos y vulnerabilidades encontrados en la capa de aplicación, con sus respectivas medidas de seguridad.

Tabla 7. Riesgos y vulnerabilidades en la capa de aplicación [26], [27].

Riesgos y vulnerabilidades	Descripción	Mecanismos de seguridad
Ataque de denegación servicio distribuido (DDoS)	El atacante inunda intencionalmente la red o los servidores con numerosas solicitudes, de manera que los servicios se interrumpen y se vuelven inaccesibles para el usuario legítimo.	Implementar sistemas de detección, configurar cortafuegos, actualizar regularmente los sistemas.
Ataques de sniffing	El atacante utiliza programas o herramientas conocidas como "sniffers" para capturar los paquetes de datos que se transmiten mediante las aplicaciones IoT.	Protocolos de comunicación seguros, segmentación de la red, monitoreo del tráfico de red.
Uso de credenciales predeterminadas	Al adquirir dispositivos IoT, los nombres de usuario y contraseñas predefinidos pueden comprometer la privacidad de los datos almacenados.	Cambiar inmediatamente las contraseñas predeterminadas, implementar políticas de cambio de contraseñas regulares.
Cifrado de transporte de bajo nivel	Los dispositivos IoT pueden compartir credenciales sin cifrado a través de protocolos HTTP sin protección.	Protocolos de cifrados seguros, actualizaciones para los sistemas.
Virus y Gusanos	Son softwares pequeños e independientes que pueden replicarse e infectar otros ordenadores.	Técnicas de machine learning, actualizaciones de seguridad, análisis de canales laterales.
Scripts Maliciosos	Un atacante engaña al usuario de la puerta de enlace a Internet al visitar anuncios o sitios web atractivos y luego ejecuta scripts activos-x con modificaciones maliciosas.	Estadísticas y tendencias geométricas, Firewalls, control de acceso.
Programas espía y publicitarios	Los atacantes usan dispositivos IoT con contraseñas predeterminadas y vulnerabilidades para propagar malware.	Software de seguridad, instalación de antivirus.
Secuestro de Firmware	El firmware es una parte integral del hardware del sistema, y un daño a este componente permite a los atacantes tomar el control total del sistema.	Monitoreo y actualización del firmware, softwares de auditoría.
Ataque de contraseña por fuerza bruta	Es un método de búsqueda y descubrimiento para obtener acceso privilegiado, donde la atacante adivina posibles combinaciones de una contraseña hasta encontrar la correcta.	Políticas de bloqueo de cuentas después de intentos fallidos de acceso, autenticación de dos factores.

b. Protocolos de comunicación en sistemas IoT

La mitigación de ataques vulnerables en dispositivos IoT se puede lograr mediante la implementación de medidas de seguridad específicas. Según su comportamiento, estos ataques se pueden categorizar de la siguiente manera:

- Ataque de nivel bajo: Se produce cuando los intrusos atacan la red sin aplicar medidas de seguridad adecuadas.

- Ataque de nivel medio: Los intrusos interceptan el tráfico de red y alteran la integridad de los datos en tránsito.

- Ataque de nivel alto: Se produce cuando los intrusos acceden a la red y modifican tanto la intensidad de la comunicación como los datos originales.

- Ataque de nivel extremadamente alto: Se da cuando los intrusos intentan acceder a la red de forma no autorizada y realizan operaciones ilícitas que pueden resultar en la suspensión o falta de disponibilidad de la red debido a una posible congestión [28].

Los dispositivos IoT recurren a estándares y protocolos de red para habilitar la comunicación entre objetos físicos conectados a través de servicios en la nube. Estos protocolos y normativas de red representan conjuntos de políticas que establecen reglas definidas para el lenguaje de comunicación entre diversos dispositivos de red [29]. En la Figura 4, se presentan los protocolos de comunicación para la arquitectura IoT de cuatro capas.

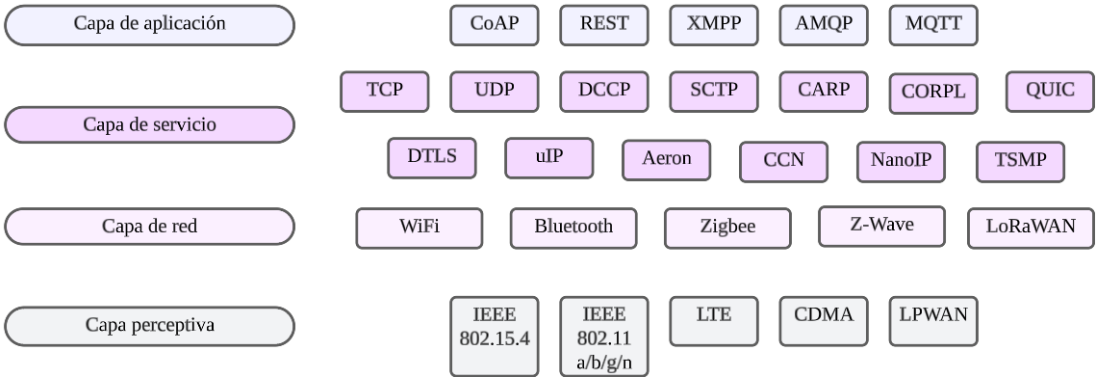


Figura 4. Protocolos de comunicación para la arquitectura IoT de cuatro capas [29].

Los protocolos de comunicación presentan sus propios riesgos y vulnerabilidades, por lo que es necesario implementar medidas de seguridad específicas que se adapten a las necesidades de cada capa de la arquitectura. En la Tabla 8, se detallan los principales riesgos y vulnerabilidades en los protocolos de comunicación en IoT, con sus respectivas medidas de seguridad.

Tabla 8. Riesgos y vulnerabilidades en protocolos de comunicación [28], [29].

Capa	Protocolo	Riesgos y vulnerabilidades	Mecanismos de seguridad
Capa Perceptiva	IEEE 802.15.4	Ataques (DoS), intercepción de datos	Autenticación y cifrado de datos
	IEEE 802.11 a/b/g/n	Ataques de fuerza bruta, robos de claves de cifrado.	Protocolos de cifrado (WPA, WPA2, WPA3)
	LPWAN	Comunicación sin cifrado	Cifrado de extremo a extremo
	CDMA	Intercepción de señales	Cifrado de señales
	Wi-Fi, LTE	Vulnerabilidades en la red, ataques de fuerza bruta	Autenticación de red, cifrado
Capa de Red	WiFi	Interceptación de datos, acceso no autorizado a la red	Autenticación, segmentación de red
	Bluetooth	Acceso no autorizado a dispositivos	Aplicación del protocolo DTLS
	Zigbee	Ataques de enrutamiento maliciosos	Autenticación, cifrado
	Z-Wave	Interceptación de señales, y acceso no autorizado	Cifrado y autenticación
	LoRaWAN	Exposición de datos privados	Control de acceso
Capa de servicios	TCP	Ataques de inundación, inyección de datos maliciosos	Cortafuegos, filtrado de paquetes
	UPD	Falta de garantías de entrega y verificación de origen	Autenticación y validación de datos
	DCCP	Posibles ataques de inundación	Autenticación y cifrado
	SCTP	Ataques de inundación secuestro de conexiones	Autenticación y cifrado
Capa de aplicación	CoAP	Ataques al tráfico de datos	Autenticación y cifrado
	REST	Falta de autenticación y autorización, ataques de inyección	Autenticación mediante tokens, uso de HTTPS
	XMPP	Amenazas de privacidad, ataques de denegación de servicio	Cifrado de extremo a extremo
	AMQP	Interceptación de mensajes, acceso no autorizado	Autenticación y cifrado de datos
	MQTT	Poca seguridad en las suscripciones, acceso no autorizado	Autenticación, autorización y control de acceso

c. Pruebas de seguridad en sistemas IoT

Las pruebas de seguridad en sistemas IoT son un componente fundamental para garantizar la integridad y el funcionamiento seguro de los dispositivos interconectados. Estas pruebas implican la evaluación y validación de las medidas de seguridad implementadas en dispositivos IoT, así como la identificación de posibles vulnerabilidades que puedan ser explotadas por posibles atacantes [6].

- ***Pruebas de penetración.*** Las pruebas de penetración, conocidas también como "pruebas de pen-testing", forman parte de las prácticas empleadas para evaluar sistemas informáticos, redes y aplicaciones web con el objetivo de descubrir vulnerabilidades que puedan ser objeto de explotación por parte de posibles atacantes. Este proceso se lleva a cabo mediante la recopilación de información sobre el objetivo del pen-testing, seguido por la identificación de posibles puntos de entrada o vulnerabilidades. A continuación, se realizan intentos de intrusión, tanto virtuales como en un entorno real, simulando ataques reales con el propósito de detectar fallos en la seguridad, y finalmente se obtiene la documentación y el reporte de los resultados obtenidos [6].

- ***Tipos de pruebas de penetración.*** En la evaluación de la seguridad de sistemas, se encuentran diversos tipos de pruebas de penetración, diseñados en función de las distintas necesidades y objetivos del evaluador [30]. En la Tabla 9, se muestran los principales tipos de pruebas de penetración.

Tabla 9. Tipos de pruebas de penetración [30].

Prueba de penetración	**Descripción**
Black Box Testing	Los evaluadores tienen un conocimiento limitado o nulo del sistema o red que se está probando, es decir, se recopila toda la información del objetivo.
White Box Testing	Los evaluadores tienen un conocimiento completo del sistema, incluyendo detalles internos y código fuente.
Gray Box Testing	Los evaluadores tienen un conocimiento parcial del sistema para una evaluación más específica sin requerir todos los detalles.

- ***Metodologías y estándares de pruebas de penetración.*** Son enfoques estructurados diseñados para evaluar la seguridad de sistemas y aplicaciones, estos proporcionan pautas y procesos para identificar y abordar vulnerabilidades. En la Tabla 10, se indican las principales metodologías y estándares utilizados en las pruebas de penetración para sistemas IoT.

Tabla 10. Metodologías y estándares de pruebas de penetración [31], [32].

Metodologías y estándares	Descripción
MIRE ATT&CK	Este marco que permite entender las tácticas, técnicas y procedimientos que los ciberdelincuentes emplean. Incluye diversas matrices que detallan cómo los atacantes se preparan, desde la recopilación de información hasta las técnicas de explotación y post-explotación.
NIST SP 800-115	Es un documento elaborado por Instituto NIST que proporciona una guía para la planificación y realización de pruebas de seguridad en la información, incluye aspectos como las pruebas de penetración, evaluación de seguridad de sistemas, aplicaciones y redes, así como evaluaciones de controles de seguridad.
OWASP Web Security Guide (WSTG)	La Guía de Pruebas de Seguridad Web OWASP es una referencia enfocada en la evaluación de aplicaciones web. Se encarga de estudiar las distintas fases de las pruebas de seguridad de aplicaciones web y explica los métodos de evaluación utilizados.
ISAF (Information Security Assessment Framework)	El marco ISSAF es una metodología de pruebas de penetración que se utiliza para evaluar la seguridad de los sistemas de información. Proporciona un enfoque estructurado para identificar y mitigar vulnerabilidades y riesgos de seguridad.
OSSTMM (Open-Source Security Testing Methodology Manual)	Es una guía enfocada en el diseño de pruebas de penetración y pretende evaluar la seguridad en sistemas y redes, se basa en estándares que permiten realizar evaluaciones de vulnerabilidades y pruebas de penetración según las necesidades tecnológicas y específicas de la organización.
PTES (Penetration Testing Execution Standard)	Es un estándar utilizado para llevar a cabo pruebas de penetración de manera efectiva. Se enfoca en todas las etapas de penetración, proporcionando una estructura y un conjunto de pauta que empiezan desde la planificación hasta la presentación de resultados y la mitigación de riesgos.
CIS Critical Security Controls	Es un estándar que establece diferentes controles críticos para la ciberseguridad, de tal manera que las organizaciones puedan mejorar su postura de seguridad.

1.4 Objetivos

1.4.1 Objetivo general

- Implementar soluciones de seguridad en sistemas IoT de hogares inteligentes para mitigar riesgos y vulnerabilidades mediante la realización de pruebas de penetración.

1.4.2 Objetivos específicos

- Identificar los principales riesgos, vulnerabilidades, medidas de seguridad y pruebas de penetración para los sistemas IoT utilizados en hogares inteligentes.
- Realizar pruebas de penetración para detectar brechas de seguridad en sistemas IoT.
- Aplicar medidas de seguridad en un sistema IoT para hogares inteligentes en un entorno controlado.
- Evaluar la efectividad y eficacia de las medidas implementadas para mitigar los riesgos y vulnerabilidades identificados.

CAPÍTULO II.- METODOLOGÍA

2.1 Materiales

Para llevar a cabo esta investigación, se seleccionaron diversos dispositivos IoT que se encuentran comúnmente en el entorno de un hogar inteligente. Entre estos dispositivos se incluyen luces, interruptores, enchufes, cámaras de seguridad, asistentes de voz como Alexa y sensores de movimiento. Estos elementos fueron utilizados para analizar y evaluar la resistencia del sistema IoT frente a posibles vulnerabilidades, mediante la realización de pruebas de penetración.

La aplicación de VMware Workstation permitió la virtualización de sistemas en una única estación de trabajo, facilitando la creación de entornos controlados. La distribución de Kali Linux proporcionó diversas herramientas diseñadas específicamente para pruebas de penetración y evaluaciones de vulnerabilidad. Además, la utilización de un adaptador USB 802.11, como el TP –Link Archer T2U Plus, permitió habilitar la conectividad inalámbrica en el entorno de pruebas y evaluar la seguridad en los dispositivos IoT.

2.2 Métodos

2.2.1 Modalidad de la investigación

A continuación, se detallan los distintos tipos de investigación que se aplicaron en el desarrollo del proyecto de investigación.

La investigación aplicada fue fundamental durante la implementación de los conocimientos teóricos adquiridos a través de diversas investigaciones, esto debido al diseño de un sistema IoT para un hogar inteligente en el cual se aplicaron las pruebas de penetración.

La investigación bibliográfica se basó la revisión y análisis de diversas fuentes de información relevantes, que incluyeron libros, artículos científicos, informes técnicos y documentos relacionados con la seguridad en sistemas IoT y hogares inteligentes.

La investigación de campo se llevó a través del análisis de un sistema IoT en un entorno doméstico real, lo que permitió recopilar datos sobre cómo funcionan los dispositivos IoT, cómo interactúan entre sí y cómo se integran en la vida cotidiana de los usuarios.

2.2.2 Recolección de información

En el proceso de recopilación de información, se utilizaron distintas fuentes de datos, que incluyeron repositorios de universidades tanto nacionales como internacionales, artículos, revistas y libros pertenecientes al campo de estudio. Además, se accedió a información técnica presente en bases de datos apropiadas.

2.2.3 Procesamiento y análisis de datos

Para el procesamiento y análisis de datos obtenidos a través de la investigación, se llevaron a cabo los siguientes pasos:

- Recopilación detallada de la información obtenida.
- Revisión de las propuestas de solución planteadas previamente en el campo de investigación.
- Análisis de los fundamentos teóricos y prácticos para el diseño de la investigación.
- Interpretación de la información más relevante que contribuya al desarrollo del proyecto de investigación.
- Aplicación de técnicas de análisis que permitan llevar a cabo la propuesta de solución.

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1 Parámetros para el desarrollo de la investigación

En el desarrollo de esta investigación, es necesario establecer ciertos parámetros que sirvan como guía para definir el alcance, la metodología y la evaluación de la efectividad de las pruebas de penetración y las medidas de seguridad. Estos parámetros son fundamentales para cada fase de la investigación:

- Identificar los límites de aplicación para la evaluación de seguridad en el sistema IoT.
- Determinar riesgos, vulnerabilidades y medidas de seguridad en sistemas IoT.
- Establecer una metodología adecuada para la recolección de datos, pruebas de penetración y la evaluación de medidas de seguridad.
- Identificar los recursos necesarios, como herramientas de análisis, software y hardware para llevar a cabo el estudio.
- Mantener un registro de los procesos, hallazgos y resultados obtenidos en la investigación.
- Realizar evaluaciones en el sistema que permitan establecer la efectividad de las medidas de seguridad implementadas.

3.2 Esquema General del Sistema

El objetivo principal de esta investigación es identificar y mitigar los riesgos y vulnerabilidades presentes en los sistemas IoT de hogares inteligentes mediante la aplicación de pruebas de penetración. La Figura 5, muestra el esquema utilizado para el desarrollo de esta investigación, indicando los componentes específicos del sistema y la relación entre cada uno de estos.

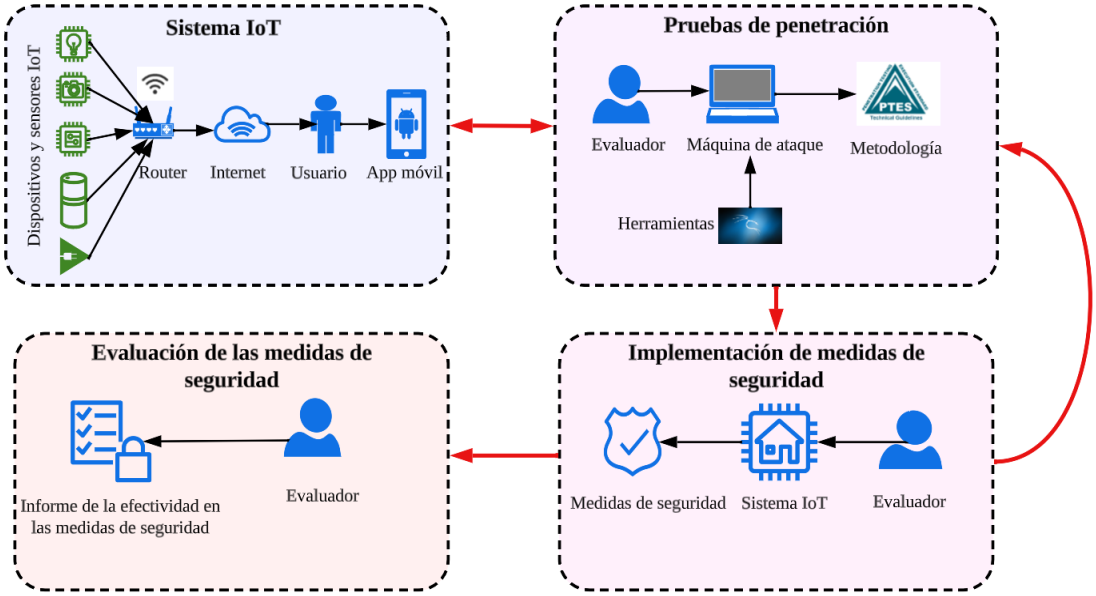


Figura 5. Diseño del esquema general del Sistema

Sistema IoT. El sistema IoT para hogares inteligentes está compuesto por diversos dispositivos y componentes, tales como interruptores, bombillas de luz, atenuadores de luz, sensores de movimiento, sensores de contacto, enchufes, cámaras y un asistente de voz “Alexa”. Además, se incorpora un router y la conexión a Internet. Este conjunto de dispositivos permite al usuario controlar el sistema mediante un dispositivo móvil.

Pruebas de penetración. El evaluador utiliza una máquina de Kali Linux, que está específicamente diseñada para la realización de ataques al sistema, ya que cuenta con un conjunto de herramientas especializadas en la ejecución de diversas pruebas. Además, se emplea una metodología de evaluación, como PTES, para el desarrollo de las pruebas de penetración.

Implementación de las medidas de seguridad. A partir de la realización de las pruebas de penetración, se implementan medidas de seguridad para mitigar los riesgos y vulnerabilidades identificados. Estas medidas implican configuraciones adicionales tanto en el router como en los dispositivos IoT del sistema y la utilización de herramientas para el control y monitoreo del tráfico de red.

Evaluación de las medidas de seguridad. A continuación, se realiza una evaluación minuciosa para verificar la efectividad y la eficiencia de las medidas de seguridad implementadas en el sistema. Los resultados obtenidos se documentan y sirven como base para investigaciones posteriores, garantizando un sistema más seguro y protegido.

3.3 Seguridad en Sistemas IoT de Hogares Inteligentes

El desarrollo de procedimientos y técnicas que garanticen la seguridad de hogares inteligentes considera diversos escenarios. Una gran cantidad de información confidencial y datos sensibles, como direcciones, ubicaciones, representaciones e información relacionada con la red se almacena en los dispositivos IoT. Esta información puede estar disponible para fabricantes, clientes, distribuidores intermediarios o comunidades, según sus derechos [33].

3.3.1 Limitaciones en la seguridad de los sistemas IoT

La aplicación de mecanismos de seguridad convencionales en redes o dispositivos IoT suele presentar desafíos debido a las limitaciones inherentes a estos dispositivos, que incluyen factores como:

- Restricciones en el hardware: limitaciones computacionales y energéticas, así como restricciones en la memoria y el acceso remoto.
- Restricciones en el software: limitaciones en el software integrado y la aplicación de parches de seguridad dinámicos que no son compatibles.
- Limitaciones de Red: consideraciones sobre movilidad, escalabilidad y diversidad en los medios de comunicación.

3.3.2 Requisitos de Seguridad en Dispositivos IoT

Los objetivos de seguridad establecidos para los dispositivos IoT, se basan en la confidencialidad, la integridad y la disponibilidad, y forman parte de la tríada CIA (Confidentiality, Integrity, Availability) [27]. Sin embargo, esta tríada puede resultar insuficiente para abordar las nuevas amenazas presentes en los dispositivos. Por lo tanto, existe un conjunto más completo de objetivos de seguridad denominado "octava de información, garantía y seguridad" (IAS-octave) [34]. La Tabla 11, detalla una breve descripción de estos requisitos de seguridad para los dispositivos IoT.

Tabla 11. Requisitos de seguridad en los dispositivos IoT [35], [34].

Requisitos de seguridad	Descripción
Confidencialidad	Es la capacidad de proteger la información sensible de los dispositivos para que solo las personas autorizadas tengan acceso a ellas.
Integridad	Se garantiza que los datos y comandos intercambiados entre los dispositivos IoT no se hayan alterado de manera no autorizada.
Disponibilidad	Los sistemas IoT, deben ser resistentes y estar disponibles en todo momento, incluso si ocurren problemas, tales como cortes de energía o fallos en los dispositivos.
No repudio	Es el procedimiento a través del cual un sistema IoT verifica la legitimidad y el origen de un evento, es decir, el sistema puede demostrar quien realizó una acción o un evento específico.
Privacidad	Es la protección de la información personal de los usuarios y la garantía de que se utilice de acuerdo con sus preferencias y consentimiento.
Auditoría	Es el proceso mediante el cual se da seguimiento y registro de las acciones ejecutadas por el sistema IoT.
Responsabilidad	Los usuarios y operadores de dispositivos IoT son legal y moralmente responsables de sus acciones en el entorno IoT.
Confianza	Un sistema IoT puede verificar la identidad de un individuo y establece confiabilidad en la seguridad del sistema.

3.3.3 Amenazas de seguridad en Hogares Inteligentes

Las amenazas son cualquier tipo de actividad destinada a comprometer la seguridad de un sistema de información, comprometiendo su funcionamiento normal, la integridad de los datos, o la confidencialidad de la información. En un hogar inteligente, estas amenazas pueden surgir de actividades maliciosas que afecten la red, los dispositivos y la información conectada en el entorno de automatización del hogar [36]. Las principales amenazas de seguridad que se pueden presentar en un hogar inteligente, se detallan en la Tabla 12.

Tabla 12. Amenazas de seguridad en Hogares Inteligentes [36].

Amenazas	Descripción del impacto a la red
Escuchas (Eavesdropping)	El atacante intercepta y escucha las comunicaciones entre dispositivos en el hogar inteligente, para obtener información confidencial.
Análisis del tráfico	El atacante observa y analiza los patrones de tráfico de datos entre los dispositivos y servicios, identifica tendencias e información sensible.
Denegación de servicio (DoS)	El atacante sobrecarga la red del hogar con un flujo masivo de tráfico falso o solicitudes, lo que provoca una saturación de los recursos de la red y limita el acceso de los usuarios legítimos a los servicios.
Nodo comprometido	El atacante captura y reprograma un nodo o dispositivo legítimo de la red del hogar inteligente, para ser utilizado en ataques adicionales.
Agujero de gusano	Un nodo malicioso manipula la información de enrutamiento en la red para atraer paquetes de datos hacia sí mismo.

Amenazas	Descripción del impacto a la red
Ataque físico	El atacante obtiene acceso a los dispositivos o sensores del hogar inteligente, lo que le permite realizar ataques directos.
Ataque de suplantación	El atacante se hace pasar por un usuario legítimo o un dispositivo autorizado dentro de la red del hogar inteligente.
Ataque de repetición	El atacante captura mensajes previamente transmitidos entre dos partes y los reenvía, para que la red los analice como una entidad autorizada.
Modificación de mensaje	El atacante altera el contenido de los mensajes en tránsito, lo que implica la reordenación o el retraso de mensajes para manipular la red.
Ataque de intercepción	El atacante intercepta paquetes de datos que se envían desde el hogar inteligente a un usuario remoto.
Ataque de robo de sesión	El atacante espera a que un usuario o dispositivo se autentique y luego suplanta su identidad, tomando el control de la sesión autenticada.
Código malicioso	Los códigos maliciosos, como virus, gusanos o troyanos, se introducen en la red del hogar y explotan las vulnerabilidades en los dispositivos.

3.3.4 Identificación de riesgos y vulnerabilidades

Los riesgos y vulnerabilidades son elementos que pueden comprometer la integridad, confidencialidad y disponibilidad de los dispositivos conectados. Los riesgos son eventos o circunstancias que podrían tener un impacto negativo en la seguridad de los sistemas IoT, mientras que las vulnerabilidades son debilidades específicas que podrían ser explotadas para comprometer la seguridad. La información de los principales riesgos y vulnerabilidades en dispositivos IoT para el hogar, se detalla en la Tabla 13.

Tabla 13. Riesgos y vulnerabilidades en dispositivos IoT [37], [38].

Riesgos y vulnerabilidades en dispositivos IoT	
Contraseñas débiles	Es el uso de contraseñas que son fáciles de adivinar o que están codificadas de una manera muy predecible. Además, se presenta el uso de credenciales que son públicamente conocidas.
Servicios en la red inseguros	Son aquellos servicios que se ejecutan en el dispositivo en sí y están expuestos a Internet, pueden comprometer la confidencialidad, integridad o autenticidad de la información.
Interfaces en Ecosistemas Inseguros	Son las interfaces web, servicios en la nube, o aplicaciones móviles que se encuentran fuera del dispositivo, pero se relacionan con él, son inseguras si carecen de autenticación y autorización adecuadas.
Falta de mecanismos de actualizaciones seguras	Es la incapacidad de actualizar el dispositivo de manera segura, puede incluir la falta de validación de firmware en el dispositivo o de notificaciones sobre cambios de seguridad y actualizaciones.
Componentes inseguros o desactualizados	El uso de componentes o bibliotecas de software que están obsoletos o son inseguros, estos componentes podrían permitir que el dispositivo sea comprometido.
Protección insuficiente de la privacidad	La información personal del usuario que se almacena en el dispositivo o sistema IoT, pero se utiliza de manera insegura, incorrecta o sin el permiso adecuado.

Riesgos y vulnerabilidades en dispositivos IoT	
Transferencia y almacenamiento de datos	Es la falta de cifrado o control de acceso para datos sensibles en cualquier parte del sistema, ya sea que se encuentre en reposo o en ejecución.
Falta de gestión de dispositivos	Es la falta de soporte de seguridad en los dispositivos que se encuentran en el mercado de producción, esto incluye la gestión de activos, la gestión de actualizaciones, la supervisión de sistemas y la capacidad de respuesta.
Configuraciones predeterminadas inseguras	Son dispositivos o sistemas que se envían con configuraciones predeterminadas inseguras o que no permiten que los operadores restrinjan la modificación de configuraciones para que el sistema sea más seguro.
Inadecuada protección física	Es la insuficiente protección física de los dispositivos, como la falta de control en el acceso no autorizado y la poca resistencia contra ciertas condiciones ambientales.
Parámetros y características de seguridad que no pueden modificarse	Son elementos de la configuración de los dispositivos que no pueden ser alterados o mejorados, lo que deja expuesto el sistema a posibles ataques.
Presencia de puertas traseras o backdoors	Son accesos no autorizados que le permiten a los atacantes una entrada oculta al sistema, por lo que podrían obtener control sobre los dispositivos y comprometer la privacidad de los usuarios.

3.3.5 Medidas de seguridad en Sistemas IoT de Hogares Inteligentes

A partir del análisis previo de las diversas técnicas y medidas de seguridad que pueden aplicarse en una arquitectura IoT, es necesario identificar aquellas que resultan más necesarias en la protección de sistemas IoT de hogares inteligentes. Sin embargo, es importante recordar que ninguna medida de seguridad es completamente eficiente por sí sola. Por lo tanto, en la Tabla 14, se presentan recomendaciones de seguridad que los usuarios y propietarios de hogares inteligentes pueden considerar para mejorar la protección de sus dispositivos IoT y mantener la privacidad de su hogar.

Tabla 14. Medidas de seguridad aplicadas en sistemas IoT de Hogares Inteligentes.

Medidas de seguridad	Descripción
Configurar el enrutador correctamente	El enrutador es el elemento central que conecta todos los dispositivos IoT, por lo tanto, es necesario aplicar ciertas medidas como cambiar el nombre o la contraseña predeterminada, y usar un nivel alto de encriptación.
Contraseñas fuertes	Se recomienda crear credenciales únicas para la cuenta y la aplicación de cada dispositivo IoT. Esto garantiza que, si la contraseña de un dispositivo se ve comprometida, los demás sigan siendo seguros.
Crear una red Wi-Fi secundaria	A partir de la creación de una red separada dedicada a los dispositivos IoT, se puede proteger la red principal contra las amenazas IoT.
Mantener los dispositivos actualizados	Las actualizaciones del firmware en el enrutador Wi-FI en ocasiones no se ejecutan automáticamente, por lo tanto, es necesario hacer una verificación manual en el sistema cada cierto tiempo.
Autenticación de múltiples factores	La identificación de múltiples factores, en la mayoría de los casos son dos, es una capa adicional de seguridad en el sistema.

3.3.6 Aplicación de una metodología para las pruebas de penetración

A partir de la investigación bibliográfica previamente realizada, se determina que la metodología más apropiada para llevar a cabo las pruebas de penetración correspondientes es la Penetration Testing Execution Standard (PTES). La elección de esta metodología se basa en su enfoque sistemático y completo para evaluar la diversidad de dispositivos interconectados en un sistema determinado. Las siete etapas principales que conforman la base de esta metodología, se muestran en la Figura 6.

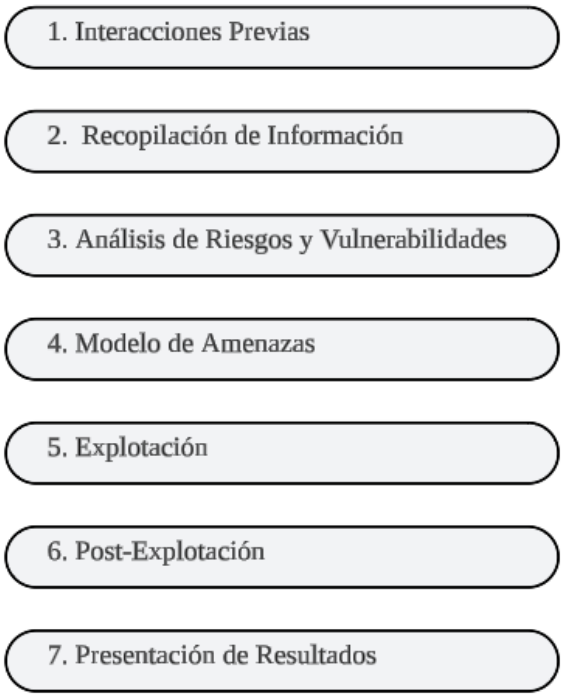


Figura 6. Etapas de la metodología (Penetration Testing Execution Standard) [37].

La aplicación de las siete etapas de PTES en una investigación de seguridad para un sistema IoT de un hogar inteligente es esencial para asegurar la protección de estos entornos. La aplicación de cada etapa de PTES en el contexto de esta investigación, se detalla en la Tabla 15.

Tabla 15. Etapas PTES en las pruebas de penetración para sistemas IoT de Hogares Inteligentes

Etapas PTES	Aplicación en la investigación
Interacciones Previas	Se realiza el diseño de un sistema IoT para un hogar inteligente, lo cual implica identificar los dispositivos IoT que serán sometidos a las pruebas de penetración.
Recopilación de Información	Se utilizan herramientas de escaneo para obtener información detallada acerca de los dispositivos IoT de la red del hogar, para obtener datos específicos sobre cada dispositivo.
Análisis de Riesgos y Vulnerabilidades	Se emplean herramientas y metodologías específicas para identificar vulnerabilidades en los dispositivos IoT, como la detección de debilidades en la autenticación y configuraciones incorrectas.
Modelo de Amenazas	Se establece un marco específico para identificar y comprender las posibles amenazas que puedan afectar a los dispositivos IoT en el hogar inteligente.
Explotación	Se realiza la explotación de las vulnerabilidades identificadas para comprender su alcance y las posibles implicaciones de seguridad para el hogar inteligente.
Post-Explotación	A partir de los resultados obtenidos previamente, se implementan medidas de seguridad para mitigar los riesgos identificados y se aplican cambios que fortalezcan la protección de entorno.
Presentación de Resultados	Por último, en esta etapa se lleva a cabo una evaluación de la efectividad de las medidas de seguridad implementadas, evidenciando la mitigación de las vulnerabilidades previamente identificadas.

3.4 Diseño de un sistema IoT para un Hogar Inteligente

La primera etapa se basa en el diseño práctico de un sistema IoT para un entorno doméstico. Esta aplicación proporciona una mejor comprensión de la seguridad, el funcionamiento y las experiencias de los usuarios. Además, muestra las potenciales vulnerabilidades y amenazas de estos dispositivos.

3.4.1 Selección y ubicación de los dispositivos IoT en el sistema

Para comprender mejor la seguridad en sistemas IoT, es necesario explorar una variedad de dispositivos IoT comúnmente utilizados en un hogar típico. En este sistema, se consideraron dispositivos de iluminación, como interruptores, bombillas y módulos atenuadores de luz; dispositivos de seguridad y vigilancia, como sensores de movimiento y de contacto; además de tomacorrientes, y un parlante de voz para que el usuario se comunique con estos dispositivos. Los dispositivos IoT se presentan en la Figura 7. Además, en el Anexo A se proporciona información del datasheet de cada uno de los dispositivos IoT.

Figura 7. Dispositivos IoT para el diseño del sistema

Los dispositivos IoT implementados cumplen con características y especificaciones técnicas propias. Las especificaciones acerca del tipo, marca, cantidad de dispositivos utilizados y protocolos de comunicación, se detallan en la Tabla 16.

Tabla 16. Especificaciones de los dispositivos IoT implementados.

No.	Tipo	Dispositivo	Marca	Cantidad	Protocolos de Comunicación
1	Iluminación	Interruptor de luz inteligente	Tuya	1	Wi-Fi (IEEE 802.11n), ZigBee
2	Iluminación	Bombilla LED inteligente color blanco	Nexxt Solutions	2	Wi-Fi (IEEE 802.11n)
	Iluminación	Bombilla LED inteligente de colores	Tuya	1	Wi-Fi (IEEE 802.11n)
3	Iluminación	Módulo WiFi regulador para luces	Tuya	1	Wi-Fi (IEEE 802.11g)
4	Parlante de Voz	Echo Dot Alexa	Amazon	1	Wi-Fi (IEEE 802.11n), Bluetooth
5	Seguridad y vigilancia	Detector de movimiento PIR con alarma	Tuya	1	Wi-Fi (IEEE 802.11b)
6	Seguridad y vigilancia	Sensor de contacto para puertas y ventana	Tuya	2	Wi-Fi (IEEE 802.11b/g)
7	Seguridad y vigilancia	Cámara inteligente para interiores	Nexxt Solutions	1	Wi-Fi (IEEE 802.11b/g)
8	Tomacorriente	Enchufe inteligente	Nexxt Solutions	1	Wi-Fi (IEEE 802.11n)

El desarrollo de un sistema IoT en un hogar inteligente implica la planificación e implementación de dispositivos, según las necesidades de los residentes. Para su distribución, se consideraron factores como la funcionalidad, la cobertura de red y la

comodidad del usuario. A continuación, se detalla la ubicación y función de los dispositivos en la primera y segunda planta del hogar.

Primera Planta:

- Sensor de contacto: Instalado en el marco de la ventana cercana a la puerta principal, detecta cualquier intento de acceso al hogar a través de este medio.
- Sensor detector de movimiento PIR con alarma: Colocado en la parte baja de la pared cercana a la puerta principal, identifica posibles movimientos cuando no hay residentes en el hogar.
- Interruptor de luz inteligente: Ubicado para controlar la iluminación de la sala y el comedor, permite al usuario un acceso fácil y directo al control de la luz.
- Enchufe inteligente: Conectado a la corriente en la zona del comedor, facilita la conexión de dispositivos electrónicos como laptops o teléfonos móviles, permitiendo al usuario controlar su conexión a la energía según sus necesidades.
- Bombilla LED inteligente de colores: Ubicada en la cocina, se encarga de iluminar el área de manera efectiva y proporciona la luz necesaria para realizar tareas culinarias.
- Módulo regulador para luces: Situado en la zona de estudio, tiene la capacidad de variar la intensidad y el tono de la luz, adaptándose a diversas necesidades de iluminación.
- Cámara inteligente para interiores: Orientada hacia la puerta principal, vigila y monitorea cualquier actividad o presencia inusual en hogar.

Segunda Planta:

- Bombillas LED inteligentes con ajuste color blanco: Colocadas en las habitaciones utilizadas regularmente, el dormitorio principal y el dormitorio denominado Isa, un acceso fácil y directo para el control de la luz.
- Sensor de contacto: Instalado en el marco de la ventana del dormitorio de invitados, registra cualquier intento de acceso al hogar por este medio.

- Echo Dot Alexa: Ubicado en el dormitorio, este parlante permite el control y monitoreo de todos los dispositivos del hogar mediante comandos de voz.

La ubicación estratégica de estos dispositivos busca optimizar la funcionalidad y seguridad del hogar. La representación visual de esta disposición, se presenta en la Figura 8.

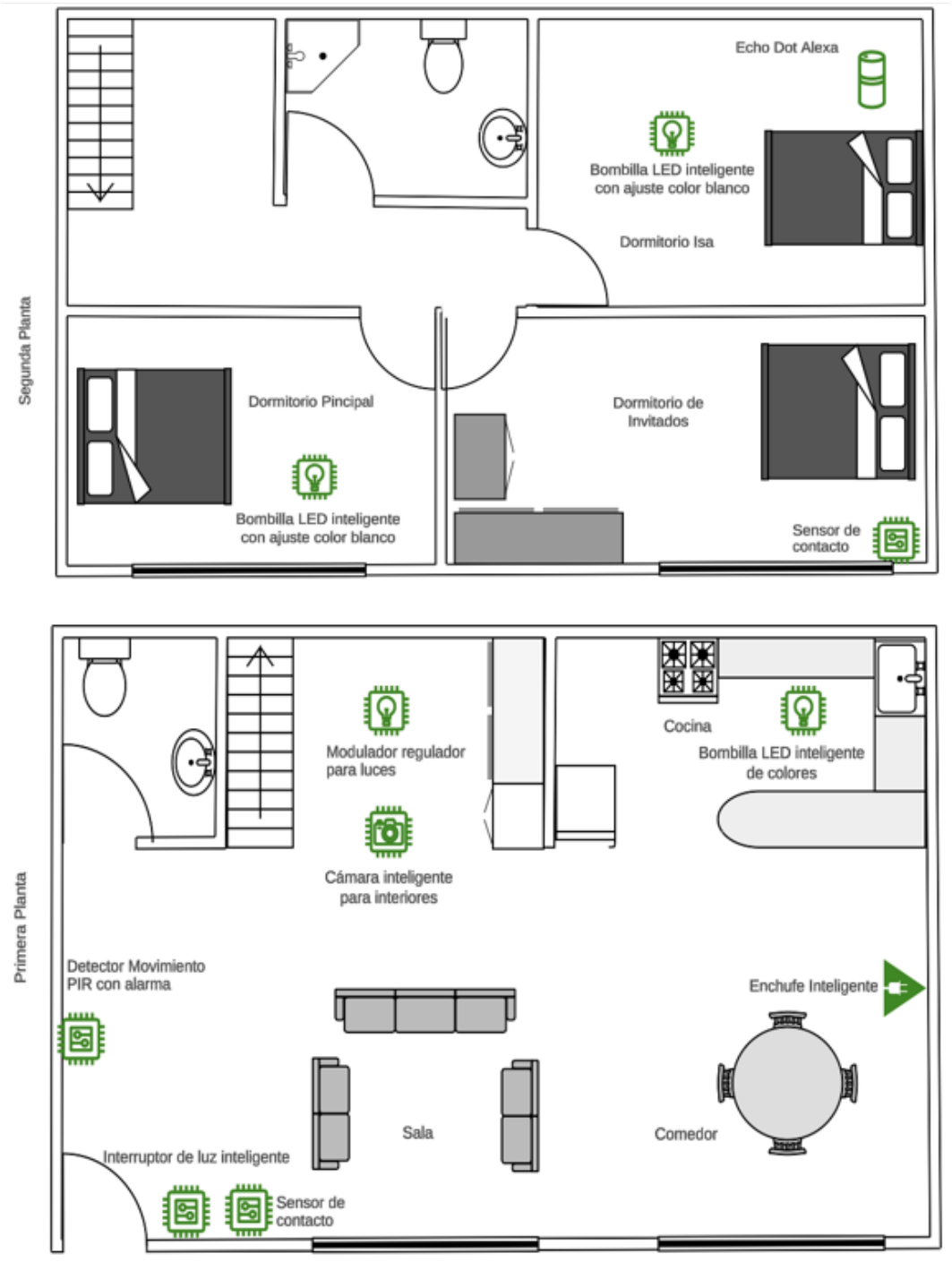


Figura 8. Distribución de los dispositivos IoT en el hogar inteligente

3.4.2 Información Técnica de los dispositivos

La gestión adecuada de un sistema IoT en un hogar inteligente requiere información técnica precisa sobre los dispositivos conectados. Esta información incluye elementos importantes como el nombre y modelo del dispositivo, el fabricante responsable de su producción, y su dirección MAC única, como se muestra en la Tabla 17.

Tabla 17. Parámetros técnicos de los dispositivos IoT.

Dispositivo	Modelo	Fabricante	Dirección MAC
Interruptor de luz inteligente	Smart Light Switch	Tuya Smart Inc.	FC:67:1F:D8:CA:35
Bombilla LED inteligente de colores	Smart Wi-Fi LED Color bulb	Beken Company	C8:47:8C:30:B8:28
Bombilla LED inteligente color blanco	Smart Wi-Fi LED Tunable White bulb	Espressif Inc.	24:62:AB:37:37:92
Bombilla LED inteligente color blanco	Smart Wi-Fi LED Tunable White bulb	Espressif Inc.	24:62:AB:32:D7:57
Módulo regulador para luces	WiFi Dimmer Module for Lights	Tuya Smart Inc.	38:1F:8D:E3:BD:98
Parlante de voz Echo Dot Alexa	Echo Dot Alexa 5ta gen.	Amazon Technologies Inc.	7C:ED:C6:D9:06:8E
Detector de movimiento PIR con alarma	PIR MOTION DETECTOR ALARM	Tuya Smart Inc.	82:91:64:14:3C:9B
Sensor de contacto para puertas y ventanas	Wi-Fi Door Window Sensor	Intel Corporate	FC:67:1F:7B:64:92
Sensor de contacto para puertas y ventanas	Wi-Fi Door Window Sensor	Intel Corporate	FC:67:1F:7B:5C:A3
Cámara inteligente para interiores	Smart Wi-Fi Camera Indoor	Espressif Inc.	A0:92:08:99:CE:7D
Enchufe inteligente	Smart Wi-Fi Plug	Espressif Inc.	FC:67:1F:F9:C2:D1
Router	F660	ZTE	9A:00:6A:93:D9:5C
Dispositivo Móvil	Samsung Galaxy S20 FE 5G	Samsung	9E:B1:D3:2F:03:C0

Actualmente, los dispositivos IoT se encuentran configurados con el protocolo DCHP, lo que indica que las direcciones IP se asignan automáticamente a los dispositivos. Este cambio dinámico de las direcciones IP, puede dificultar el seguimiento de los dispositivos en la red.

3.4.3 Configuración y comunicación en la red de los dispositivos IoT

En la implementación de un sistema IoT en un hogar, uno de los principales pasos es la configuración y comunicación de los dispositivos en la red. Después de ubicar estratégicamente estos dispositivos en el entorno doméstico, se procedió a conectarlos a la red local. La Figura 9 presenta el esquema de red utilizado, indicando que la topología seleccionada para esta configuración específica es la topología estrella. Este enfoque, donde cada dispositivo se conecta directamente a un punto central, facilita la gestión y comunicación eficiente entre los dispositivos IoT del hogar.

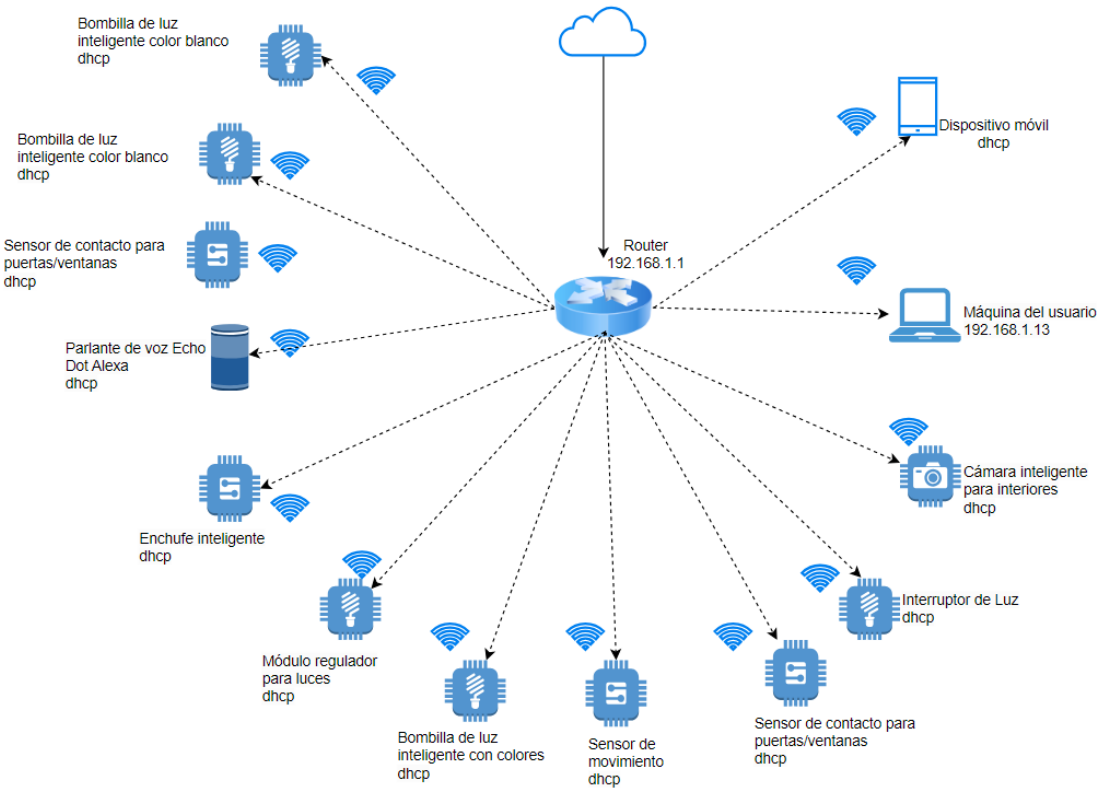


Figura 9. Esquema de red del sistema IoT

Además, la configuración de los dispositivos IoT mediante las aplicaciones móviles del usuario permitirá establecer una conexión efectiva y sincronizada entre los dispositivos y la red local. A través de las interfaces intuitivas de las aplicaciones móviles diseñadas para diferentes grupos de dispositivos IoT, el usuario podrá personalizar y ajustar las configuraciones, según sus requerimientos.

a. Aplicación Nexxt Home

Se realizó la descarga de la aplicación NexxtHome desde la Play Store, y a continuación, se completó el registro y activación de la cuenta mediante un correo electrónico. Posteriormente, se añadió cada uno de los dispositivos Nexxt Solutions mediante la configuración de la aplicación, como se muestra en la Figura 10.

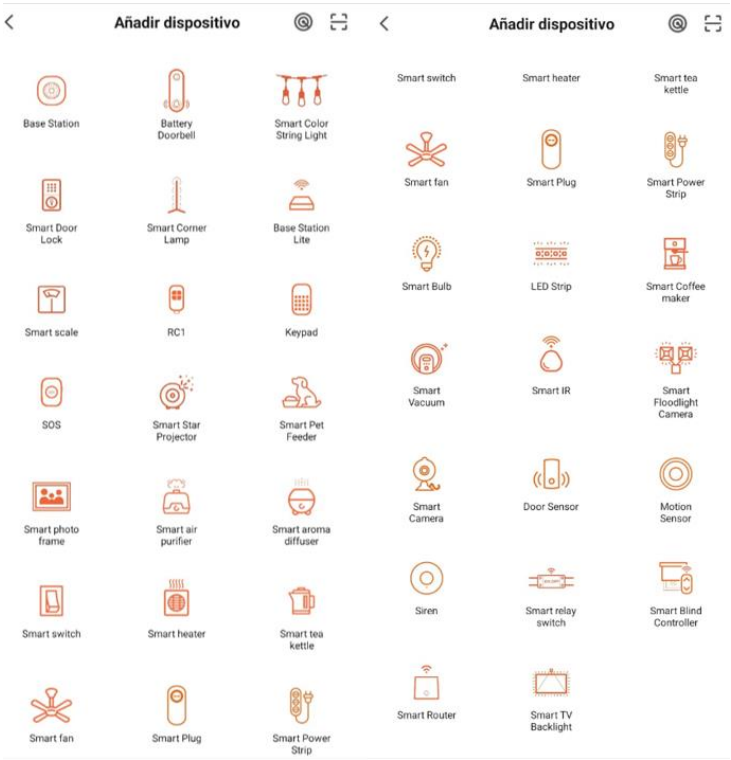


Figura 10. Vinculación de los dispositivos Nexxt Solutions

Una vez que se han agregado los dispositivos correspondientes, es posible realizar su monitoreo y control mediante el menú principal de la aplicación, como se muestra en la Figura 11.

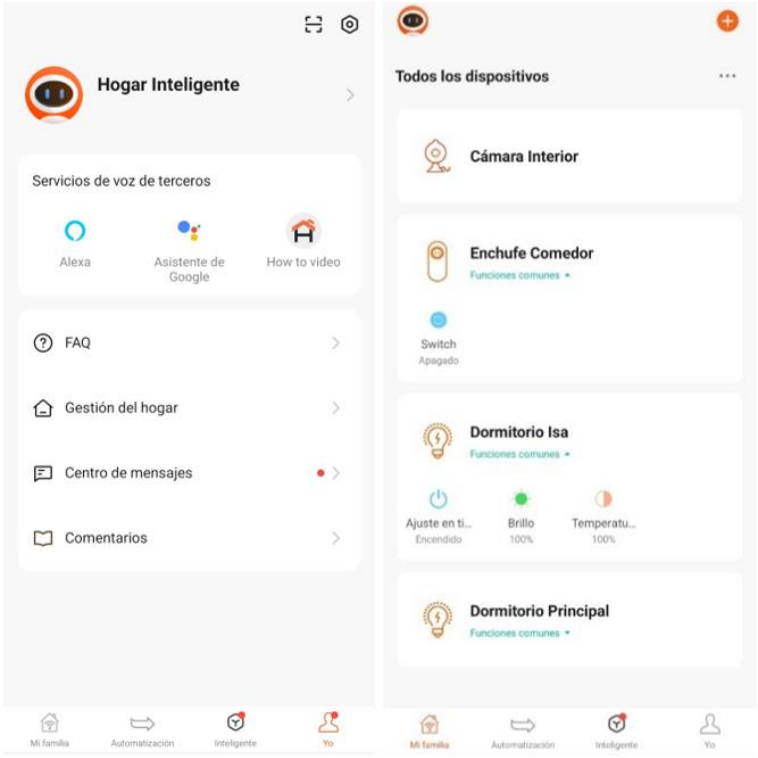


Figura 11. Monitoreo y control de los dispositivos IoT en NexxtHome

b. Aplicación Smart Life

A continuación, se llevó a cabo un procedimiento similar para vincular los dispositivos de la marca TUYA en la aplicación Smart Life. La descarga de la aplicación se realizó mediante Play Store y se completó el registro y activación de cuenta mediante un correo electrónico. Se añadió cada uno de los dispositivos TUYA mediante la configuración de la aplicación, como se muestra en la Figura 12.

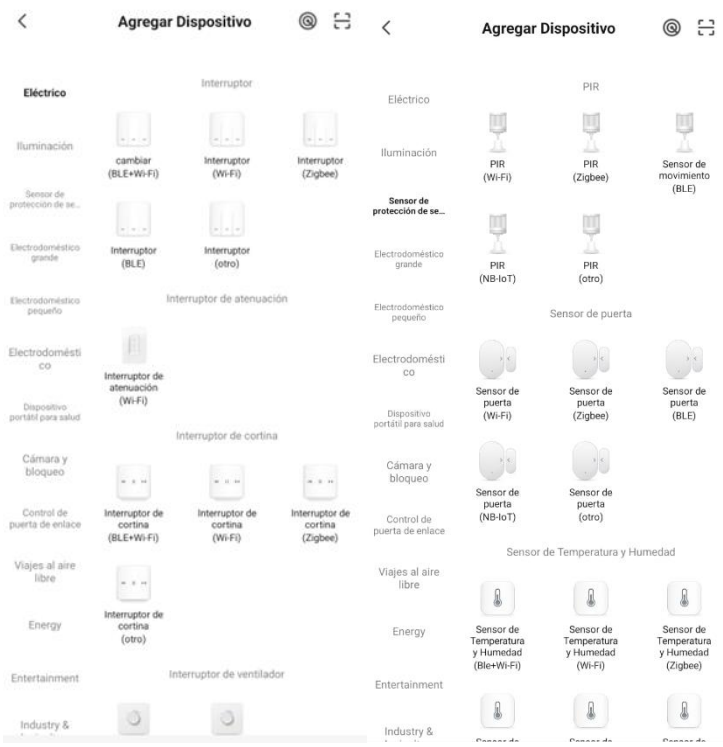


Figura 12. Vinculación de los dispositivos TUYA

De la misma manera, una vez agregados los dispositivos correspondientes, es posible realizar su monitoreo y control mediante el menú principal de la aplicación, como se muestra en la Figura 13.

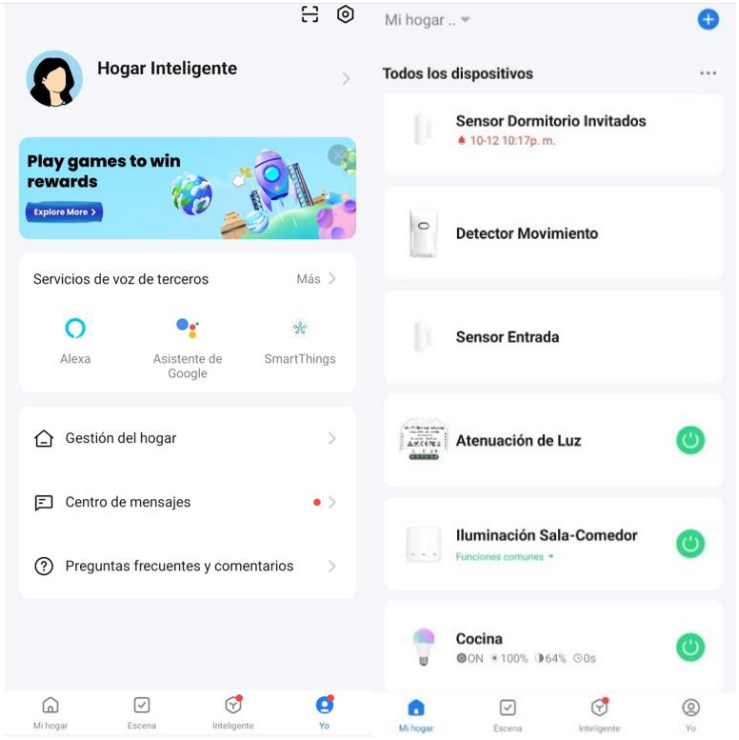


Figura 13. Monitoreo y control de los dispositivos IoT en SmartLife

c. Aplicación Amazon Alexa

Por último, se realizó la instalación y la configuración de la aplicación Amazon Alexa en el dispositivo móvil para el funcionamiento del parlante Echo Dot. Además del registro del usuario mediante correo electrónico, esta aplicación requirió la activación de las funciones de bluetooth y ubicación en el móvil, lo que permitió que el parlante detectara los dispositivos inteligentes cercanos. La Figura 14 muestra todos los dispositivos inteligentes conectados a la red local.

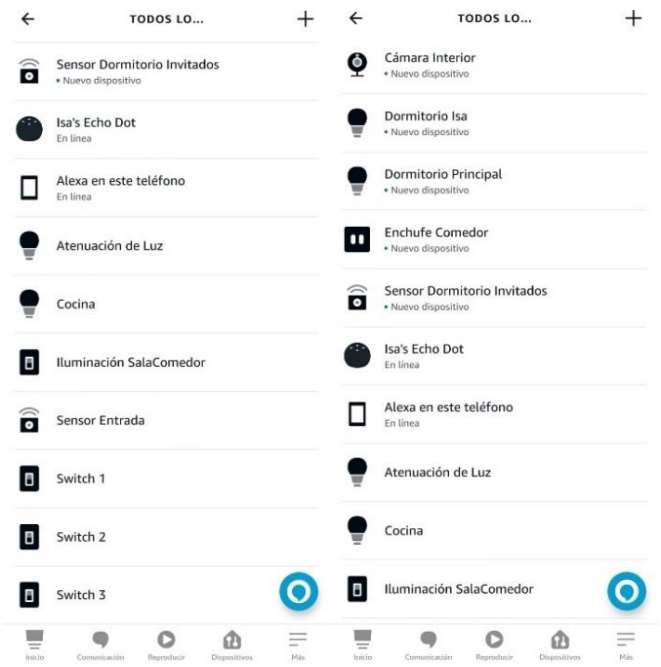


Figura 14. Vinculación de los dispositivos IoT en Amazon Alexa

Por lo tanto, el parlante Echo Dot junto con la aplicación Alexa, funciona como un dispositivo central que permite la comunicación entre distintos dispositivos IoT compatibles. Esto se logra a través de comandos de voz o la aplicación asociada, lo que permite la ejecución de diversas tareas, según las necesidades del usuario.

3.4.4 Verificación y autenticación de datos en el Sistema IoT

Los dispositivos implementados en el sistema IoT cumplen una serie de parámetros esenciales, que incluyen el acceso a la red, la eficacia en la comunicación y la compatibilidad con otras aplicaciones del sistema. Esto permite la posibilidad de que los usuarios gestionen los dispositivos según sus requerimientos y rutinas individuales.

La Tabla 18 muestra el cumplimiento de estos parámetros para cada dispositivo IoT perteneciente al sistema.

Tabla 18. Verificación y autenticación de datos en el sistema IoT.

Aplicación	Dispositivo	Acceso a la red	Comunicación	Compatibilidad
Nexxt Home	Smart Wi-Fi Plug	✓	✓	✓
	Smart Wi-Fi LED Tunable White bulb	✓	✓	✓
	Smart Wi-Fi Camera Indoor	✓	✓	✓
Smart Life	Smart Light Switch	✓	✓	✓
	Smart Wi-Fi LED Color bulb	✓	✓	✓
	WiFi Dimmer Module for Lights	✓	✓	✓
Smart Life	Pir Motion Detector Alarm	✓	✓	✓
	Wi-Fi Door Window Sensor	✓	✓	✓
Amazon Alexa	Echo Dot Alexa 5ta gen.	✓	✓	✓

3.5 Pruebas de penetración en el sistema IoT

3.5.1 Recopilación de Información

La información referente a la dirección de red y la máscara se basa en la configuración del router que se encuentra conectado a la red doméstica, este funciona como punto central de la red y se encarga de asignar las direcciones IP a los dispositivos mediante DHCP. La dirección de red y la máscara se utilizan para definir el rango de direcciones IP disponibles en la red y asegurar que los dispositivos puedan comunicarse entre sí. En la Figura 15, se presenta la información de la red doméstica, obtenida a través el comando `ipconfig`. En donde se identifica que la dirección IP de la máquina es `192.168.1.13`, y la máscara de subred correspondiente es `255.255.255.192`.

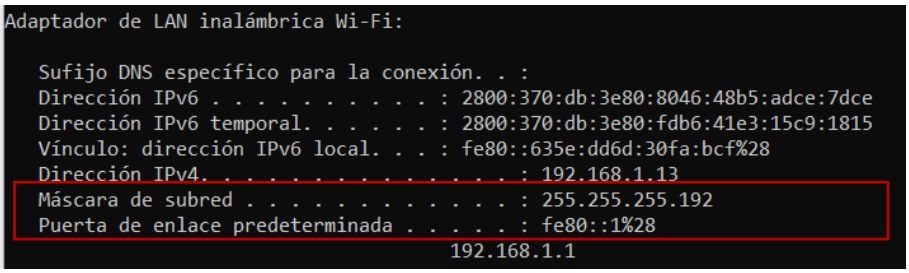


Figura 15. Información de la red doméstica.

Por lo tanto, la asignación de direcciones IP para los dispositivos IoT del hogar inteligente se encuentra comprendido entre `192.168.1.0` y `192.168.1.63`. Esta configuración de red delimitada asegura que los dispositivos dentro de la red doméstica inteligente cuenten con direcciones IP que se ajusten al rango predefinido, facilitando la identificación y administración de los dispositivos IoT en la red.

En la gestión de dispositivos IoT en una red determinada, el empleo de herramientas enfocadas en recopilar información permite ofrecer una comprensión detallada del funcionamiento de los dispositivos interconectados. La Tabla 19 realiza un análisis de distintas herramientas utilizadas con este propósito, con la finalidad de identificar y seleccionar aquellas que sean más apropiadas para la recopilación de información en el sistema IoT.

Tabla 19. Herramientas para recopilar información de los dispositivos IoT [39]-[40].

Especificaciones	**Wireshark**	**Advanced IP Scanner**	**Lansweeper**	**Kismet**	**NetStumbler**
Soporte de protocolos	TCP, UPD, ICMP, etc.	TCP, UPD, ICMP, etc.	TCP, UPD, ICMP, etc.	802.11 a/b/g/n/ac	802.11 a/b/g/n/ac
Interfaz Gráfica	Sí	Sí	Sí	No	No
Captura de paquetes	Sí	No	No	Sí	No
Análisis de Tráfico	Sí	No	No	Sí	No
Inyección de paquetes	Sí	Sí	No	Sí	Sí
Escaneo de dispositivos	No	Sí	Sí	Sí	Sí
Identificación de dispositivos	Sí	Sí	Sí	Sí	No
Análisis de seguridad	Sí	No	No	Sí	No
Capacidad de monitoreo	Sí	No	No	Sí	No
Escaneo de puertos	Sí	Sí	No	No	No
Detección de vulnerabilidades	Sí	Sí	No	Sí	Sí
Escaneo de Red	Sí	Sí	Sí	Sí	Sí
Plataformas Disponibles	Windows, Linux, macOS	Windows	Windows, Linux, macOS	Linux	Windows
Aplicaciones	Análisis de paquetes, inyección de paquetes.	Escaneo e identificación de puertos, detección de vulnerabilidades.	Escaneo de activos, inventario de software.	Detección de protocolos inalámbricos, análisis de paquetes.	Detección de protocolos inalámbricas, análisis de paquetes.

En esta comparativa, se destacan tres herramientas fundamentales que abordan distintos aspectos de la seguridad y el análisis de redes: Wireshark, por su capacidad para realizar análisis del tráfico y actividad de los dispositivos en la red; Advanced IP Scanner, útil en el mapeo y descubrimiento de dispositivos, facilitando la identificación de los dispositivos conectados a la red; y Kismet, específicamente diseñada para la detección de redes inalámbricas, permitiendo un monitoreo detallado y específico de las señales Wi-Fi en un entorno determinado. La instalación y configuración de las herramientas que no están predefinidas en el entorno de pruebas se detallan en el Anexo C.

a. Wireshark

A través de Wireshark, se obtuvo información del tráfico de paquetes dentro de la red, incluyendo un análisis del envío de datos entre los dispositivos del sistema IoT. La Figura 16 muestra el tráfico de datos capturados en la red, lo que permitió identificar la interacción de los dispositivos IoT.

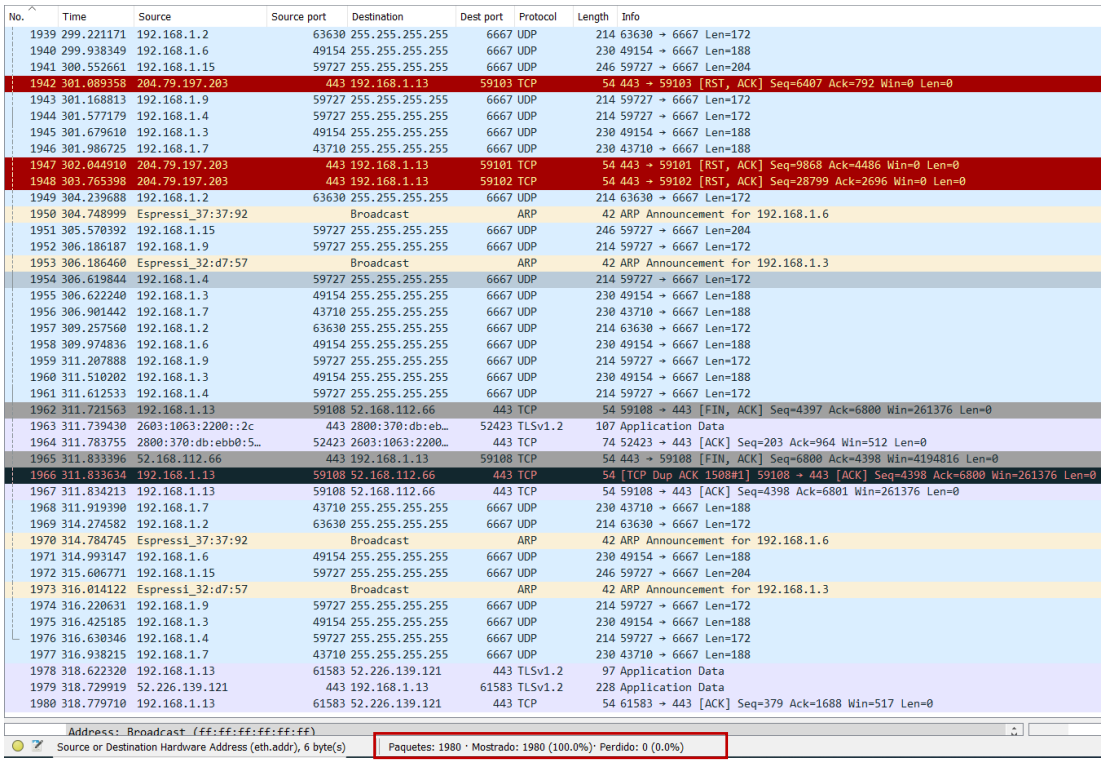
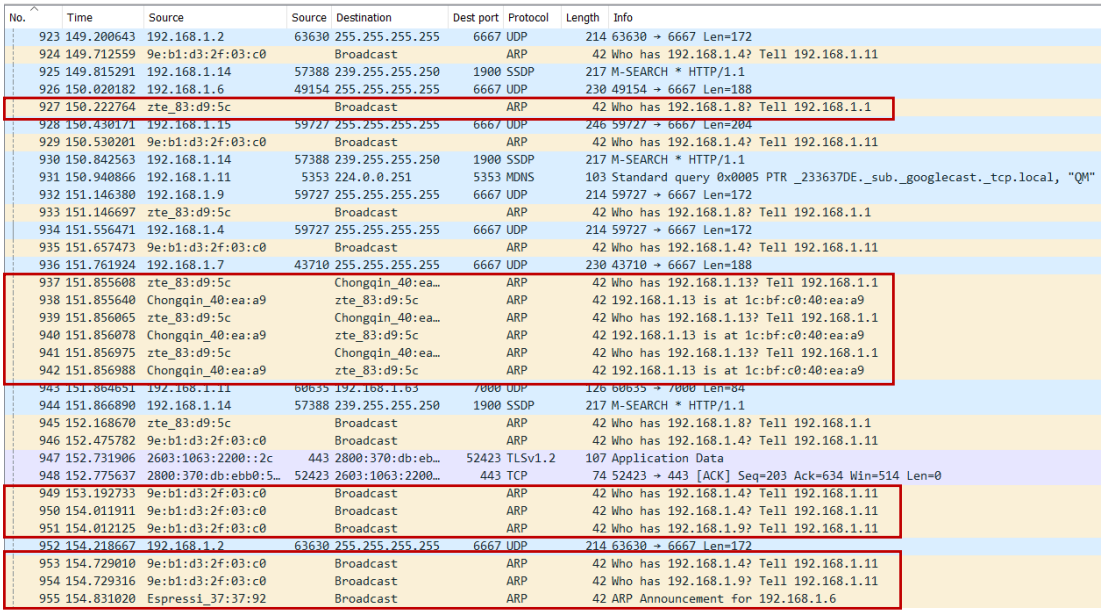


Figura 16. Análisis del tráfico de datos en la red con Wireshark.

Durante la captura de paquetes, se identificó el tráfico generado en la red al utilizar el dispositivo móvil para controlar el sistema IoT. Estos datos indican cómo la

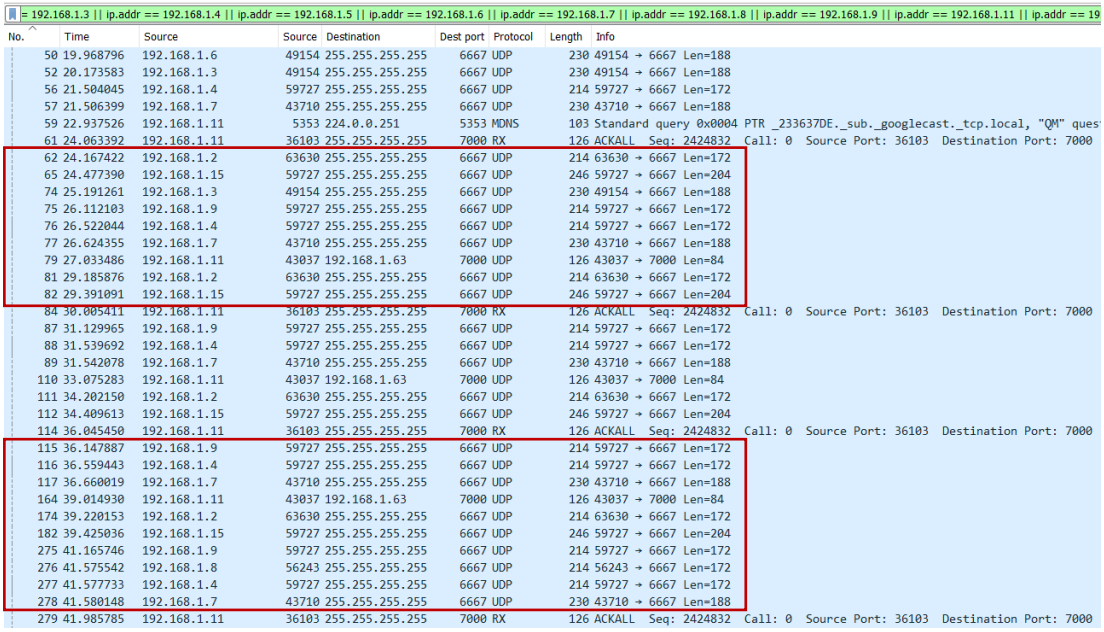
interacción del usuario a través de la aplicación móvil influye en la comunicación de los dispositivos. La información recopilada de los dispositivos IoT indican la presencia de solicitudes ARP en la red, como se muestra en la Figura 17.



No.	Time	Source	Source	Destination	Dest port	Protocol	Length	Info
923	149.200643	192.168.1.2	63630	255.255.255.255	6667	UDP	214	63630 → 6667 Len=172
924	149.712559	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.4? Tell 192.168.1.11
925	149.815291	192.168.1.14	57388	239.255.255.250	1900	SSDP	217	M-SEARCH * HTTP/1.1
926	150.020182	192.168.1.6	49154	255.255.255.255	6667	UDP	230	49154 → 6667 Len=188
927	150.222764	zte_83:d9:5c		Broadcast		ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
928	150.430171	192.168.1.15	59727	255.255.255.255	6667	UDP	246	59727 → 6667 Len=204
929	150.530201	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.4? Tell 192.168.1.11
930	150.842563	192.168.1.14	57388	239.255.255.250	1900	SSDP	217	M-SEARCH * HTTP/1.1
931	150.940866	192.168.1.11	5353	224.0.0.251	5353	MDNS	103	Standard query 0x0005 PTR _233637DE._sub._googlecast._tcp.local, "QM"
932	151.146380	192.168.1.9	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
933	151.146697	zte_83:d9:5c		Broadcast		ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
934	151.556471	192.168.1.4	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
935	151.657473	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.4? Tell 192.168.1.11
936	151.761924	192.168.1.7	43710	255.255.255.255	6667	UDP	230	43710 → 6667 Len=188
937	151.855608	zte_83:d9:5c		Chongqin_40:ea…		ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
938	151.855640	Chongqin_40:ea:a9		zte_83:d9:5c		ARP	42	192.168.1.13 is at 1c:bf:c0:40:ea:a9
939	151.856065	zte_83:d9:5c		Chongqin_40:ea…		ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
940	151.856078	Chongqin_40:ea:a9		zte_83:d9:5c		ARP	42	192.168.1.13 is at 1c:bf:c0:40:ea:a9
941	151.856975	zte_83:d9:5c		Chongqin_40:ea…		ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
942	151.856988	Chongqin_40:ea:a9		zte_83:d9:5c		ARP	42	192.168.1.13 is at 1c:bf:c0:40:ea:a9
943	151.864651	192.168.1.11	60635	192.168.1.63	7000	UDP	126	60635 → 7000 Len=84
944	151.866890	192.168.1.14	57388	239.255.255.250	1900	SSDP	217	M-SEARCH * HTTP/1.1
945	152.168670	zte_83:d9:5c		Broadcast		ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
946	152.475782	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.4? Tell 192.168.1.11
947	152.731906	2603:1063:2200::2c	443	2800:370:db:eb…	52423	TLSv1.2	107	Application Data
948	152.775637	2800:370:db:ebb0:5…	52423	2603:1063:2200…	443	TCP	74	52423 → 443 [ACK] Seq=203 Ack=634 Win=514 Len=0
949	153.192733	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.4? Tell 192.168.1.11
950	154.011911	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.4? Tell 192.168.1.11
951	154.012125	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.9? Tell 192.168.1.11
952	154.218667	192.168.1.2	63630	255.255.255.255	6667	UDP	214	63630 → 6667 Len=172
953	154.729010	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.4? Tell 192.168.1.11
954	154.729316	9e:b1:d3:2f:03:c0		Broadcast		ARP	42	Who has 192.168.1.9? Tell 192.168.1.11
955	154.831020	Espressi_37:37:92		Broadcast		ARP	42	ARP Announcement for 192.168.1.6

Figura 17. Tráfico generado al controlar y monitorear el sistema IoT.

A continuación, se aplicó un filtro que permitió aislar los paquetes de datos correspondientes a las direcciones IP específicas de los dispositivos IoT en la red. De esta manera se obtuvo como resultado que el protocolo de comunicación predominante es el UDP, y el puerto de destino más recurrente en las comunicaciones de los dispositivos IoT es el puerto 6667. En la Figura 18 se observa la información correspondiente al envío de paquetes en los dispositivos IoT.

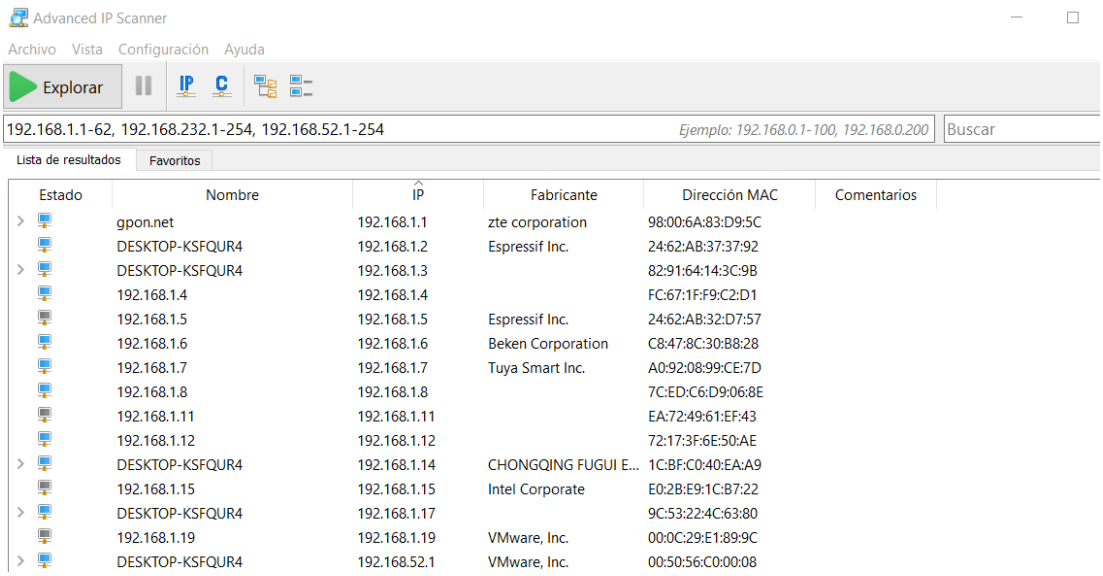


No.	Time	Source	Source	Destination	Dest port	Protocol	Length	Info
50	19.968796	192.168.1.6	49154	255.255.255.255	6667	UDP	230	49154 → 6667 Len=188
52	20.173583	192.168.1.3	49154	255.255.255.255	6667	UDP	230	49154 → 6667 Len=188
56	21.504045	192.168.1.4	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
57	21.506399	192.168.1.7	43710	255.255.255.255	6667	UDP	230	43710 → 6667 Len=188
59	22.937526	192.168.1.11	5353	224.0.0.251	5353	MDNS	103	Standard query 0x0004 PTR _233637DE._sub._googlecast._tcp.local, "QM" ques
61	24.063392	192.168.1.11	36103	255.255.255.255	7000	RX	126	ACKALL Seq: 2424832 Call: 0 Source Port: 36103 Destination Port: 7000
62	24.167422	192.168.1.2	63630	255.255.255.255	6667	UDP	214	63630 → 6667 Len=172
65	24.477390	192.168.1.15	59727	255.255.255.255	6667	UDP	246	59727 → 6667 Len=204
74	25.191261	192.168.1.3	49154	255.255.255.255	6667	UDP	230	49154 → 6667 Len=188
75	26.112103	192.168.1.9	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
76	26.522044	192.168.1.4	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
77	26.624355	192.168.1.7	43710	255.255.255.255	6667	UDP	230	43710 → 6667 Len=188
79	27.033486	192.168.1.11	43037	192.168.1.63	7000	UDP	126	43037 → 7000 Len=84
81	29.185876	192.168.1.2	63630	255.255.255.255	6667	UDP	214	63630 → 6667 Len=172
82	29.391091	192.168.1.15	59727	255.255.255.255	6667	UDP	246	59727 → 6667 Len=204
84	30.005411	192.168.1.11	36103	255.255.255.255	7000	RX	126	ACKALL Seq: 2424832 Call: 0 Source Port: 36103 Destination Port: 7000
87	31.129965	192.168.1.9	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
88	31.539692	192.168.1.4	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
89	31.542078	192.168.1.7	43710	255.255.255.255	6667	UDP	230	43710 → 6667 Len=188
110	33.075283	192.168.1.11	43037	192.168.1.63	7000	UDP	126	43037 → 7000 Len=84
111	34.202150	192.168.1.2	63630	255.255.255.255	6667	UDP	214	63630 → 6667 Len=172
112	34.409613	192.168.1.15	59727	255.255.255.255	6667	UDP	246	59727 → 6667 Len=204
114	36.045450	192.168.1.11	36103	255.255.255.255	7000	RX	126	ACKALL Seq: 2424832 Call: 0 Source Port: 36103 Destination Port: 7000
115	36.147887	192.168.1.9	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
116	36.559443	192.168.1.4	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
117	36.660019	192.168.1.7	43710	255.255.255.255	6667	UDP	230	43710 → 6667 Len=188
164	39.014930	192.168.1.11	43037	192.168.1.63	7000	UDP	126	43037 → 7000 Len=84
174	39.220153	192.168.1.2	63630	255.255.255.255	6667	UDP	214	63630 → 6667 Len=172
182	39.425036	192.168.1.15	59727	255.255.255.255	6667	UDP	246	59727 → 6667 Len=204
275	41.165746	192.168.1.9	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
276	41.575542	192.168.1.8	56243	255.255.255.255	6667	UDP	214	56243 → 6667 Len=172
277	41.577733	192.168.1.4	59727	255.255.255.255	6667	UDP	214	59727 → 6667 Len=172
278	41.580148	192.168.1.7	43710	255.255.255.255	6667	UDP	230	43710 → 6667 Len=188
279	41.985785	192.168.1.11	36103	255.255.255.255	7000	RX	126	ACKALL Seq: 2424832 Call: 0 Source Port: 36103 Destination Port: 7000

Figura 18. Identificación de protocolos y puertos en dispositivos IoT.

b. Advanced IP Scanner

El software Advanced IP Scanner permitió realizar un escaneo de la red, identificando todos los dispositivos conectados y proporcionando información detallada sobre cada uno de ellos. En la Figura 19, se muestran los dispositivos encontrando en la red junto con la información respectiva de cada uno de ellos, incluyendo su nombre, dirección IP, fabricante y dirección MAC.



Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
	gpon.net	192.168.1.1	zte corporation	98:00:6A:83:D9:5C	
	DESKTOP-KSFQUR4	192.168.1.2	Espressif Inc.	24:62:AB:37:37:92	
	DESKTOP-KSFQUR4	192.168.1.3		82:91:64:14:3C:9B	
	192.168.1.4	192.168.1.4		FC:67:1F:F9:C2:D1	
	192.168.1.5	192.168.1.5	Espressif Inc.	24:62:AB:32:D7:57	
	192.168.1.6	192.168.1.6	Beken Corporation	C8:47:8C:30:B8:28	
	192.168.1.7	192.168.1.7	Tuya Smart Inc.	A0:92:08:99:CE:7D	
	192.168.1.8	192.168.1.8		7C:ED:C6:D9:06:8E	
	192.168.1.11	192.168.1.11		EA:72:49:61:EF:43	
	192.168.1.12	192.168.1.12		72:17:3F:6E:50:AE	
	DESKTOP-KSFQUR4	192.168.1.14	CHONGQING FUGUI E...	1C:BF:C0:40:EA:A9	
	192.168.1.15	192.168.1.15	Intel Corporate	E0:2B:E9:1C:B7:22	
	DESKTOP-KSFQUR4	192.168.1.17		9C:53:22:4C:63:80	
	192.168.1.19	192.168.1.19	VMware, Inc.	00:0C:29:E1:89:9C	
	DESKTOP-KSFQUR4	192.168.52.1	VMware, Inc.	00:50:56:C0:00:08	

Figura 19. Dispositivos encontrados en la red con Advanced IP Scanner.

c. Kismet

La utilización conjunta de un adaptador Wi-Fi, cuya configuración se muestra en el Anexo B, y la herramienta Kismet permitió identificar, monitorear y registrar información detallada sobre redes inalámbricas cercanas y los dispositivos que se encuentran asociados. La Figura 20 presenta la información obtenida durante el escaneo para la red inalámbrica identificada como “Hogar Inteligente”.

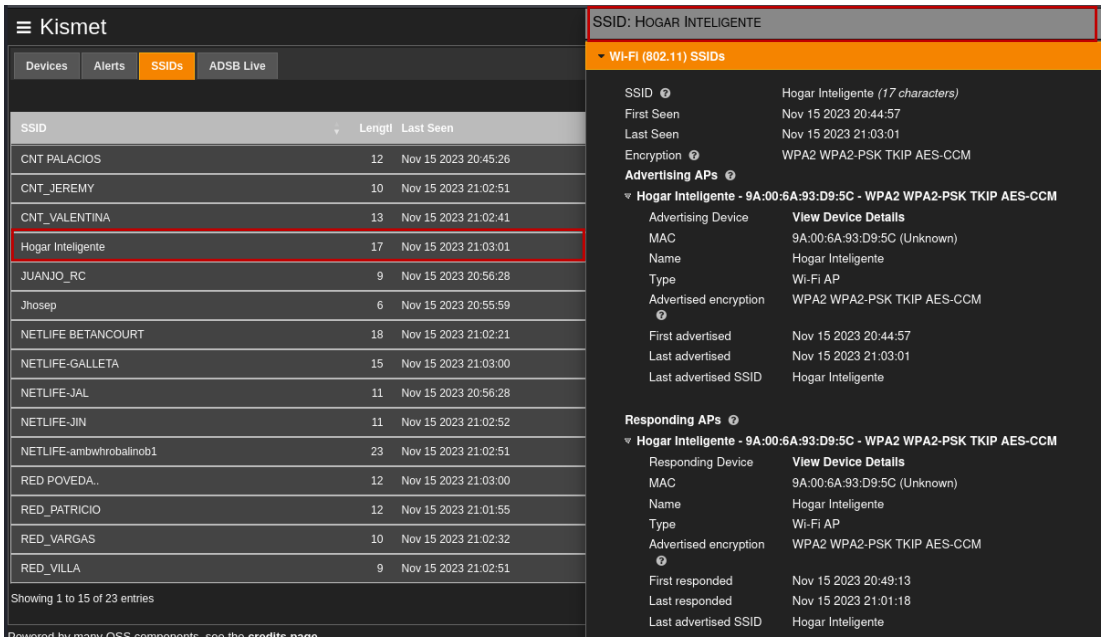


Figura 20. Escaneo de redes inalámbricas con Kismet.

Al identificar la red inalámbrica correspondiente, es posible acceder a información detallada sobre los dispositivos conectados a esta red. En la Figura 21 se presentan datos específicos para cada dispositivo, incluyendo su dirección MAC, tipo de dispositivo, transmisión de datos, encriptación, señal, canal de transmisión, paquetes de datos, clientes conectados y la dirección MAC correspondiente al punto de acceso inalámbrico.

Name	Type	Phy	Encryption	Sgn	Chan	Data	Packets	Clients	BSSID
Hogar Inteligente	Wi-Fi AP	IEEE802.11	WPA2-PSK	-44	10	0 B		11	9A:00:6A:93:D9:5C
A0:92:08:99:CE:7D	Wi-Fi Client	IEEE802.11	n/a	-62	12	5.90 KB		0	9A:00:6A:93:D9:5C
9E:B1:D3:2F:03:C0	Wi-Fi Client	IEEE802.11	n/a	-22	1	10.50 KB		0	9A:00:6A:93:D9:5C
38:1F:8D:E3:BD:98	Wi-Fi Client	IEEE802.11	n/a	-66	12	4.42 KB		0	9A:00:6A:93:D9:5C
24:62:AB:37:37:92	Wi-Fi Client	IEEE802.11	n/a	-51	9	7.20 KB		0	9A:00:6A:93:D9:5C
24:62:AB:32:D7:57	Wi-Fi Client	IEEE802.11	n/a	-76	12	6.86 KB		0	9A:00:6A:93:D9:5C
FC:67:1F:F9:C2:D1	Wi-Fi Client	IEEE802.11	n/a	-44	16	8.15 KB		0	9A:00:6A:93:D9:5C
C8:47:8C:30:B8:28	Wi-Fi Client	IEEE802.11	n/a	-64	15	8.15 KB		0	9A:00:6A:93:D9:5C
CC:78:5F:E7:62:17	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	9A:00:6A:93:D9:5C
FC:67:1F:D8:CA:35	Wi-Fi Client	IEEE802.11	n/a	-66	12	3.82 KB		0	9A:00:6A:93:D9:5C
FC:02:96:33:67:A6	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	9A:00:6A:93:D9:5C
7C:ED:C6:D9:06:8E	Wi-Fi Client	IEEE802.11	n/a	-24	10	415 B		0	9A:00:6A:93:D9:5C
54:F1:5F:B0:CA:48	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	9A:00:6A:93:D9:5C

Figura 21. Dispositivos conectados a la red inalámbrica.

A partir de la identificación de los dispositivos conectados a la red en cuestión, es posible acceder a información más detallada y específica acerca de cada uno de estos componentes. La Figura 22 presenta la información técnica correspondiente dispositivos IoT conectados a la red, como su dirección MAC, fabricante, frecuencia en la que trabaja y datos sobre el router al cual se encuentra conectado.

Figura 22. Información técnica de un dispositivo IoT.

3.5.2 Análisis de Riesgos y Vulnerabilidades

La detección de riesgos y vulnerabilidades en un sistema es posible mediante la utilización de herramientas que permiten la identificación de puntos de acceso potencialmente vulnerables y posibles brechas en la seguridad de la comunicación

entre dispositivos IoT. En la Tabla 19, se realiza un análisis de distintas herramientas enfocadas en la detección de riesgos y vulnerabilidades en los dispositivos IoT.

Tabla 20. Herramientas para la detección de riesgos y vulnerabilidades en los dispositivos IoT [41]-[42].

Especificaciones	**Angry IP Scanner**	**Nmap**	**Zenmap**	**Nessus**	**OpenVAS**
Interfaz Gráfica	Sí	Sí	Sí	Sí	Sí
Escaneo de IP	Sí	Sí	Sí	Sí	Sí
Escaneo de puertos	Sí	Sí	Sí	Sí	Sí
Escaneo de redes	Sí	Sí	Sí	Sí	Sí
Identificación de sistemas	No	Sí	Sí	Sí	Sí
Escaneo de vulnerabilidades	No	Sí	No	Sí	Sí
Análisis de puertos	No	Sí	No	Sí	Sí
Escaneo de servicios	No	Sí	No	Sí	Sí
Información Detallada	No	Sí	Sí	Sí	Sí
Escaneo de Rango IP	Sí	Sí	Sí	Sí	Sí
Escaneo de subredes	Sí	Sí	Sí	Sí	Sí
Escaneo de DNS	No	Sí	Sí	Sí	No
Escaneo de Host Online	Sí	Sí	Sí	Sí	Sí
Gestión de Escaneos	No	Sí	Sí	Sí	Sí
Detección de Sistemas Operativos	Sí	Sí	No	Sí	Sí
Evaluación de vulnerabilidades	No	No	No	Sí	Sí
Escaneo de SSL/TLS	No	Sí	No	Sí	Sí

La comparación realizada entre estas herramientas, permitió destacar tres de ellas: Angry IP Scanner, por su capacidad para escanear direcciones IP y puertos de manera rápida y sencilla; Nmap, realiza el mapeo de redes y detección de sistemas operativos y servicios; y Nessus, característico por sus escaneos detallados en vulnerabilidades y la elaboración respectiva de informes. La instalación y configuración de las herramientas que no están predefinidas en el entorno de pruebas se detallan en el Anexo D.

a. Angry IP Scanner

A través de Angry IP Scanner se realizó un escaneo de los dispositivos conectados a la red, y el estado respectivo de cada uno. En la Figura 23, se observa la información recopilada en la red del hogar, indicando los dispositivos que se encuentran activos y el tiempo de respuesta de cada uno. Sin embargo, esta herramienta no mostró de manera completa los puertos abiertos de los dispositivos.

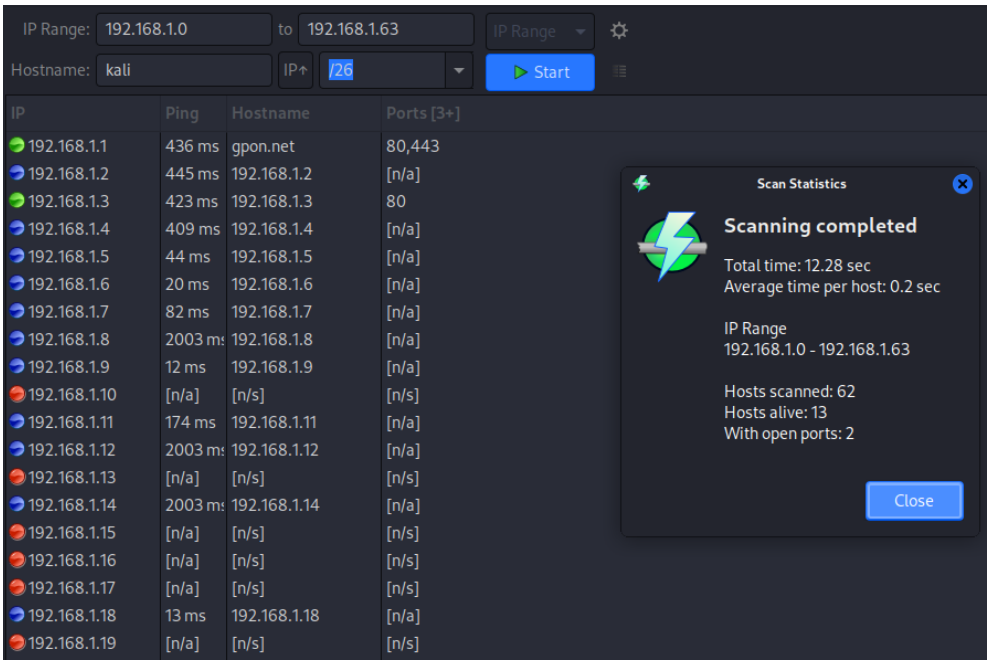


Figura 23. Escaneo de red con Angry IP Scanner.

b. Nmap

La herramienta de Nmap permitió realizar un análisis de la red doméstica, indicando información acerca de los dispositivos conectados, los servicios activos y los puertos disponibles. La Figura 24 presenta el escaneo de hosts realizado en la red, y, de esta manera identificar aquellos que se encuentran activos actualmente en la red.

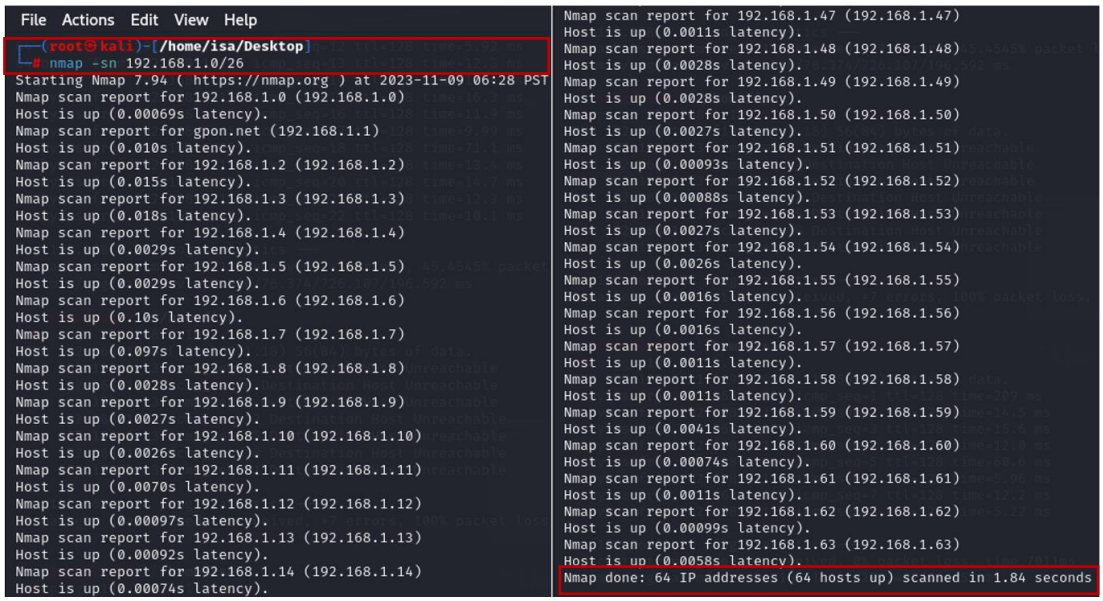


Figura 24. Enumeración de dispositivos en la red con Nmap.

A continuación, se llevó a cabo un escaneo individual de cada equipo perteneciente a la red IoT para identificar los puertos abiertos de cada uno, con el objetivo de determinar posibles puntos de vulnerabilidad. En diversos dispositivos de la red, no se lograron identificar sus puertos abiertos de manera específica. El escaneo de puertos mostró un mensaje en el cual se indicaba que todos los puertos fueron escaneados, pero el estado de cada uno de ellos no pudo ser determinado. En la Figura 25, se muestra la información resultante en los dispositivos IoT.

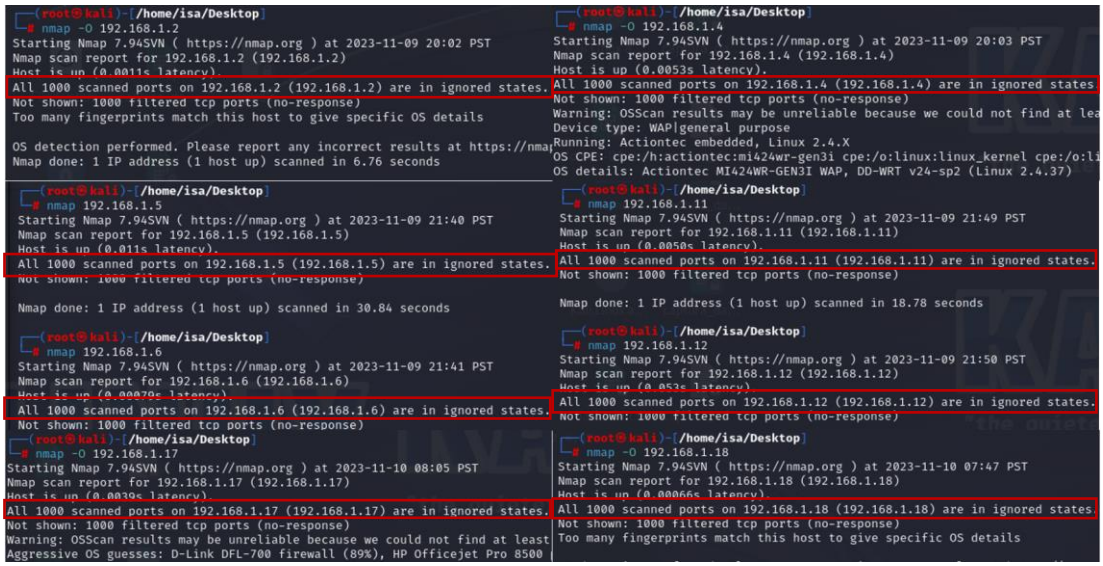


Figura 25. Escaneo de puertos en los dispositivos IoT.

Sin embargo, durante este proceso, se identificaron puertos abiertos en los siguientes dispositivos: router de la red, Smart Wi-Fi Plug, Smart Wi-Fi Camera Indoor, Smart Wi-Fi LED Color bulb y Echo Dot Alexa 5ta gen. En la Figura 26, se muestra la información de los puertos abiertos encontrados en cada dispositivo, respectivamente.

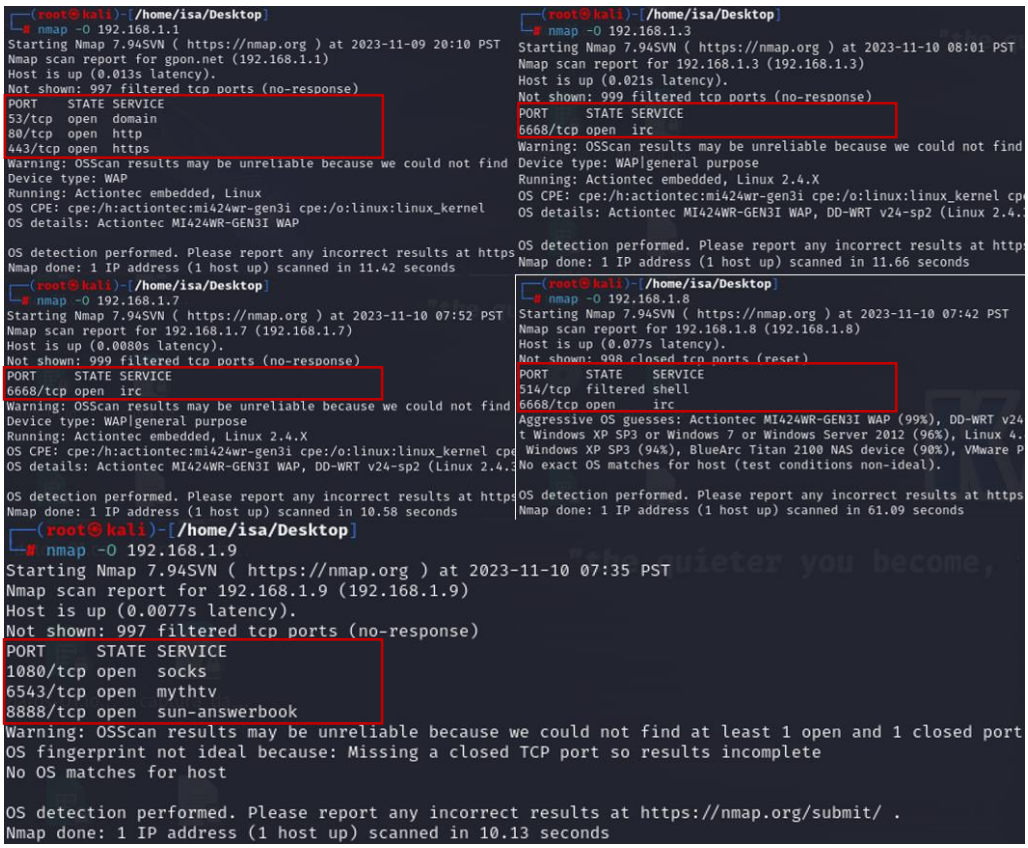


Figura 26. Identificación de puertos abiertos en los dispositivos IoT.

c. Nessus

La herramienta Nessus permitió escanear la configuración de puertos, servicios y vulnerabilidades de los dispositivos pertenecientes a la red del hogar. La Figura 27 muestra las vulnerabilidades identificadas en los dispositivos que se encuentran en la red analizada, y a través de este análisis, destacaron dos dispositivos con vulnerabilidades críticas: el asistente de voz Alexa Echo Dot y el router principal de la red, con dirección IP 192.168.1.8 y 192.168.1.1, respectivamente.

Figura 27. Escaneo de vulnerabilidades en los dispositivos de la red.

La Figura 28 y la Figura 29 muestran un análisis detallado de las vulnerabilidades identificadas en los dispositivos más susceptibles, el Echo Dot Alexa y el router del sistema, respectivamente. Las principales vulnerabilidades de estos dispositivos están relacionadas a los protocolos de cifrado SSL y TLS.

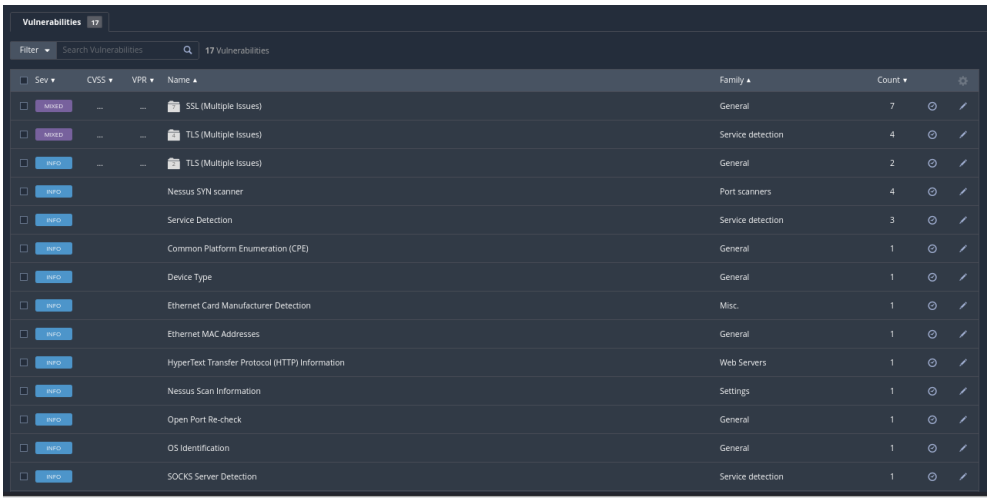


Figura 28. Vulnerabilidades en el dispositivo con dirección IP 192.168.1.8

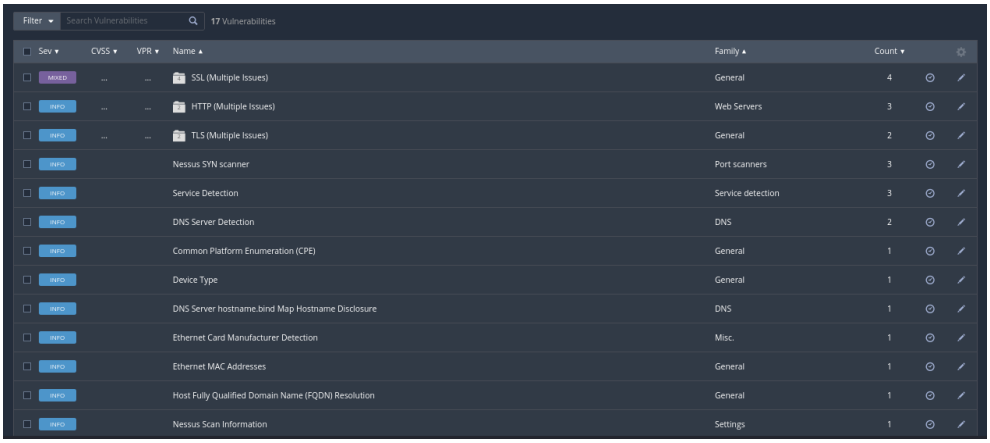


Figura 29. Vulnerabilidades en el dispositivo con dirección IP 192.168.1.1

3.5.3 Explotación

Esta etapa se llevó a cabo mediante la realización de pruebas de penetración, utilizando herramientas específicas, cuyas configuraciones se detallan en el Anexo E, para poner a prueba las vulnerabilidades previamente identificadas en el sistema IoT de un hogar inteligente. Estas pruebas se basaron en el modelo de amenazas STRIDE, un enfoque que analiza las vulnerabilidades de un sistema a través de seis categorías de amenazas distintas:

- S (Spoofing) – Suplantación de Identidad: El atacante puede suplantar identidades legítimas para obtener acceso no autorizado a sistemas o datos.
- T (Tampering) – Manipulación de datos: Es cualquier intento de manipular datos o sistemas, ya sea alterando la información o el funcionamiento de un sistema.
- R (Repudiation) – Repudio: Es la incapacidad de comprobar que una acción específica ha ocurrido en los dispositivos o en el sistema.
- I (Information Disclosure) – Divulgación de Información: Es la exposición no autorizada de datos sensibles o confidenciales a personas no autorizadas.
- D (Denial of Service) – Denegación de Servicio: Es la interrupción o limitación del acceso legítimo a recursos o servicios del sistema.

- E (Elevation of Privilege) – Elevación de Privilegios: El atacante busca obtener un nivel de acceso mayor al que se le ha concedido inicialmente, de manera que pueda realizar acciones a las cuales normalmente no tendría acceso

El análisis de herramientas de pruebas de amenazas es fundamental para seleccionar los instrumentos de evaluación adecuados según las necesidades específicas de la red [43].

a. Suplantación de Identidad

Las pruebas de suplantación de identidad evalúan vulnerabilidad de un sistema o red cuando un atacante intenta hacerse pasar por otra entidad legítima. Estos ataques buscan engañar a sistemas, usuarios o dispositivos haciéndoles creer que la identidad falsificada es auténtica. La Tabla 21 presenta un análisis de herramientas enfocadas en la realización de pruebas de suplantación de identidad, con la finalidad de identificar y seleccionar aquellas más adecuadas para ejecutar en el sistema IoT.

Tabla 21. Herramientas para pruebas de suplantación de identidad [44], [45].

Características	SpoofMAC	Macchanger	NetCut	Bettercap
Cambiar/Restaurar Dirección MAC	Sí	Sí	Sí	Sí
Generación Aleatoria de MAC	Sí	Sí	No	Sí
Detección de dispositivos	No	No	Sí	Sí
Habilitar/Deshabilitar Red	No	No	Sí	Sí
Plataformas Disponibles	Linux	Linux, Windows, macOS	Windows	Linux, macOS, Windows
Aplicaciones	Listas de OUI	Manipulación de OUI, escaneo de red.	Detección de dispositivos, escaneo de red.	Intercepción de tráfico, ataques MITM, intercepción y modificación de tráfico.

Se determinó que tanto Macchanger como Bettercap destacan como las herramientas más completas para realizar este tipo de pruebas. Ambas herramientas tienen la capacidad de cambiar y restaurar direcciones MAC, así como generar aleatoriamente direcciones MAC para suplantar identidades. Además, Macchanger presenta y

manipula listas de OUI y escaneo de red, mientras que Bettercap ofrece funciones avanzadas de intercepción y modificación de tráfico.

En este contexto, la herramienta Macchanger permitió analizar evaluar la eficiencia de los controles de acceso a la red basados en direcciones MAC mediante la función `macchanger -list`. A través de este comando, se obtuvo una lista de los rangos de direcciones MAC asociadas a fabricantes específicos de dispositivos, como se muestra en la Figura 30.

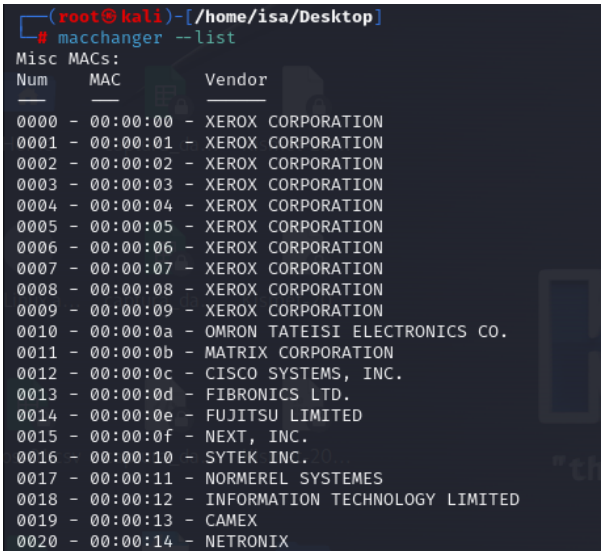


Figura 30. Direcciones MAC asociadas a fabricantes de dispositivos

El adaptador USB 802.11 utilizado para escanear la red inalámbrica tiene la capacidad de cambiar su dirección MAC, por lo que puede ocultar su identidad real en la red y evaluar su seguridad. En la Figura 31 presenta la modificación de la dirección MAC del adaptador mediante la ejecución del comando `macchanger -r wlan0`.

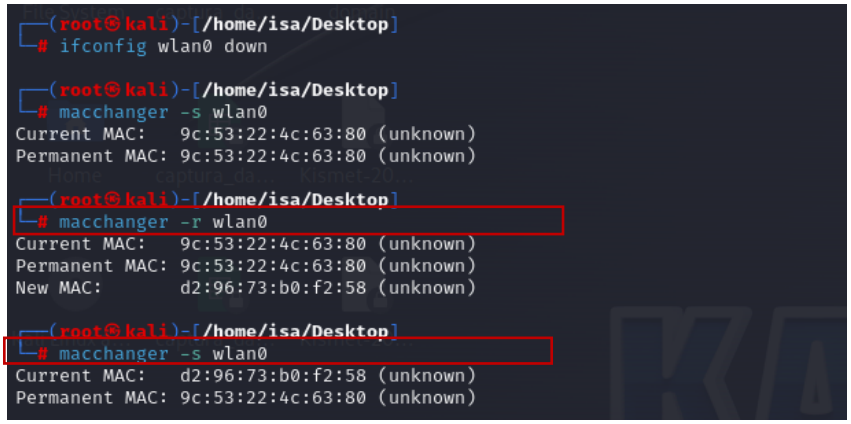


Figura 31. Modificación de la dirección MAC en el adaptador USB 802.11

A través del comando `netdiscover`, se identificaron las direcciones MAC presentes en la red. Posteriormente, se cambió la dirección MAC del adaptador simulando ser uno de los dispositivos IoT de la red, demostrando vulnerabilidades en los controles de acceso a la red y la posibilidad de suplantación de identidad por parte de un atacante. La Figura 32 muestra la suplantación de identidad en la dirección MAC del Echo Dot Alexa perteneciente a Amazon Technologies In. mediante el comando macchanger `--mac=MAC del dispositivo wlan0`.

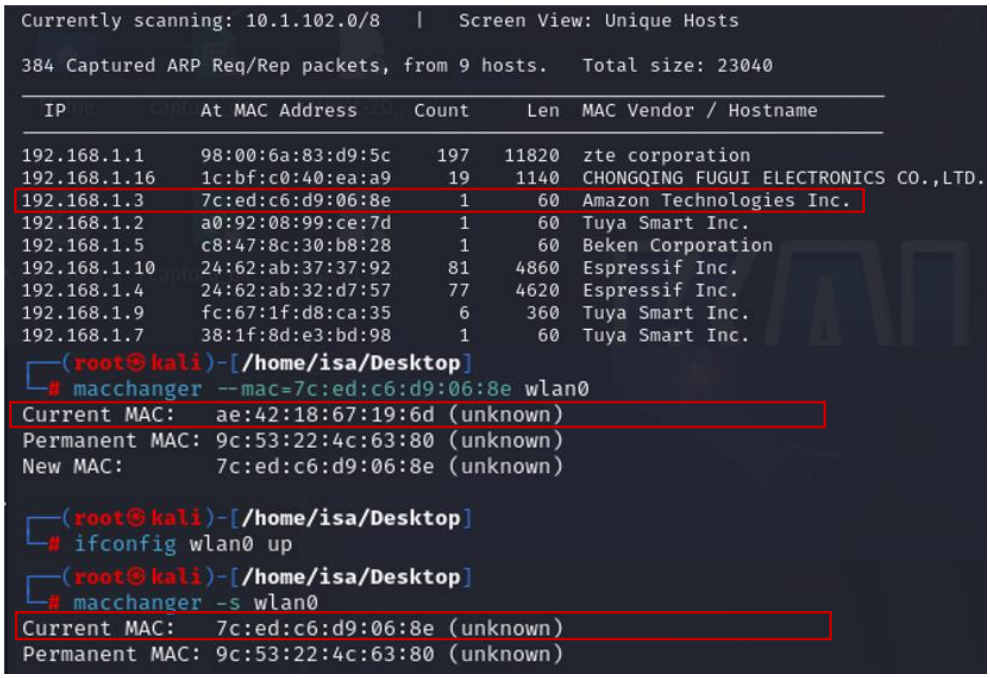


Figura 32. Suplantación de identidad en la dirección MAC.

Por otra parte, la herramienta Bettercap se empleó para analizar la seguridad en la red, y mediante el comando `net.probe on` se identificaron los dispositivos activos. La Figura 33 muestra los resultados obtenidos para los dispositivos activos que se detectaron en la red del hogar inteligente.

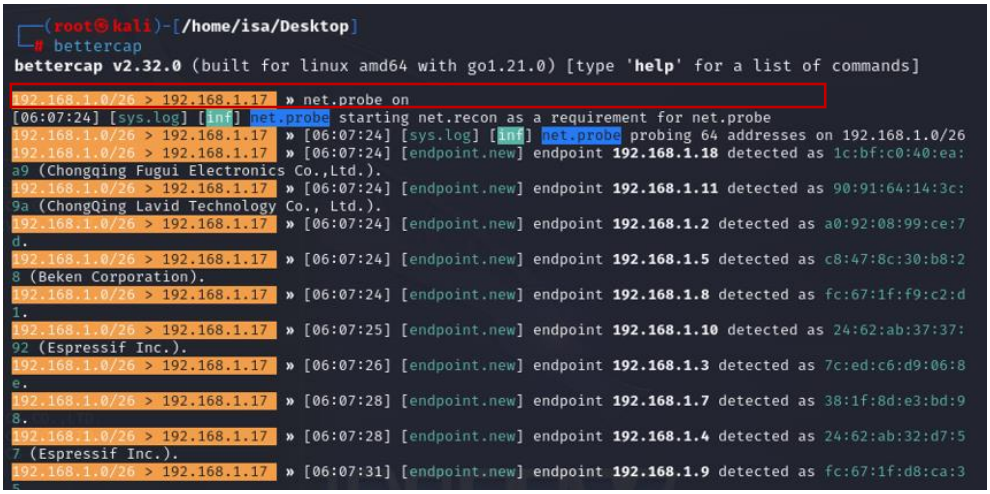


Figura 33. Identificación de los dispositivos activos en la red

El comando `net.show` permitió obtener información de los dispositivos conectados a la red, como sus direcciones IP, MAC, fabricante, y la cantidad de paquetes capturados desde cada uno. La Figura 34 muestra la información correspondiente a los dispositivos activos en la red, identificados como los dispositivos IoT del sistema.

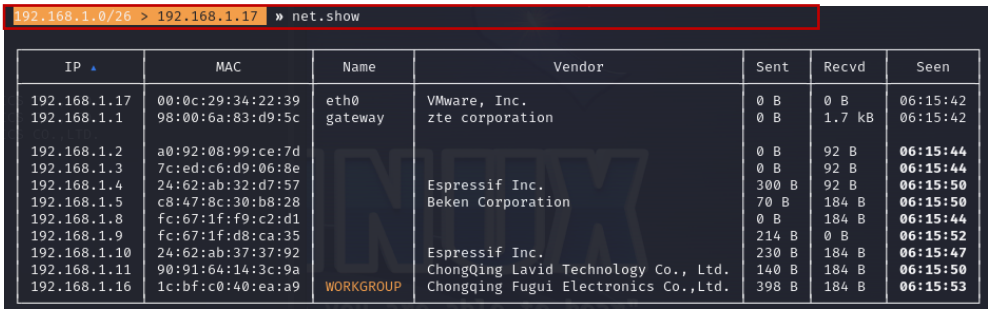


Figura 34. Información de los dispositivos activos en la red

A continuación, para llevar a cabo el ataque ARP Spoofing en los dispositivos IoT identificados con las direcciones IP 192.168.1.3, 192.168.1.11 y 192.168.1.16, se procedió a seleccionarlos mediante el comando `set arp.spoof targets <direcciones ip>`. Para activar este ataque, se utilizó el comando `arp.spoof on`, el cual engañó a los dispositivos haciéndoles creer que la dirección MAC del atacante es la dirección MAC del router del sistema, cuya dirección IP es 192.168.1.1, y así dirigir el tráfico de datos hacia el atacante, como se muestra en la Figura 35.

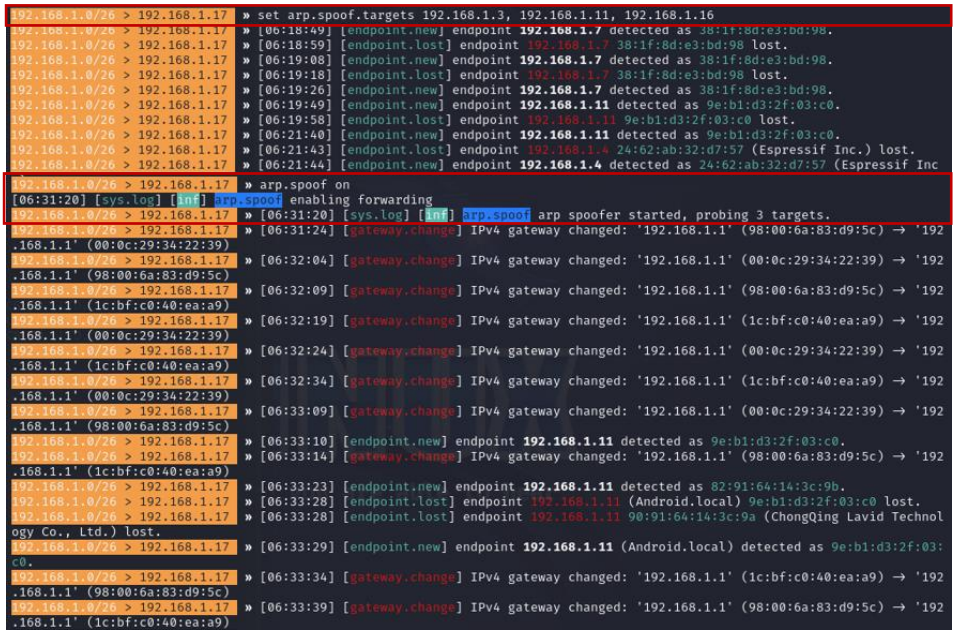


Figura 35. Ataque ARP Spoofing en los dispositivos IoT seleccionados

A través del comando `net.sniff` se capturó y analizó el tráfico de red en tiempo real presente entre los dispositivos atacados y la red, como se muestra en la Figura 36. Esta información mostró el intercambio de datos entre los dispositivos seleccionados durante el monitoreo de los dispositivos IoT mediante el monitoreo de la aplicación del dispositivo móvil.

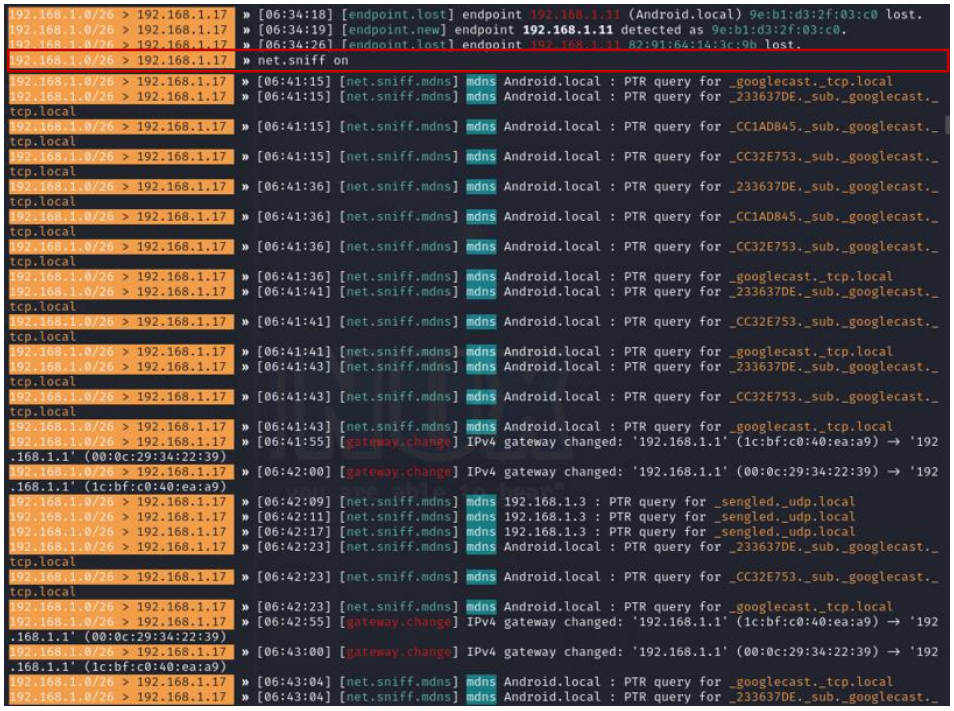


Figura 36. Análisis del tráfico en los dispositivos víctima

Durante la ejecución del ataque, se registró la actividad del usuario al acceder al sistema mediante el dispositivo móvil. Este registro incluyó información sensible, como credenciales de inicio de sesión y actividades de navegación web realizadas por el usuario, lo cual se identifica en la Figura 37.

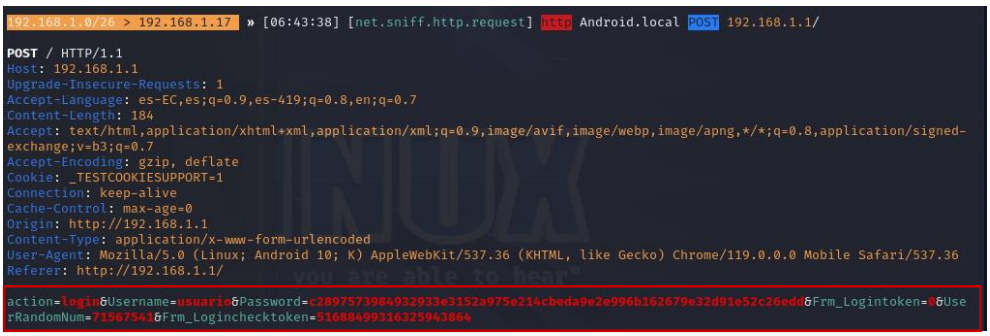


Figura 37. Registro de actividad del usuario en el dispositivo objetivo

Los resultados obtenidos en la ejecución del ataque ARP Spoofing en los dispositivos IoT, además de la aplicación de la herramienta Macchanger para modificar la dirección MAC del atacante por la de dispositivos IoT, reveló vulnerabilidades significativas en la seguridad de la red, al indicar la capacidad del atacante para suplantar la identidad de un dispositivo del sistema y, también, para acceder a información confidencial.

b. Manipulación de Datos

Los ataques de manipulación de datos en el sistema IoT pueden engañar al sistema para que reserve recursos para conexiones falsas, lo que conduce a una sobrecarga y posible manipulación de la información. En la Tabla 22, se presenta un análisis de herramientas enfocadas en la realización de pruebas de manipulación de datos, para identificar y seleccionar aquellas más adecuadas para ejecutar en el sistema IoT.

Tabla 22. Herramientas para pruebas de manipulación de datos [41], [46], [47].

Característica	PackETH	Scapy	Nemesis	Impacket
Manipulación de paquetes	Sí	Sí	Sí	Sí
Soporte de protocolos	Amplia variedad	Amplia variedad	Amplia variedad	Variedad considerable
Creación de paquetes personalizados	SÍ	Sí	Sí	Sí
Captura y análisis de tráfico	No	Sí	No	Sí
Creación de tráfico personalizado	SÍ	Sí	Sí	Sí

Característica	PackETH	Scapy	Nemesis	Impacket
Manejo de sesiones TCP/IP	No	Sí	Sí	No
Plataformas Disponibles	Linux, Windows	Linux, macOS, Windows	Linux, BSD, Windows	Linux, macOS, Windows
Aplicaciones	Filtros, estadísticas, scripting.	Inyección de paquetes, scripting y manipulación avanzados.	Inyección de paquetes en tiempo real.	Generación de patrones de tráfico.

La herramienta Scapy se muestra como la más adecuada para la realización de estas pruebas en el sistema IoT, debido a su amplio soporte de protocolos, capacidad para la creación y manipulación detallada de paquetes, así como su funcionalidad para la captura y análisis de tráfico.

Al acceder a la herramienta Scapy en el entorno de pruebas y al ejecutar el comando `sniff(iface= "eth0", prn=lambda x:x.summary`, se visualizó una secuencia de resúmenes de paquetes que proporcionaron información clave, como direcciones de origen y destino, tipos de protocolos, y otros aspectos relevantes de los dispositivos IoT, como se muestra en Figura 38. Este enfoque admite el análisis y comprensión de la actividad en la red, permitiendo la identificación de patrones de tráfico y la realización de diagnósticos en tiempo real.

Figura 38. Captura de tráfico y resumen de paquetes con Scapy

La Figura 39 muestra la creación y manipulación de paquetes mediante la función `send(IP(src="192.168.1.11", dst = "192.168.1.1") / TCP(sport=80, dport=80), count= 2000)`, la cual está diseñada para enviar 2000 paquetes TCP desde la dirección IP de origen “192.168.1.11” hacia la dirección de destino “192.168.1.1” a través del puerto 80. El resultado de este ataque, capturado mediante la interfaz de Wireshark como se muestra en la Figura 39, permite una inspección detallada de los paquetes enviados.

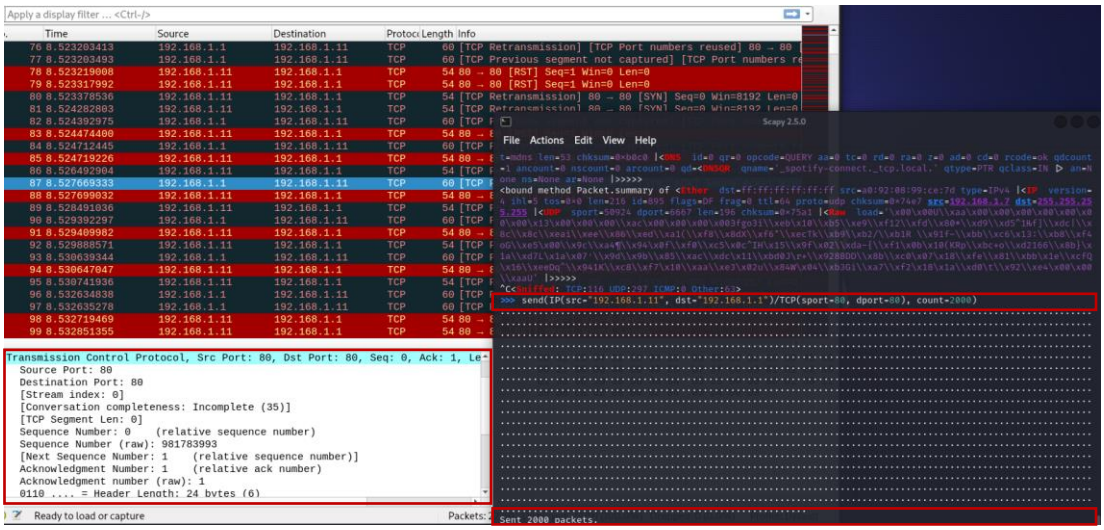


Figura 39. Creación de paquetes TCP desde la ip 192.168.1.11

La Figura 40 muestra la creación y manipulación de paquetes mediante la función `send(IP(src="192.168.1.8", dst = "192.168.1.1") / UDP(sport=80, dport=80), count= 2000)`, en este caso, diseñada para enviar 2000 paquetes UDP desde la dirección IP de origen “192.168.1.19” hacia la dirección de destino “192.168.1.1” a través del puerto 80. El resultado de este ataque, capturado mediante la interfaz de Wireshark como se muestra en la Figura 40, permite una inspección detallada de los paquetes enviados.

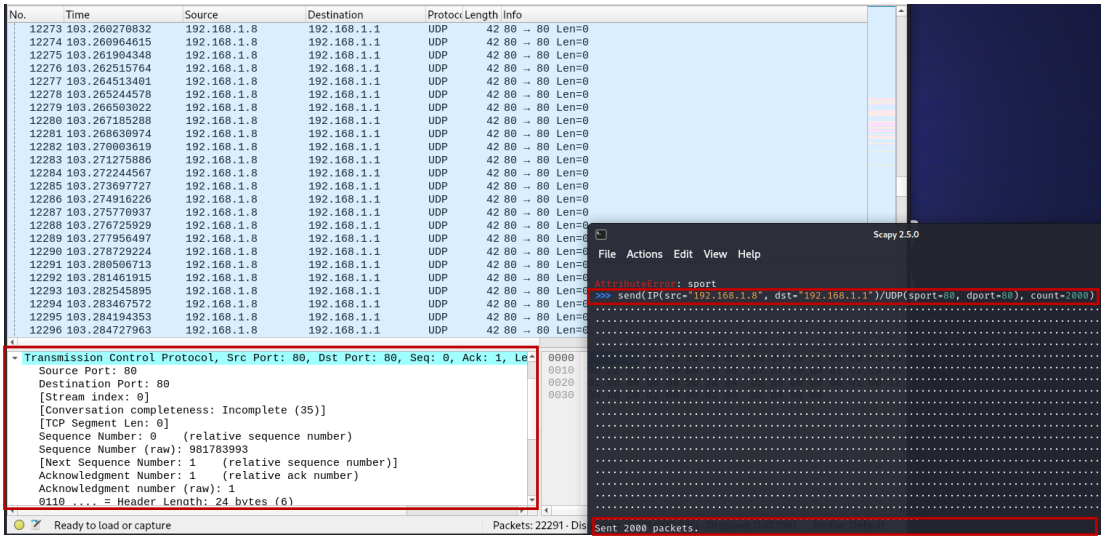


Figura 40. Creación de paquetes UDP desde la ip 192.168.1.8

La estrategia de emplear direcciones IP de dispositivos IoT como origen y la dirección IP del router como destino demostró ser efectiva al aumentar la credibilidad del ataque, ya que simula tráfico proveniente de fuentes confiables en la red. Como resultado de este tipo de ataque, se generó una sobrecarga en el sistema debido a la acumulación de múltiples solicitudes pendientes, lo cual limitó su capacidad para gestionar conexiones legítimas. Además, mediante este ataque es posible enviar paquetes con información maliciosa al sistema.

c. Repudio

Las amenazas de repudio en un sistema IoT implican la negación de transacciones específicas por parte de un dispositivo, pueden negar el envío de datos y bloquear la recepción de mensajes desde su origen. La Tabla 23 presenta un análisis de herramientas enfocadas en la realización de pruebas de repudio, con la finalidad de identificar y seleccionar aquellas más adecuadas para ejecutar en el sistema IoT.

Tabla 23. Herramientas para pruebas de repudio [40], [48], [49].

Características	NetworkMiner	Ettercap	Dsniff	Cain&Abel
Intercepción de tráfico	Sí	Sí	Sí	Sí
Captura de contraseñas	No	Sí	Sí	Sí
Manipulación de paquetes	No	Sí	No	Sí
Filtrado de tráfico	Sí	Sí	Sí	Sí
Análisis de sesiones	Sí	Sí	Sí	Sí
Inyección de paquetes	No	Sí	Sí	Sí
Soporte para plugins	No	Sí	No	No
Intercepción SSL/TLS	No	Sí	No	No

Características	NetworkMiner	Ettercap	Dsniff	Cain&Abel
Sistemas Operativos	Windows, Linux	Linux	Linux	Windows
Aplicaciones	Captura y análisis del tráfico de red.	Sniffing, ataques MITM, manipulación de tráfico	Captura y análisis de tráfico de red.	Captura e inyección de paquetes.

La herramienta Ettercap se destacó por ser la más idónea en entornos IoT por su versatilidad y eficiencia, debido a que cumple con funciones de Man-in-the-Middle (MITM), manipulación de paquetes y técnicas como ARP spoofing.

El ataque ARP Poisoning permite manipular la tabla de resolución de direcciones (ARP) en una red, envenenando la información de direcciones MAC de los dispositivos víctima. A través del comando `netdiscover`, se obtiene información detallada de los dispositivos presentes en la red, incluyendo sus direcciones IP, direcciones MAC, y otra información relevante como el fabricante o el nombre del host cuando es posible identificarlo, como se muestra en la Figura 41.

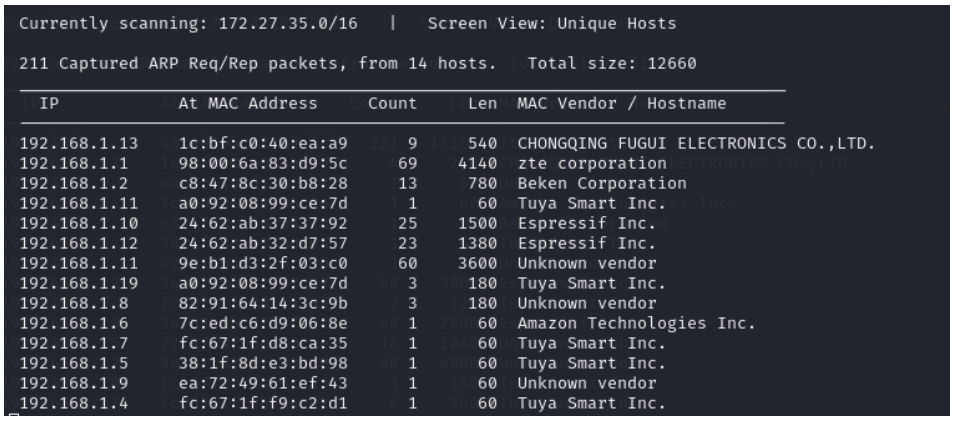


Figura 41. Resultado del escaneo de dispositivos en la red utilizando netdiscover

A través de la ejecución del comando `ettercap -G`, se accedió a la interfaz de Ettercap, la cual permitió visualizar y enumerar todos los hosts conectados a la red en ese momento. Los dispositivos Hosts conectados a la red inalámbrica del hogar, se visualizan en la Figura 42, incluyendo las diferentes opciones de ataques Man In The Middle que se pueden realizar para interceptar y manipular el tráfico de red.

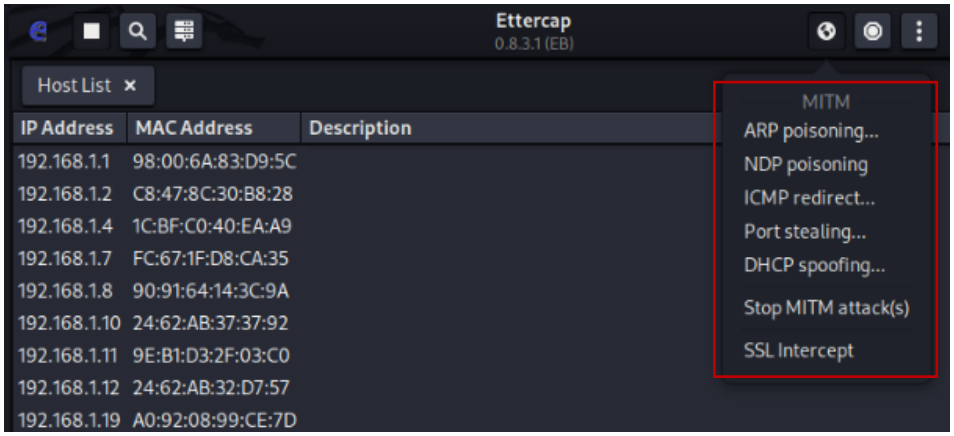


Figura 42. Lista de Hosts conectados a la red inalámbrica

La selección de los dispositivos IoT como objetivos víctima, incluyendo el router, el dispositivo móvil, la iluminación de los dormitorios y la cámara, junto con la ejecución del ataque ARP Poisoning, reveló la manipulación de información de estos dispositivos, como se muestra en la Figura 43. Cada dispositivo atacado modificó su dirección MAC y su identificador de distribuidor a uno único, generando un estado de incertidumbre acerca de la identidad original de cada dispositivo.

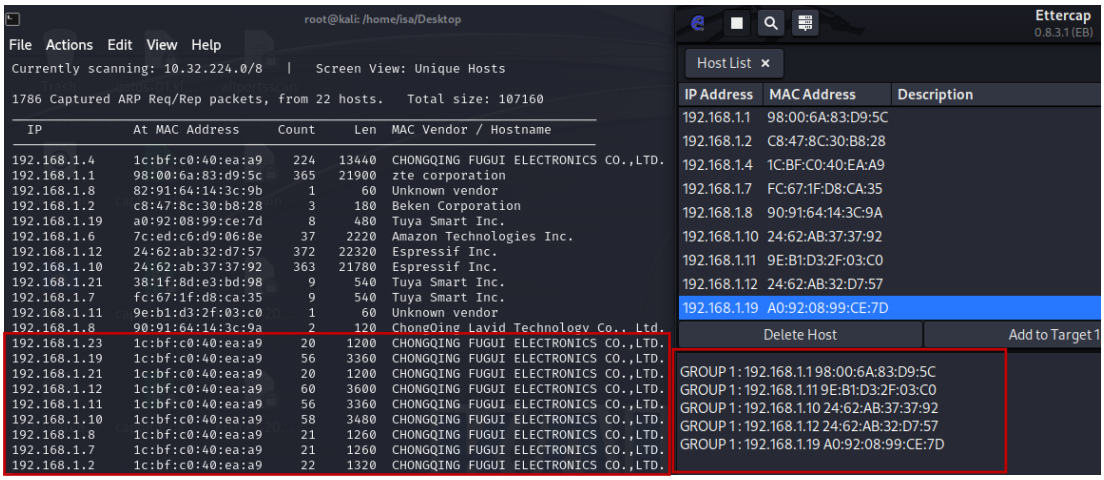


Figura 43. Ejecución del ataque ARP Poisoning

La inspección del tráfico de datos reveló un aumento considerable en la cantidad de información transmitida en la red en corto período de tiempo, por lo que se llegó a congestionar la misma. Como se evidencia en la Figura 44, múltiples dispositivos en la red fueron asignados a la misma dirección IP como resultado de la manipulación de la taba ARP.

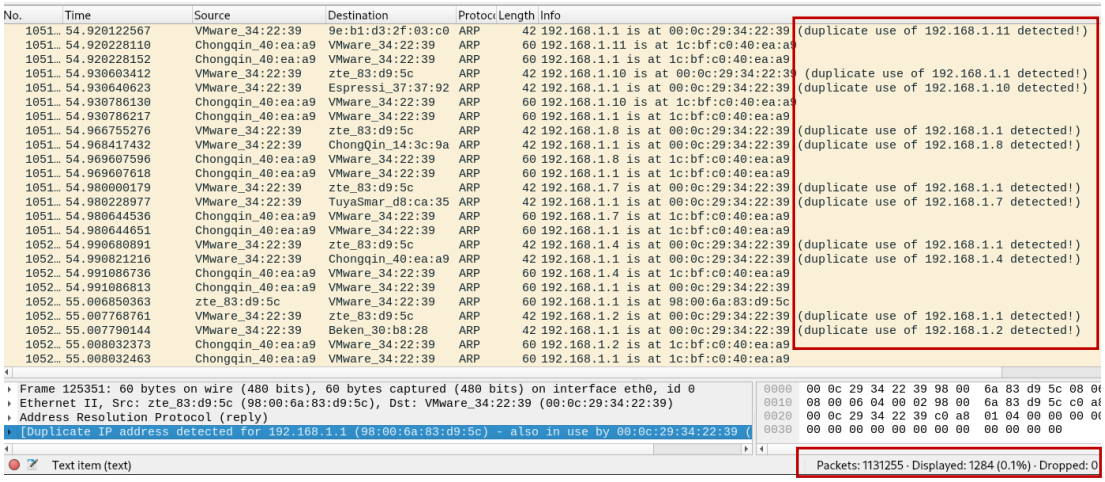


Figura 44. Tráfico de datos capturados en el ataque ARP Poisoning

Además, durante la ejecución de este ataque, se logró obtener información de credenciales en los dispositivos IoT, siempre y cuando el usuario acceda a la red comprometida, como se indica en la Figura 45.

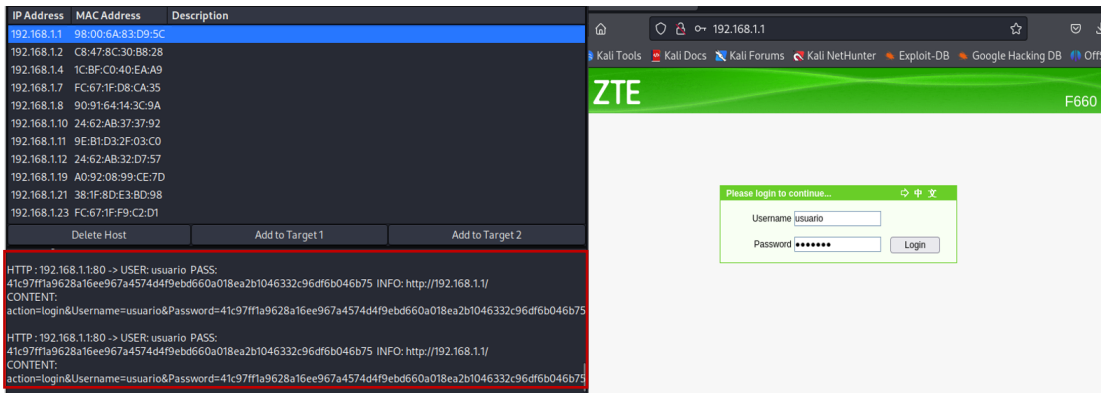


Figura 45. Obtención de credenciales mediante ARP Poisoning

Como resultado de este ataque, los dispositivos IoT seleccionados perdieron su conexión a la red y necesitaron ser reconfigurados para ser reintegrados al sistema. La manipulación exitosa de la tabla ARP y la consecuente pérdida de conectividad evidenciaron la vulnerabilidad de estos dispositivos ante este tipo de ataques.

d. Divulgación de Información

La divulgación de información ocurre cuando un atacante accede a datos confidenciales que no estaban destinados originalmente a él. Este tipo de ataque puede manifestarse de varias formas, como la interceptación de comunicaciones inalámbricas, acceso no autorizado a redes o dispositivos, o la obtención de información confidencial almacenada en sistemas. La Tabla 24 presenta un análisis de herramientas enfocadas en la realización de pruebas para la divulgación de información, con la finalidad de identificar y seleccionar aquellas más adecuadas para ejecutar en el sistema IoT.

Tabla 24. Herramientas para pruebas de divulgación de información [41], [50].

Características	**Hydra**	**Aircrack-ng**	**Wifite**	**Hashcat**	**John the Ripper**
Soporte de protocolos	TCP, UPD, ICMP, etc.	802.11 a/b/g/n/ac	802.11 a/b/g/n/ac	MD5, SHA1, etc.	MD5, SHA1, etc.
Filtrado de paquetes	Sí	Sí	Sí	Sí	Sí
Análisis de tráfico	Sí	Sí	Sí	No	No
Soporte de GPUs	No	Sí	Sí	Sí	Sí
Captura y desencriptación de paquetes	No	Sí	No	No	No
Soporte de diccionarios personalizados	No	Sí	Sí	Sí	Sí
Ataques a contraseñas específicas	Sí	Sí	No	No	Sí
Sistemas Operativos	Windows, Linux, macOS	Linux, macOS	Linux, macOS	Windows, Linux, macOS	Windows, Linux, macOS
Modos de ataque	Fuerza bruta, diccionario, ataques híbridos	Ataques de diccionario, ataques por fuerza bruta, ataques WPS	Automatización de ataques WEP, WPA, WPS.	Ataques de diccionario, ataques de máscara.	Ataques de diccionario, ataques de fuerza bruta.

Las herramientas Aircrack-ng y Wifite se destacaron por su enfoque en redes Wi-Fi, también por su capacidad para automatizar ataques y su soporte para diccionarios personalizados. Estas características resaltan su eficiencia en la auditoría y penetración de entornos inalámbricos, posicionándose como opciones destacadas en la evaluación de seguridad en dispositivos IoT.

Para la obtención de datos a través de Aircrack-ng, se deben seguir una serie de pasos específicos. El comando `airodump-ng –band abg wlan0` se utiliza para desplegar un sniffer de paquetes en redes Wi-Fi. Este procedimiento tiene como objetivo escanear y recopilar datos de las redes en los rangos de frecuencias asociados a los estándares 802.11a, 802.11b y 802.11g. La elección de la interfaz inalámbrica “wlan0”, correspondiente al adaptador de red, configurada en modo monitor facilita la detección de información relevante, como nombres de redes, direcciones MAC y canales de operación. La ejecución de este comando permitió obtener una lista de redes inalámbricas disponibles en el área y la identificación de la red perteneciente al hogar inteligente, como se muestra en la Figura 46.

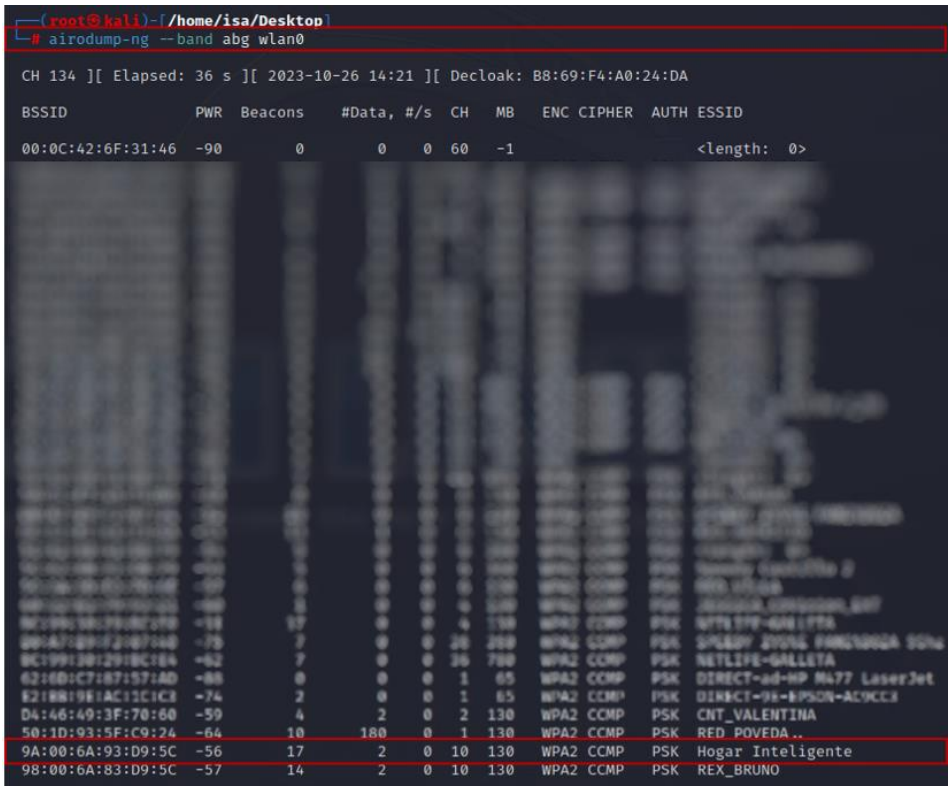


Figura 46. Redes inalámbricas disponibles en el área

A continuación, el comando `airodump -ng –bssid BSSID -c CANAL -w nombre_archivo wlan0` permitió la captura de paquetes de la red Wi-Fi en un archivo. La dirección MAC y el canal en que opera la red del hogar inteligente son especificados como parámetros, y los datos capturados se almacenan en un archivo con extensión .cap, como se muestra en la Figura 47. En esta etapa se está a la espera

de que un dispositivo IoT se conecte o reconecte a la red inalámbrica, y el router, en su proceso de autenticación, creó un punto crítico para descifrar la contraseña.

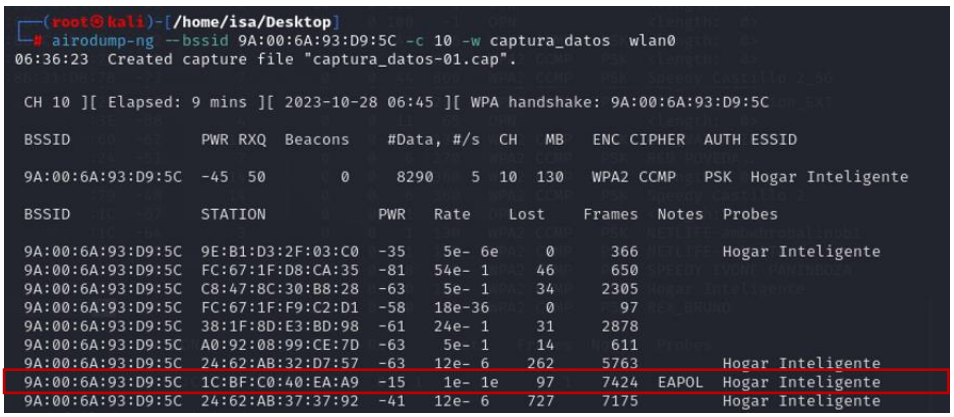


Figura 47. Reconexión de dispositivos a la red Wi-Fi

Para la desautenticación de clientes se ejecutó el comando `aireplay-ng --deauth canal -a BSSID -c MAC dispositivo IoT wlan0`, esta herramienta tiene como propósito enviar paquetes de desautenticación a los dispositivos que están actualmente conectados a la red Wi-Fi. Para evaluar la capacidad de resistencia de la red frente a intentos de interrupción del servicio. La desautenticación en los dispositivos IoT de la red se observa en la Figura 48.

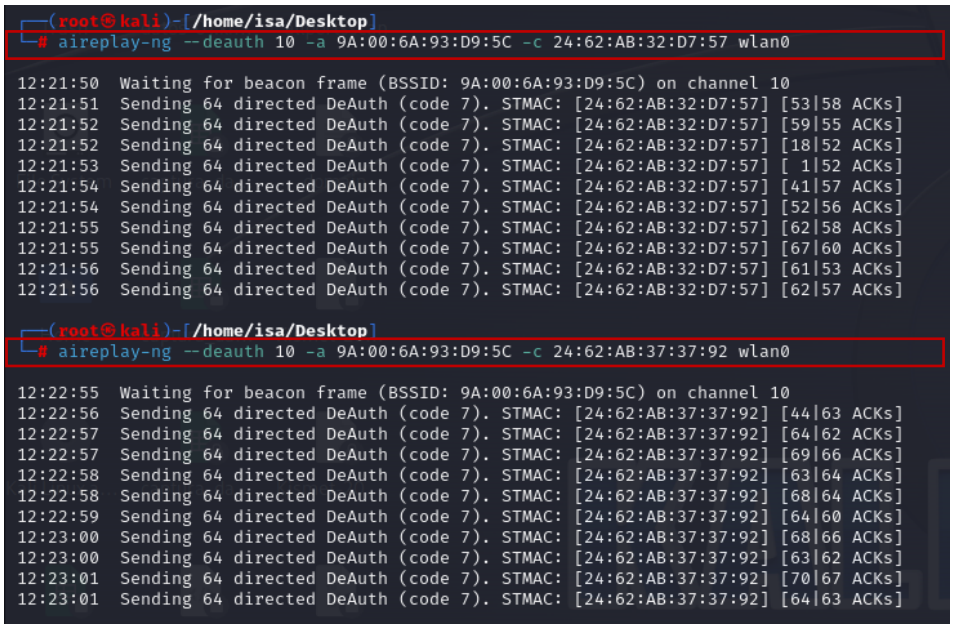


Figura 48. Desautenticación de los dispositivos IoT conectados a la red

Tras la captura de datos y la generación de diccionarios de contraseñas, se procedió al descifrado de la red objetivo. En este proceso, se utilizó el comando `aircrack-ng -w archivo_diccionario archivo_capturadatos.cap`, con el objetivo de obtener la clave de seguridad WPA/WPA2 mediante la verificación de coincidencias entre los datos capturados y las contraseñas almacenadas en el diccionario, con el fin de identificar la clave correcta que permitirá acceder a la red. La ejecución exitosa de este comando, utilizando los archivos creados previamente, el diccionario ubicado en `/home/isa/diccionario1.txt` y la captura de datos almacenada en `/home/isa/Desktop/captura_datos01.cap`, como se identifica en la Figura 49.

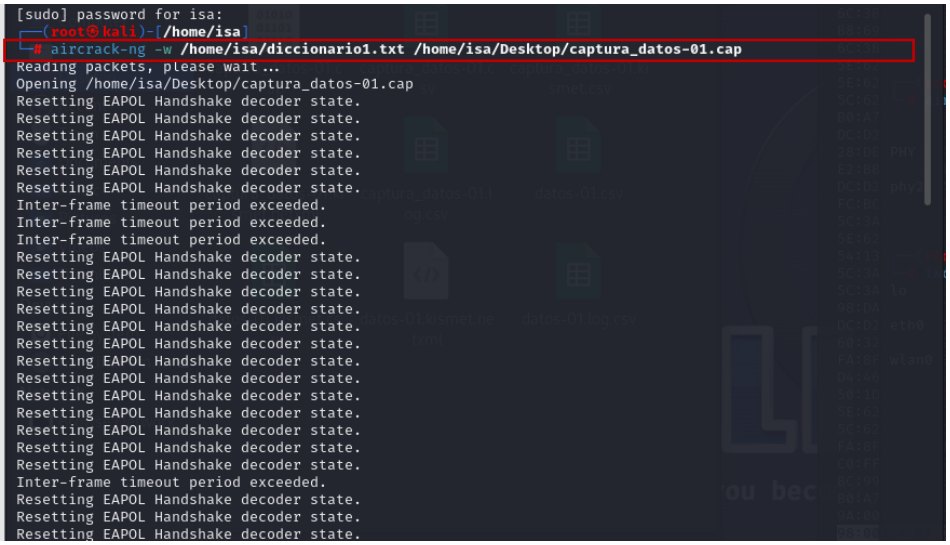


Figura 49. Proceso de descifrado en la clave WPA/WPA2 mediante aircrack-ng

En el primer intento de descifrado de la clave de acceso a la red, no se obtuvieron resultados ya que la combinación de datos capturados no coincidió con ninguna de las contraseñas del diccionario utilizado. Este proceso llevó un tiempo aproximado de una hora, como se identifica en la Figura 50.

Figura 50. Resultado del primer intento de descifrado con aircrack-ng

En el segundo intento de descifrado de la clave de acceso a la red, se logró obtener resultados en un tiempo aproximado de una hora. Este resultado evidencia que, a pesar de la falta de éxito inicial, persistir en un ataque mediante diccionarios y técnicas de fuerza bruta puede eventualmente llevar al acceso no autorizado a la red. La clave de acceso a la red y el tiempo que la herramienta tomó en descifrarla, se identifican en la Figura 51.

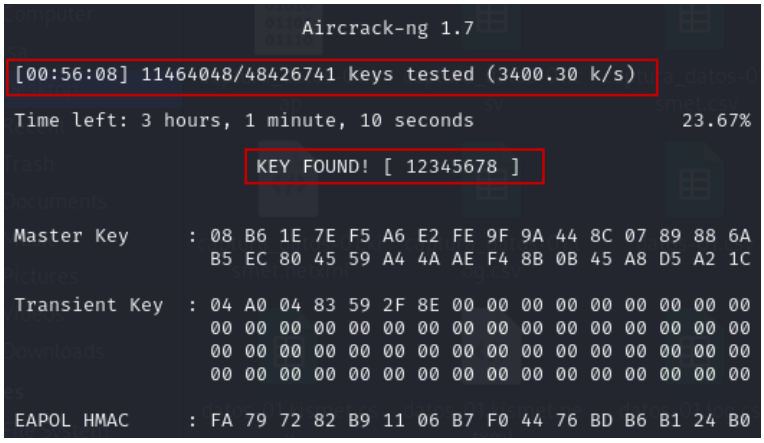


Figura 51. Resultado del segundo intento de descifrado con aircrack-ng

Por otra parte, la herramienta Wifite se utilizó como complemento para escanear las redes disponibles en el entorno, identificando puntos de acceso cercanos y recolectando información de estas redes. La información obtenida mediante Wifite, incluyendo datos como las redes detectadas, el canal de operación, el tipo de encriptación utilizado, la potencia de la señal (pwr), el estado del WPS y la cantidad de clientes conectados a cada red, se muestra en la Figura 52.

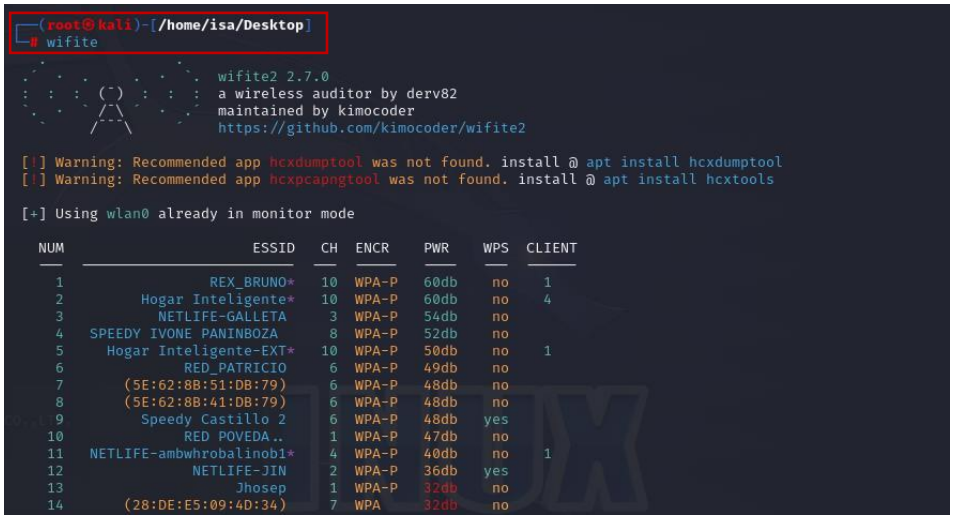


Figura 52. Captura de información con Wifite

Posteriormente, se ejecutó un ataque dirigido a la red específica vinculada al sistema IoT del hogar inteligente, logrando la obtención de credenciales de acceso en cuestión de pocos minutos, como se observa en la Figura 53. El rápido acceso a la información de autenticación resalta la eficacia de Wifite en la adquisición de datos cruciales.

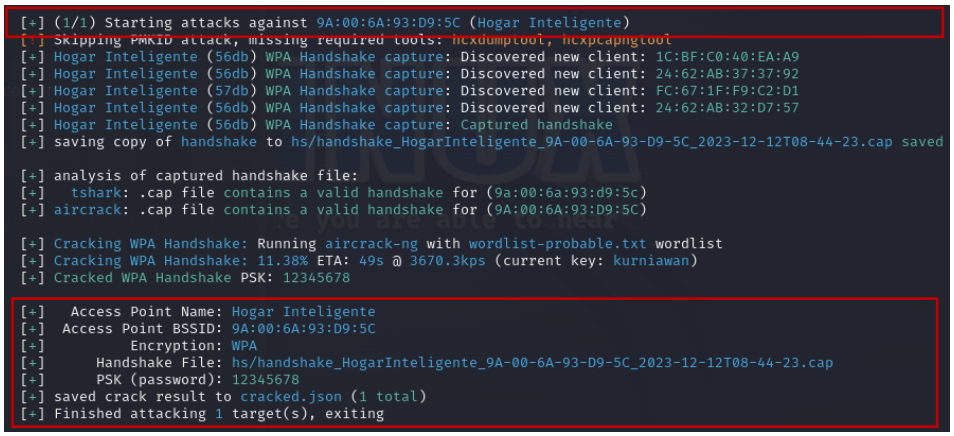


Figura 53. Obtención de credenciales de acceso a la red mediante Wifite

En resumen, tanto Aircrack-ng como Wifite destacaron en la evaluación de la seguridad de redes Wi-Fi asociadas a dispositivos IoT. Aircrack-ng por su capacidad de desautenticación y descifrado de claves WPA/WPA2, mientras que Wifite permitió un análisis rápido y efectivo de redes, destacándose en la obtención rápida de credenciales. Los atacantes podrían explotar estas debilidades para obtener control sobre los dispositivos IoT, comprometiendo la privacidad y seguridad de los usuarios.

e. Denegación de Servicio

Los ataques de denegación de servicio (DoS) se basan en la generación masiva de tráfico de red, el cual puede provocar que los dispositivos se queden sin recursos y dejen de responder correctamente. La Tabla 25 presenta un análisis de herramientas enfocadas en la realización de pruebas de denegación de servicios, con la finalidad de identificar y seleccionar aquellas más adecuadas para ejecutar en el sistema IoT.

Tabla 25. Herramientas para pruebas de denegación de servicios [41], [51].

Características	**LOIC**	**hping3**	**PyLoris**	**Slowloris**
Protocolos Soportados	HTTP, UPD, TCP.	TCP, UPD, ICMP.	HTTP	HTTP
Análisis de tráfico de datos	No	Sí	Sí	No
Filtrado de paquetes	Sí	Sí	Sí	Sí
Inyección de paquetes	Sí	Sí	Sí	Sí
Creación de paquetes	No	Sí	Sí	Sí
Manipulación de paquetes	No	Sí	No	No
Velocidad	Rápida	Rápida	Rápida	Lenta
Plataformas disponibles	Windows, Linux, macOS	Windows, Linux, macOS	Windows, Linux, macOS	Windows, Linux, macOS
Modo de ataque	DDoS, Ping, Scan	DDoS	DDoS	DDoS

La herramienta hping3 es la más adecuada para pruebas de denegación de servicio (DoS) en dispositivos IoT, debido a su compatibilidad con los protocolos utilizados por estos dispositivos, capacidad de análisis de tráfico, filtrado y manipulación de paquetes, así como su velocidad de ataque.

El comando `hping3 --rand-source –flood dirección ip -p puerto` se utilizó para realizar un ataque de inundación TCP desde múltiples direcciones IP de manera aleatoria hacia el dispositivo con la dirección IP especificada, que en este caso es 192.168.1.2. La opción `--rand-source` indica que las direcciones IP de origen serán seleccionadas al azar, mientras que `–flood` significa que se enviarán paquetes tan rápido como sea posible. Los resultados de este ataque TCP se encuentran registrados en Wireshark, y se pueden visualizar en la Figura 54.

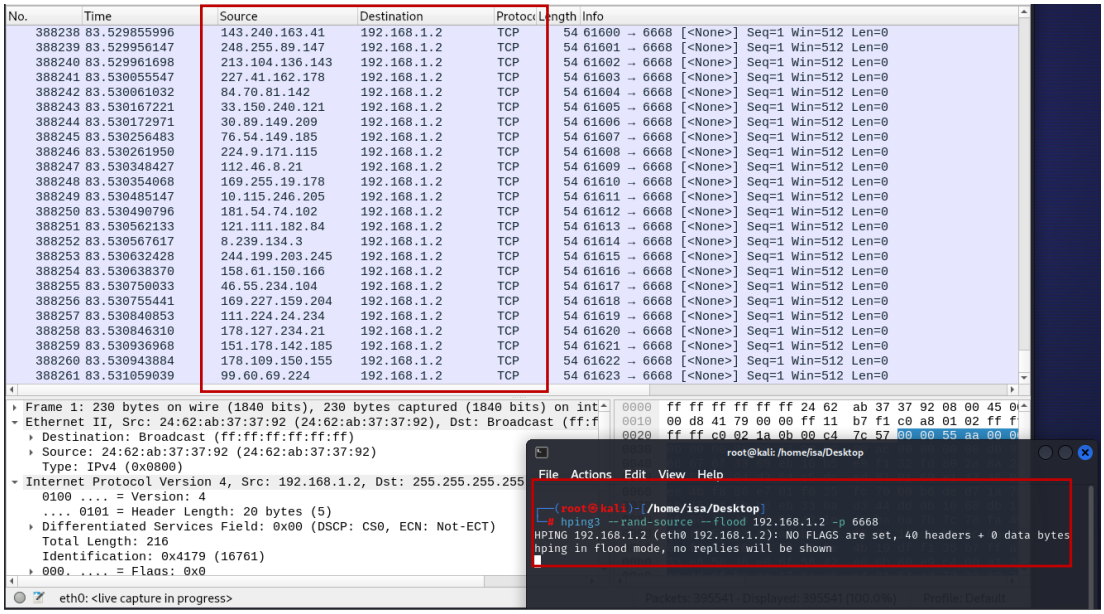


Figura 54. Inundación TCP en el dispositivo IoT con dirección IP 192.168.1.2

De igual manera, se llevó a cabo un ataque de inundación TCP similar utilizando el comando `hping3 --rand-source -flood` dirigido hacia el dispositivo con la dirección IP 192.168.1.5. Los resultados de este ataque TCP se encuentran registrados en Wireshark, y se pueden visualizar, se muestran en la Figura 55.

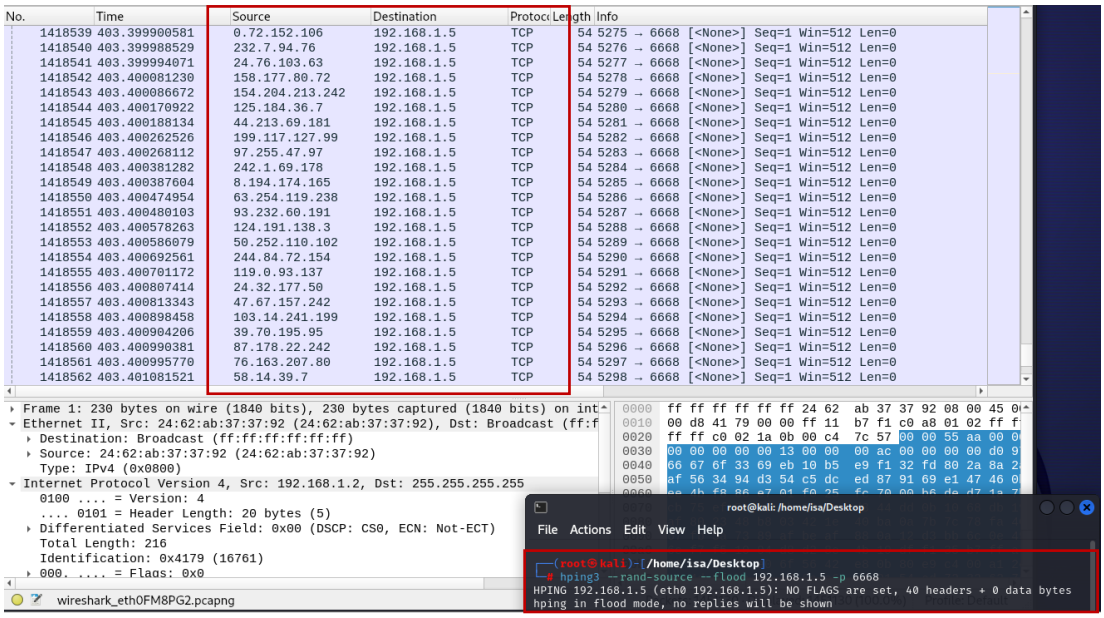


Figura 55. Inundación TCP en el dispositivo IoT con dirección IP 192.168.1.5

Por último, el comando `hping3 --rand-source -udp -flood dirección ip -p puerto` se utilizó para realizar un ataque de inundación UDP desde múltiples direcciones IP de manera aleatoria hacia el dispositivo con la dirección IP

especificada, que en este caso es 192.168.1.8. Este comando indica que los paquetes UDP serán enviados desde múltiples direcciones IP de manera aleatoria, generando una carga significativa del tráfico hacia el dispositivo objetivo. Los resultados de este ataque UDP se encuentran registrados en Wireshark, y se pueden visualizar en la Figura 56.

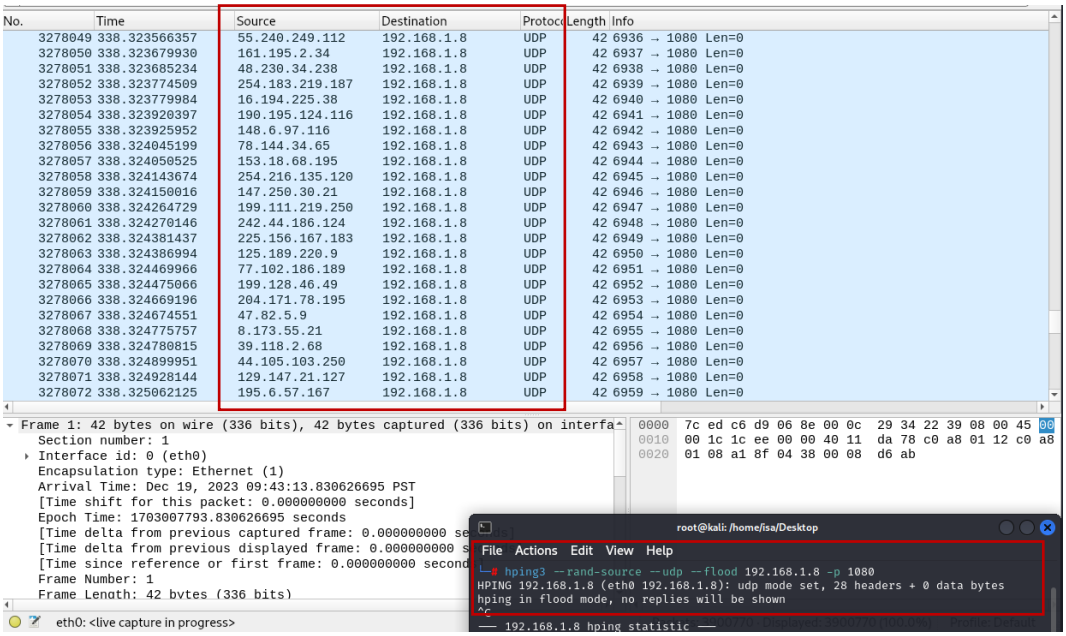


Figura 56. Inundación UDP en el dispositivo IoT con dirección IP192.168.1.8

Los ataques ejecutados con hping3 utilizando diversas técnicas, como inundación TCP y UDP, demostraron la vulnerabilidad de los dispositivos IoT en el entorno de prueba. La generación de una sobrecarga de tráfico de datos afectó la funcionalidad de estos dispositivos, comprometiendo su capacidad de operación dentro del sistema. Este tipo de ataques demostraron la dificultad en la identificación y detección de los intrusos en el sistema.

f. Elevación de Privilegios

Los ataques de elevación de privilegios o servicios se refieren a técnicas en las cuales un atacante busca obtener un nivel de acceso más alto del que debería tener en un sistema o dispositivo. La Tabla 26 presenta un análisis de herramientas enfocadas en la realización de pruebas de elevación de privilegios, con la finalidad de identificar y seleccionar aquellas más adecuadas para ejecutar en el sistema IoT.

Tabla 26. Herramientas para pruebas de elevación de servicios [52], [53].

Características	Metasploit	Routersploit	PowerSploit
Soporte de protocolos	TCP, UDP, HTTP, HTTPS, SMB, DNS, etc.	TCP, UDP, HTTP, HTTPS, SNMP, Telnet, SSH, etc.	TCP, UDP, ICMP, etc.
Exploits y Payloads	Para diferentes servicios y protocolos.	Routers y dispositivos IoT.	Post-explotación en sistemas Windows.
Soporte para una amplia gama de dispositivos	Sí	Sí	No
Soporte para dispositivos IoT de baja potencia	No	Sí	No
Herramienta gratuita y de código abierto	Sí	Sí	No
Explotación de vulnerabilidades	Sí	Sí	Sí
Automatización de ataques	Sí	Sí	No
Plataformas Disponibles	Windows, Linux, macOS.	Linux, Android	Windows, Powershell

La herramienta Routersploit se destacó por ser la herramienta más específica y orientada a dispositivos IoT, especialmente routers, siendo particularmente adecuada para llevar a cabo ataques de elevación de servicios en el sistema IoT. Además, esta herramienta proporciona exploits específicos para estos dispositivos.

Al acceder a RouterSploit, se inició la búsqueda de exploits que permitan vulnerar los dispositivos del sistema. En el primer ataque, el dispositivo objetivo fue el router del sistema, con dirección IP 192.168.1.1, como se identifica en la Figura 57.

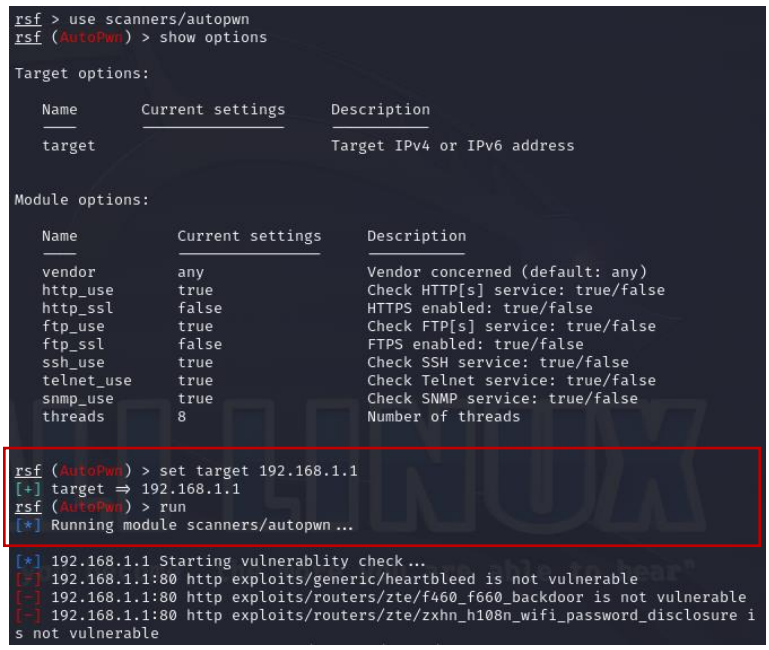


Figura 57. Búsqueda de exploits en el router del sistema con dirección ip 192.168.1.1

Sin embargo, tras finalizar la búsqueda de exploits en el dispositivo, en tan solo unos minutos, no se logró identificar ninguna vulnerabilidad que permitiera comprometer la seguridad del mismo. Este resultado evidenció la robustez del dispositivo router frente a los ataques explorados con RouterSploit, como se identifica en Figura 58.

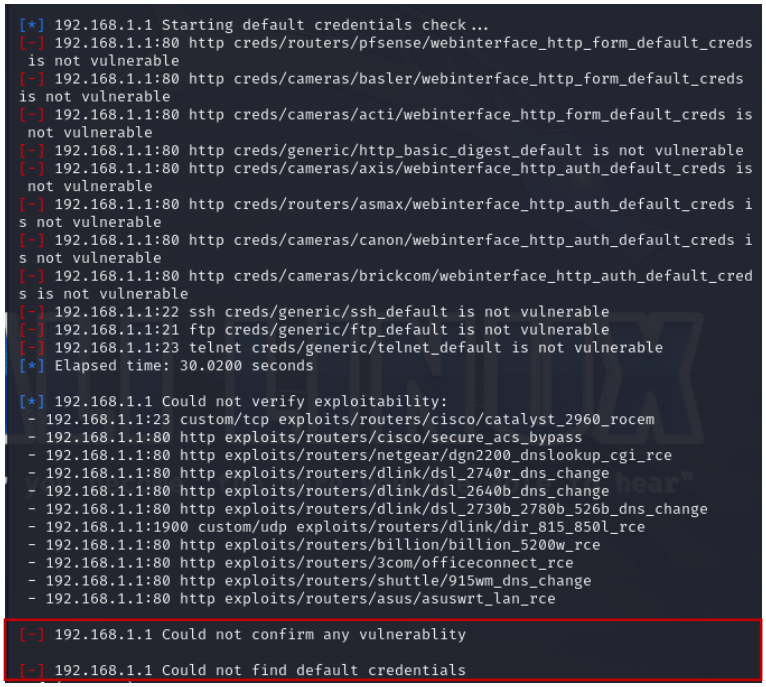


Figura 58. Resultados en la búsqueda de exploits en el dispositivo 192.168.1.1

A continuación, se realizó un segundo ataque mediante la herramienta RouterSploit, al dispositivo IoT identificado con la dirección IP 192.168.1.3, como se muestra en la Figura 59.

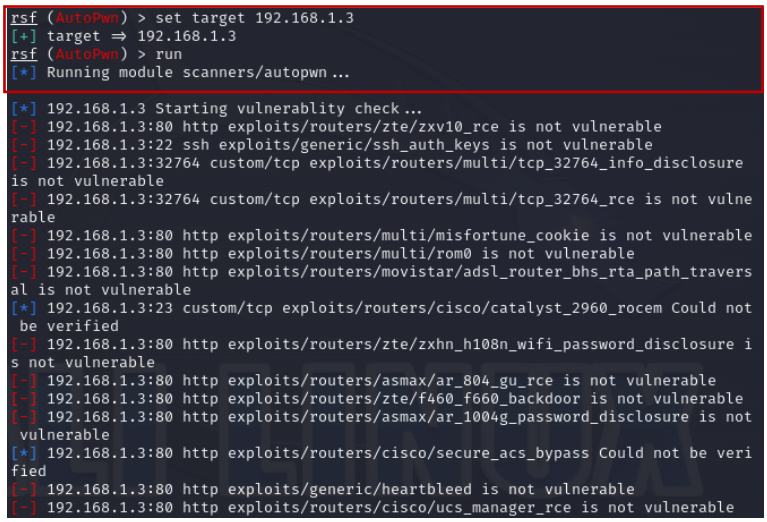


Figura 59. Búsqueda de exploits en el dispositivo IoT con dirección ip 192.168.1.3

Al finalizar la búsqueda de exploits en el dispositivo IoT, se identificó que es vulnerable mediante el exploit específico localizado en exploits /routers /linksys /eseries_themoon_r, identificado en la Figura 60.

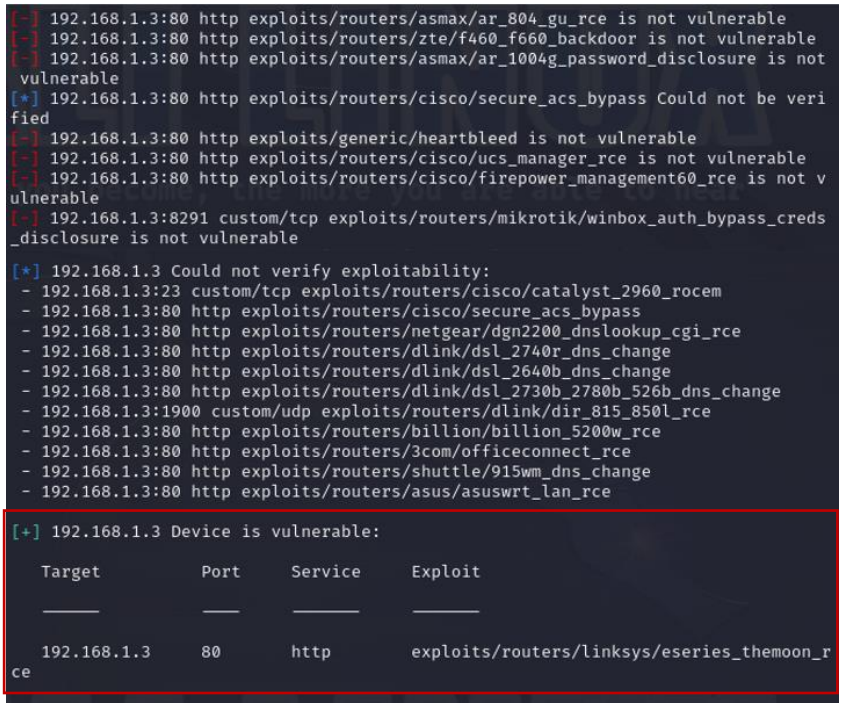


Figura 60. Resultados en la búsqueda de exploits en el dispositivo 192.168.1.3

A través de la ejecución del exploit identificado, se logró aprovechar la vulnerabilidad presente en el dispositivo IoT. Esto permitió un acceso no autorizado al sistema, como se indica en la Figura 61.

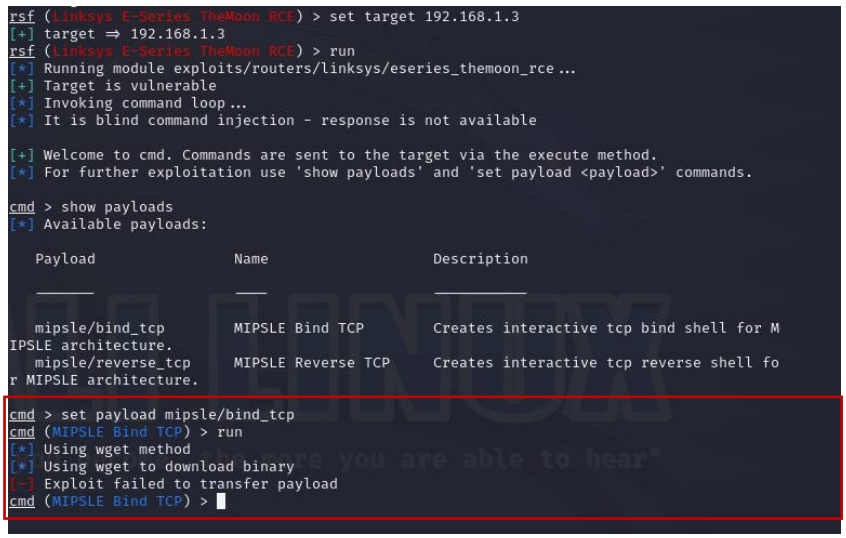


Figura 61. Acceso al sistema a través de la ejecución del exploit encontrado

Los ataques de explotación utilizando la herramienta RouterSploit, evidenciaron las vulnerabilidades en estos dispositivos. Aunque el primer intento en el router principal no tuvo éxito, el segundo ataque a un dispositivo específico IoT reveló una vulnerabilidad explotable, resaltando la implementación de actualizaciones y políticas de seguridad robustas para prevenir accesos no autorizados al sistema.

3.5.4 Resultados de la explotación en los dispositivos

La revisión de los resultados obtenidos durante la etapa de explotación en los dispositivos IoT ofrece una visión clara y detallada de lo que sucedió en cada tipo de ataque, como se muestra en la Tabla 27.

Tabla 27. Resultados en la explotación de los dispositivos

Explotación	Dispositivos	Resultados
Suplantación de identidad	Parlante de voz Echo Dot Alexa, dispositivo móvil, detector de movimiento PIR.	Se suplantó la identidad en la dirección MAC de los dispositivos y la identidad del router del sistema.
Manipulación de datos	Parlante de voz Echo Dot Alexa, interruptor de luz inteligente.	Se enviaron paquetes de información falsa desde la dirección ip de los dispositivos.
Repudio	Router, dispositivo móvil, bombilla inteligente color blanco, módulo regulador para luces, cámara inteligente.	Se modificó los protocolos ARP de los dispositivos y se congestionó la red.
Divulgación de Información	Router	Se obtuvo la contraseña de acceso al sistema.
Denegación de Servicios	Bombilla inteligente de colores, enchufe inteligente, sensor de contacto para la entrada.	Se realizó una inundación en el tráfico de la red hacia los dispositivos.
Elevación de privilegios	Router, bombilla inteligente de color blanco	Se obtuvo acceso a la configuración del dispositivo.

3.6 Post – Explotación

Después de llevar a cabo las pruebas de penetración, se procedió con la implementación de las medidas de seguridad en el sistema IoT, y, posteriormente, se realizó una nueva serie de pruebas de penetración para explorar el sistema y determinar si las vulnerabilidades identificadas previamente se mitigaron con las medidas de seguridad implementadas.

3.6.1 Implementación de medidas de seguridad

Las medidas de seguridad tienen como objetivo fortalecer la protección del sistema, reducir los riesgos de posibles ataques y mantener la integridad de los dispositivos interconectados. Su implementación pretende mitigar las vulnerabilidades descubiertas en el sistema, garantizando un entorno más seguro para los dispositivos. Las medidas específicas implementadas en distintos dispositivos del sistema, se detallan en la Tabla 28.

Tabla 28. Medidas de seguridad implementadas

Dispositivo	Medida de seguridad
Router	Asignación de direcciones IP a los dispositivos del sistema.
	Control de acceso basado en las direcciones MAC
	Aplicación de una contraseña fuerte y segura
Máquina del usuario	Implementación de una herramienta de monitoreo y control de las tablas del protocolo ARP
	Aplicación de un Firewall adicional al sistema.
Dispositivo móvil	Activación de las actualizaciones automáticas en los dispositivos.

a. Aplicación de la técnica IP-MAC Binding

A través del acceso al router del sistema, se identificaron los dispositivos conectados a la red, junto con sus direcciones IP y MAC respectivas. La técnica LAN-DHCP Binding, también conocida como IP-MAC Binding es un método de seguridad que permite vincular una dirección IP específica con una dirección MAC correspondiente. Esta configuración asegura que un dispositivo con una dirección MAC particular siempre reciba una dirección IP específica de la red local. En la Figura 62 se presenta la asignación IP-MAC correspondiente en los dispositivos del sistema IoT.

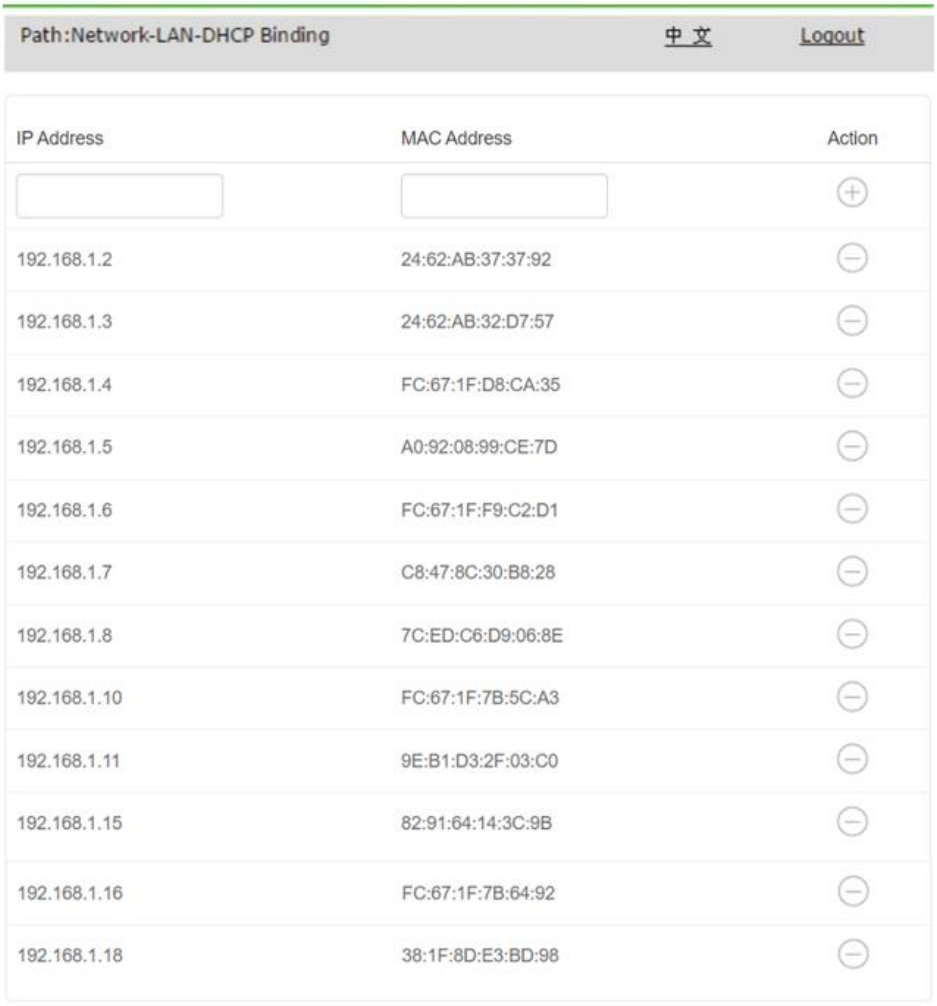


Figura 62. Tabla de Asignación IP-MAC

b. Configuración de acceso basado en las direcciones MAC

La configuración de acceso a partir de las direcciones MAC de los dispositivos permite una gestión adecuada de la red en el entorno de un hogar inteligente con dispositivos IoT. Al emplear esta configuración, se ha restringido el acceso a la red únicamente a los dispositivos cuyas direcciones MAC estén previamente autorizadas, lo que permite un nivel adicional de protección y control en el sistema. Esta configuración, se muestra en la Figura 63.

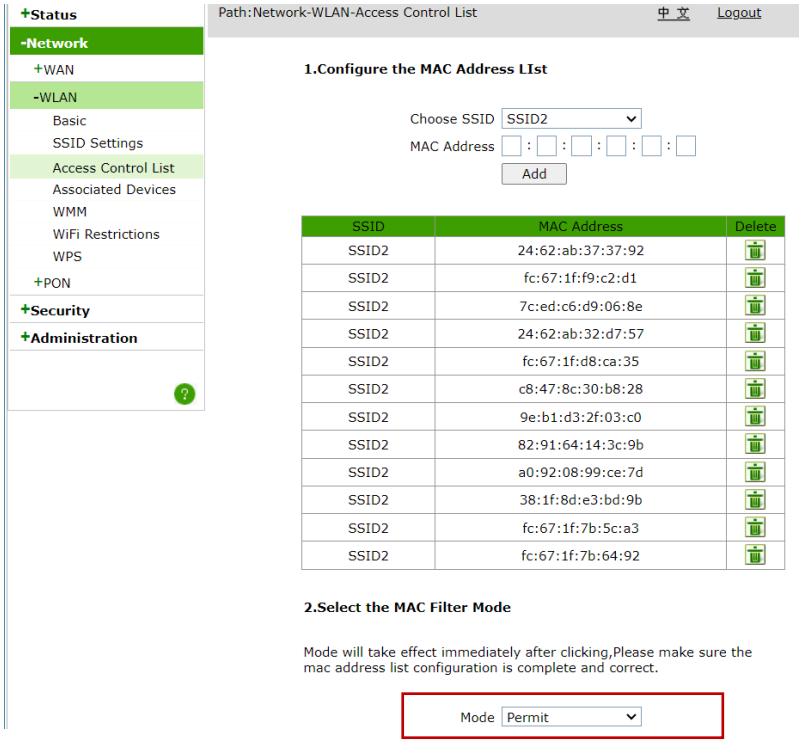


Figura 63. Control de Acceso basado en las direcciones MAC

c. Aplicación de contraseñas seguras

La implementación de una contraseña robusta y segura en el sistema IoT se basa en criterios específicos de seguridad, que requieren al menos 8 caracteres formados por una combinación de dígitos, letras y símbolos especiales. Además, es la aleatoriedad dentro de una contraseña lo que les brinda resistencia frente a métodos de ataque de fuerza bruta. La aplicación de una nueva contraseña más segura al sistema IoT del hogar inteligente, se identifica en la Figura 64.

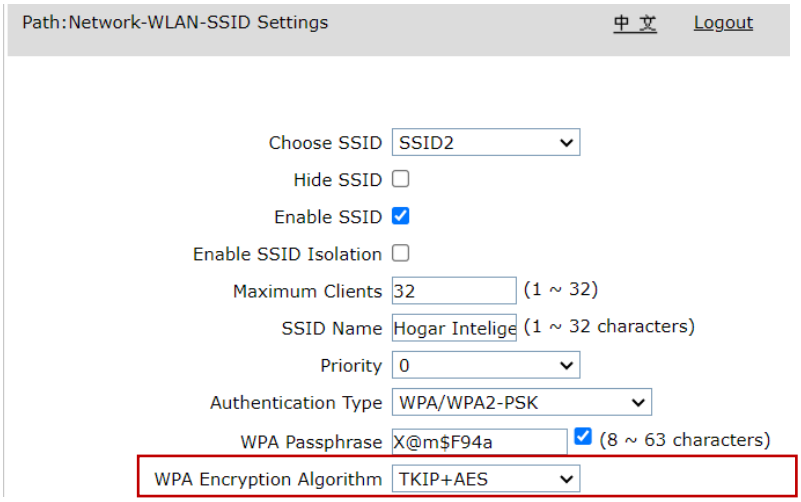


Figura 64. Aplicación de una contraseña segura al sistema IoT

d. Monitoreo de las tablas ARP

El protocolo ARP no cuenta con un mecanismo adecuado para la autenticación de información entre hosts, por lo que el monitoreo de estas tablas ARP en los dispositivos IoT es fundamental para mantener la integridad y seguridad de un sistema conectado. La Tabla 29 muestra la comparación realizada entre herramientas comúnmente utilizadas en la detección y prevención contra ataques de suplantación a los protocolos ARP.

Tabla 29. Herramientas para la de detección y prevención de ataques de suplantación a los protocolos ARP [54].

Herramienta	**Potencia de detección**	**Detección e inspección**	**Plataforma**	**Facilidad de uso**
ARPWatch	Medio	Requiere inspección manual	Linux	Requiere conocimientos técnicos
XArp	Moderada	Requiere inspección manual	Linux, Windows	Interfaz de usuario intuitiva
ARPAlert	Bajo	No requiere inspección manual	Linux	Requiere conocimientos técnicos

La herramienta XArp se muestra como la adecuada para el monitoreo de ARP en sistema IoT, debido a su capacidad de analizar y monitorear las tablas ARP de dispositivos IoT, identificando cambios inesperados o direcciones MAC desconocidas. Además, su interfaz de usuario intuitiva permite simplifica el proceso de configuración. La instalación de esta herramienta se muestra en el Anexo F y la información en tiempo real de las tablas ARP del sistema se muestra en la Figura 65.

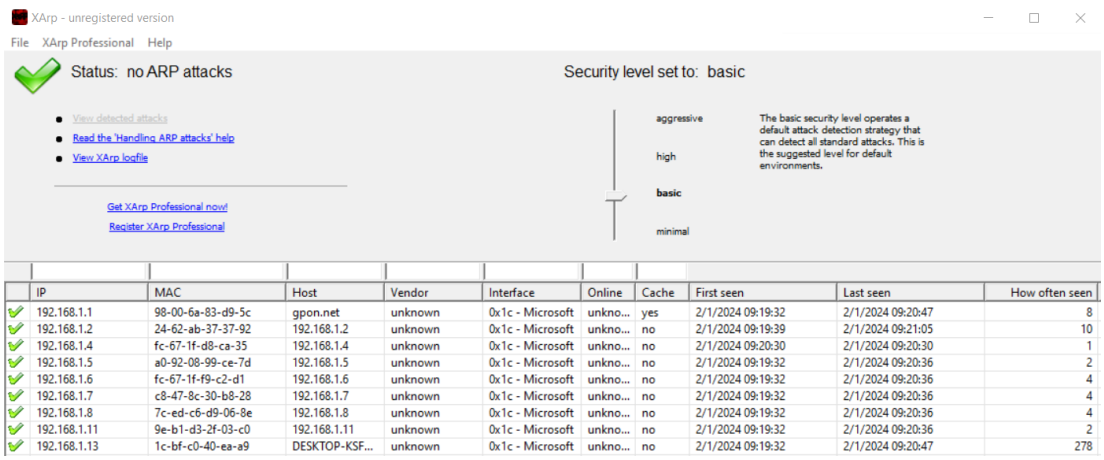


Figura 65. Monitoreo de las tablas ARP del sistema IoT

e. Aplicación de Firewalls

Los firewalls son dispositivos o softwares que controlan el tráfico de red entrante y saliente. Su principal función se basa en la protección del sistema contra amenazas cibernéticos, actuando como un escudo defensivo para la red. En este contexto, los firewalls ligeros se muestran como una opción adecuada para dispositivos con recursos limitados, como los IoT. La Tabla 30 presenta una comparación entre firewalls aplicables a dispositivos entornos IoT.

Tabla 30. Firewalls para entornos IoT [55], [56].

Características	**CrowdSec**	**Fail2Ban**	**SentinelOne**
Funciones	Detección y bloqueo de ataques de fuerza bruta, bots maliciosos, ataques DoS	Detección y bloque de ataques de fuerza bruta	Detección y prevención de amenazas, tales como malware, ransomware y pishing
Compatibilidad	Linux, MacOS y Windows	Linux	Windows, MacOS, Linux y sistemas móviles
Aplicaciones IoT	Muy Recomendable	Recomendable	Recomendable para organizaciones industriales
Interfaz	Intuitiva para el usuario	Intuitiva para el usuario	Requiere conocimientos técnicos
Precio	Gratuito y de código abierto	Gratuito y de código abierto	Comercial

El software CrowdSec se destaca principalmente por su adaptabilidad a sistemas IoT, donde estos estos dispositivos son constantemente víctimas de ataques de fuerza bruta, ya que son más vulnerables que los dispositivos tradicionales. Además, es compatible con una variedad de dispositivos IoT.

Después de instalar CrowdSec en la máquina del usuario, como se muestra en el Anexo G, se procedió a aplicar reglas de firewall basadas en la información recopilada por esta herramienta. A través del comando `cscli metrics`, se verificó la instalación exitosa de la herramienta, como se muestra en la Figura 66.

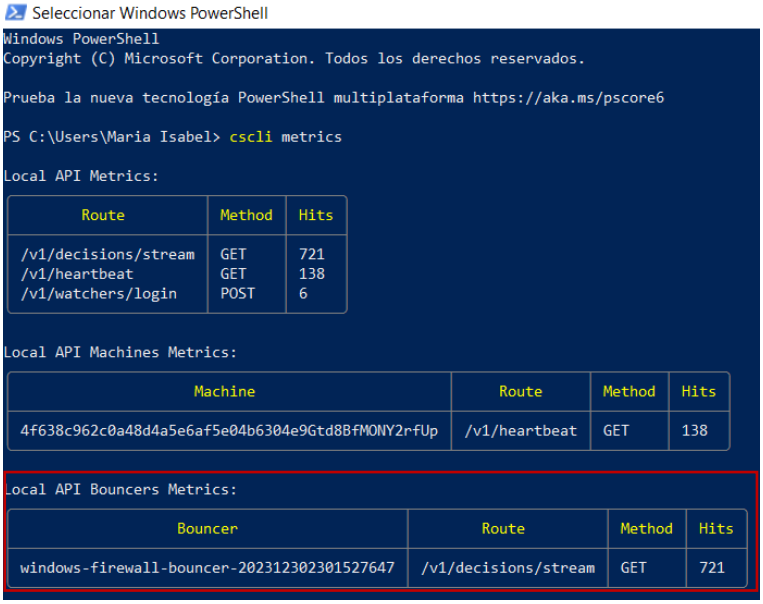


Figura 66. Verificación de la herramienta CrowdSec en el sistema

Se requiere la integración del firewall de CrowdSec al sistema mediante la ejecución del comando `cscli bouncers add firewall`, como se muestra en la Figura 67, para habilitar y activar las funciones de protección que ofrece la herramienta. Al agregar el firewall, se establecen las bases necesarias para CrowdSec funcione de manera efectiva, permitiendo que el sistema adquiera las funciones de detección y respuesta ante amenazas.

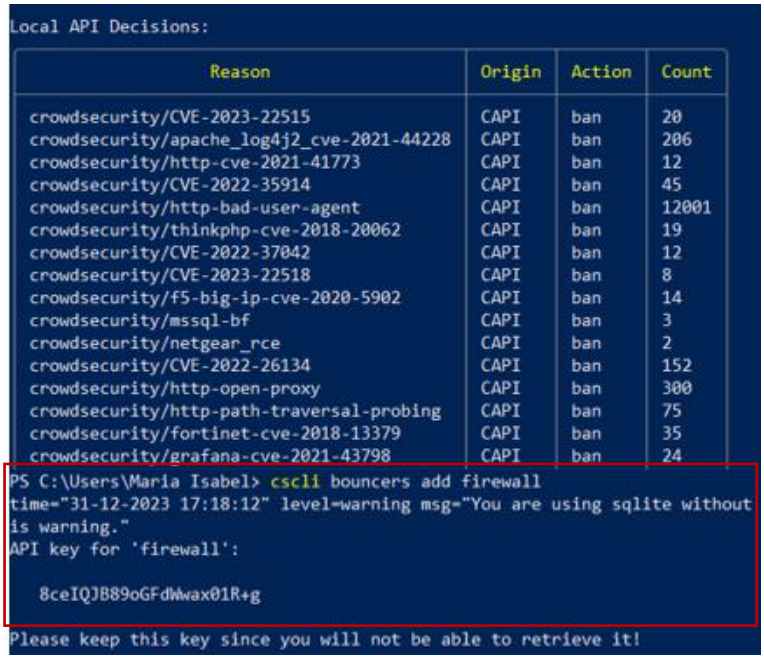


Figura 67. Configuración del Firewall de CrowdSec

A continuación, se requiere inicializar el servicio correspondiente a CrowdSec a través de los servicios del sistema, como se muestra en la Figura 68Figura 68. Esto garantiza el correcto funcionamiento de la herramienta, permitiéndole llevar a cabo de manera constante y efectiva las funciones de monitoreo y protección en el entorno de la red.

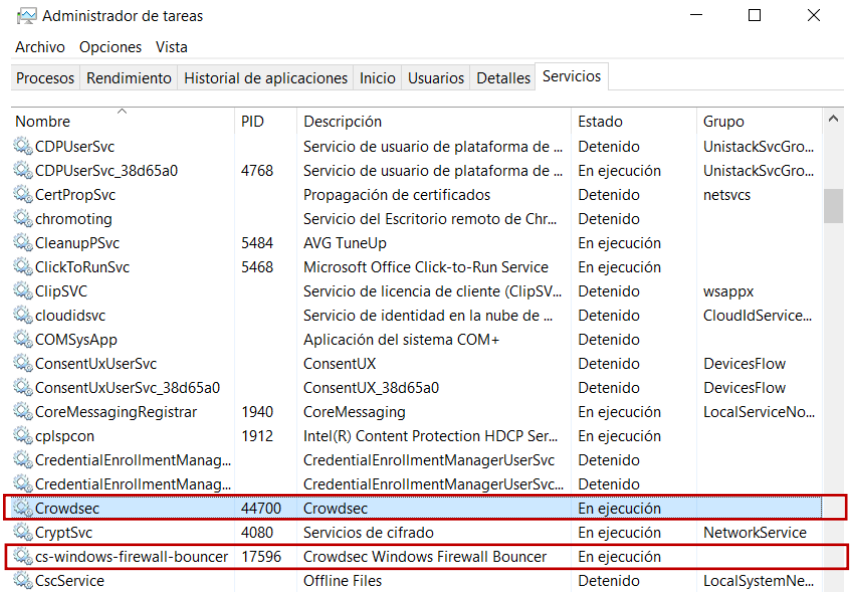


Figura 68. Ejecución de los servicios de CrowdSec

A través de la configuración del Windows Defender Firewall con seguridad avanzada, se puede obtener información detallada del funcionamiento y la interacción de CrowdSec en la red. Esta configuración, presentada en la Figura 69, permite observar los registros de las reglas y los eventos de seguridad asociados a este firewall.

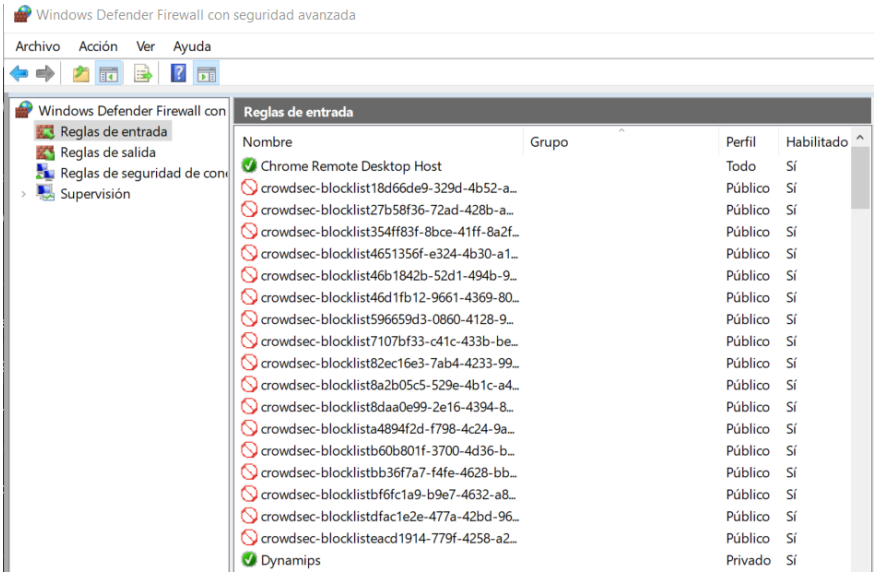


Figura 69. Registros y eventos de seguridad asociados a CrowdSec

f. Actualizaciones en los dispositivos IoT

Las actualizaciones de software en lo dispositivos IoT permiten fortalecer su protección contra vulnerabilidades. Es esencial que los usuarios verifiquen y aseguren actualizaciones periódicas en estos dispositivos. Esta práctica constante garantiza no solo el correcto funcionamiento del sistema, sino que también mejora progresivamente la seguridad de los dispositivos IoT. La Figura 70, presenta la activación de actualizaciones en los dispositivos IoT a través de las aplicaciones móviles utilizadas para su control y monitoreo.

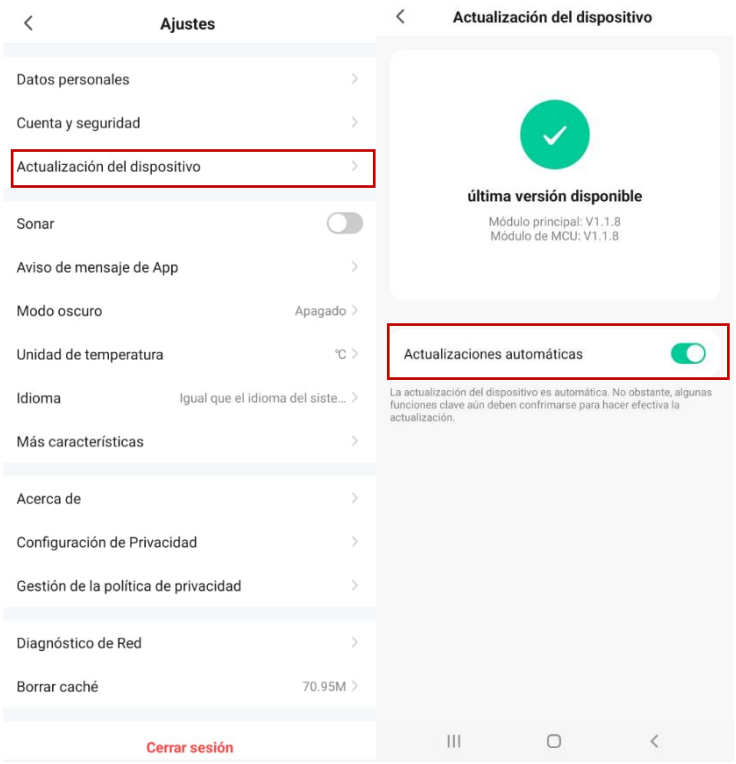


Figura 70. Activación de actualizaciones automáticas en los dispositivos IoT

3.6.2 Explotación Post – Medidas de seguridad

Tras la implementación de las medidas de seguridad en el sistema IoT, se procedió a realizar nuevamente las pruebas de penetración según el modelo de amenazas establecido, para determinar la eficacia de las soluciones adoptadas y el nivel de mitigación de las vulnerabilidades presentes.

a. Suplantación de Identidad

El intento de cambiar la dirección MAC del adaptador utilizando la herramienta macchanger, con la finalidad de adoptar la identidad de un dispositivo IoT de la red, se vio impedido por las restricciones de control de acceso a la red. En la Figura 71 se presenta el mensaje de error específico obtenido al tratar de ejecutar este ataque.

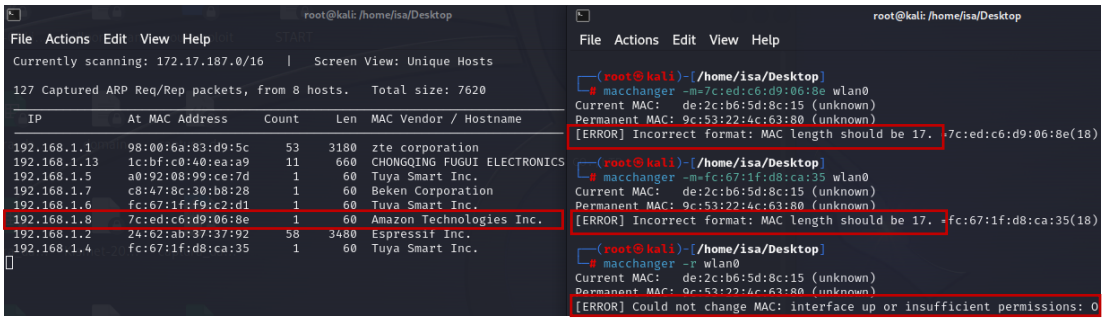


Figura 71. Intento de modificación en la dirección MAC del adaptador

Por otra parte, la herramienta Bettercap facilitó el inicio de un ataque `arp.spoof` a los dispositivos IoT seleccionados, aunque con una velocidad más lenta en comparación con el ataque inicial. Sin embargo, como se muestra en la Figura 72, al intentar utilizar el comando `net.sniff` para analizar el tráfico de red, esta acción no se completó satisfactoriamente.

Figura 72. Resultados en el intento de ataque de Bettercap

b. Manipulación de datos

El intento de creación y manipulación de paquetes, mediante Scapy, se vio impedido por el sistema. Esto debido a las medidas de seguridad, como firewalls y actualizaciones que interfirieron en el funcionamiento adecuado de este tipo de ataques. El intento de creación y manipulación de paquetes mediante la función

`send(IP(src="192.168.1.8", dst = "192.168.1.1") / TCP(sport=80, dport=80), count= 2000)`, la cual estaba diseñada para enviar 2000 paquetes TCP desde la dirección IP de origen “192.168.1.8” hacia la dirección de destino “192.168.1.1” a través del puerto 80. Sin embargo, el sistema envío un mensaje de error en el cual indicaba que el atacante no podía establecer la comunicación con el router, como se identifica en la Figura 73.

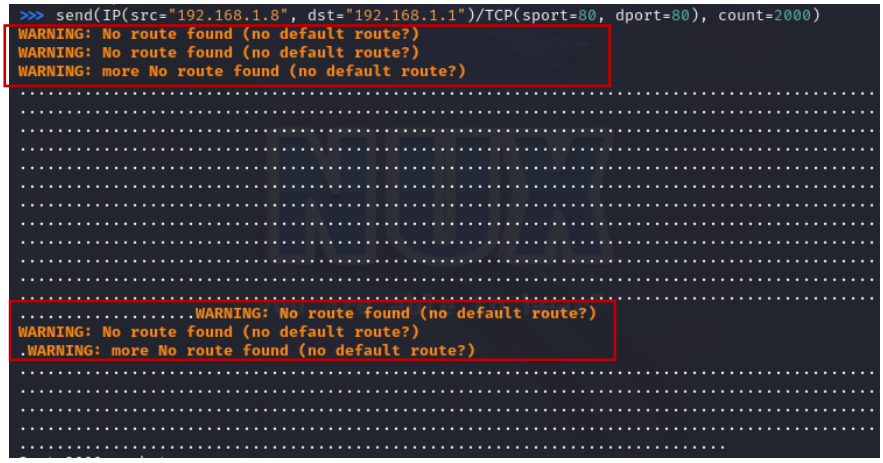


Figura 73. Intento de creación de paquetes TCP desde la ip 192.168.1.8

De igual manera, el intento de creación y manipulación de paquetes mediante la función `send(IP(src="192.168.1.4", dst = "192.168.1.1") / TCP(sport=80, dport=80), count= 2000)`, la cual estaba diseñada para enviar 2000 paquetes TCP desde la dirección IP de origen “192.168.1.4” hacia la dirección de destino “192.168.1.1” a través del puerto 80, tampoco pudo ser completada. El sistema envío el mismo mensaje de error en el cual indicaba que el atacante no podía establecer la comunicación con el router, indicado en la Figura 74.

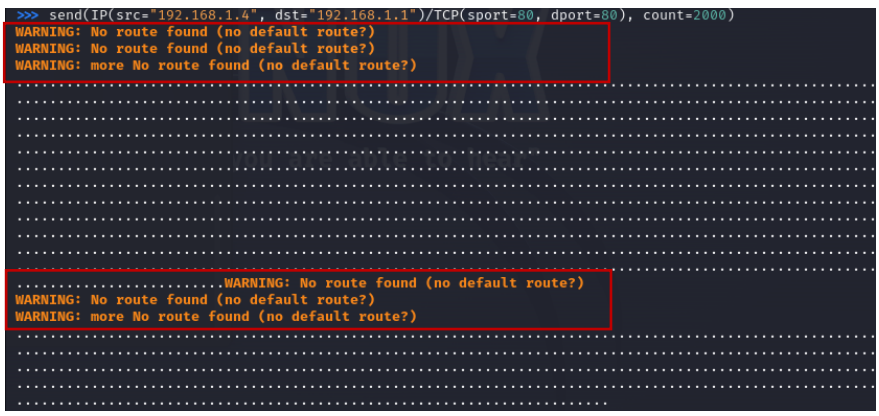


Figura 74. Intento de creación de paquetes TCP desde la ip 192.168.1.4

c. Repudio

El intento de ejecución del ataque ARP Poisoning, el cual implica la manipulación de tablas de direcciones ARP para redirigir el tráfico, no tuvo éxito. La herramienta Ettercap no logró identificar los dispositivos host conectados al sistema, resultando en la incapacidad de llevar a cabo el ataque de manera exitosa, como se muestra en la Figura 75, esto debido al bloqueo de ataques ARP que ejecuta la herramienta XArp. Además, cabe destacar que, durante este proceso, esta herramienta emitió una alerta, informando al usuario sobre el intento de este ataque y proporcionando una capa adicional de seguridad al sistema.

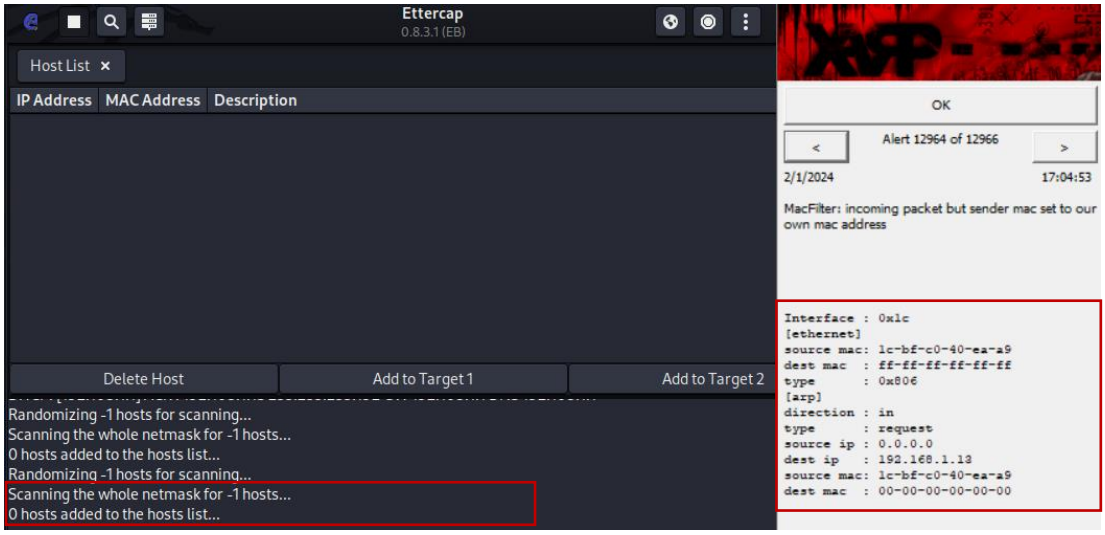


Figura 75. Intento de ataque a las tablas ARP y notificación de alerta en XArp

d. Divulgación de Información

La utilización de la suite Aircrack-ng para obtener credenciales resultó en un tiempo de descifrado considerable, superando las 17 horas. Este período extenso resalta la complejidad del proceso, principalmente si se tiene en cuenta el intento de ataque anterior, que logró acceder a la información de la contraseña en un tiempo aproximado de una hora. Este contraste sugiere que, a medida que la contraseña se vuelve más segura, el tiempo que un atacante utiliza para descifrarla aumenta significativamente, como se muestra en la Figura 76.

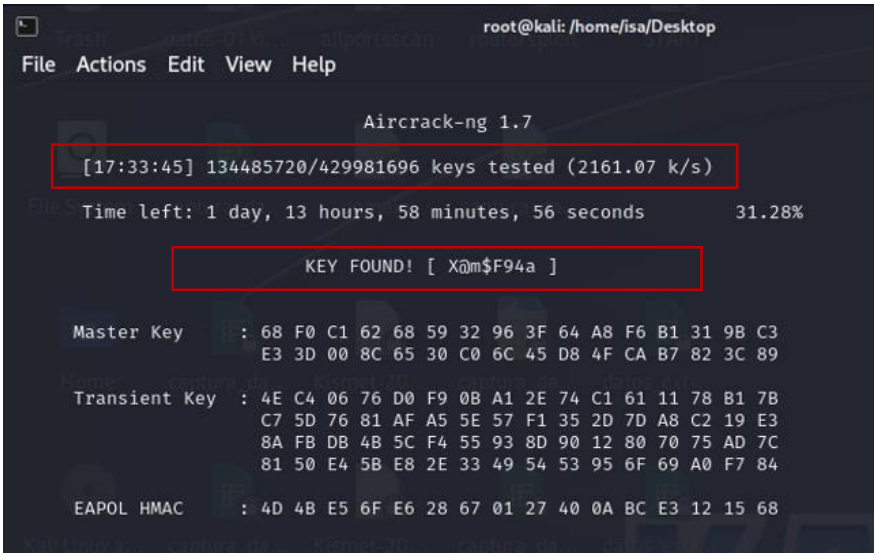


Figura 76. Resultados en la obtención de clave de acceso a la red

Además, la implementación de una contraseña más sólida y segura, también impidió la obtención de credenciales mediante la herramienta Wifite. A pesar de prolongar el tiempo en este intento de ataque con respecto al ataque inicial, no se lograron obtener resultados, como se observa en la Figura 77.

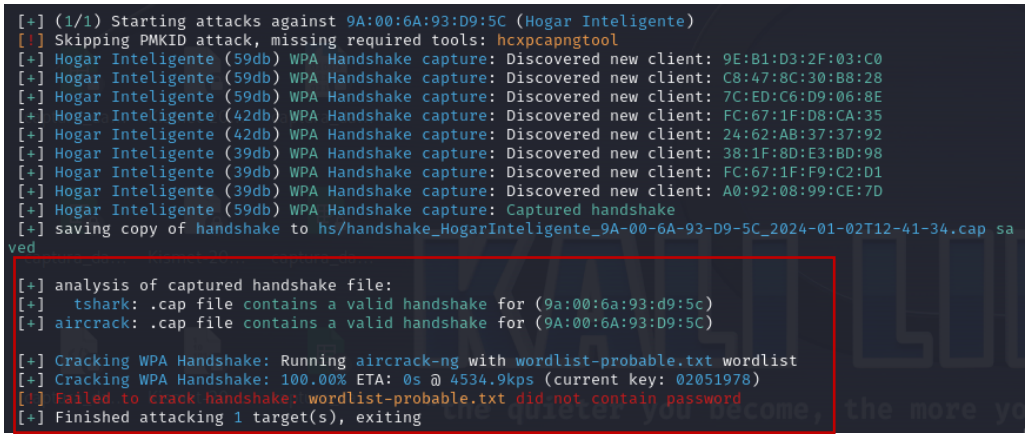


Figura 77. Resultados en el intento de obtención de credenciales mediante Wifite

e. Denegación de Servicios

La ejecución de la herramienta hping3 utilizada para generar y enviar paquetes personalizados no fue exitosa. A pesar de que al ingresar el comando en la terminal no se presentó un mensaje de error o advertencia, la observación del tráfico de red mediante Wireshark reveló que la generación de paquetes no estaba ocurriendo como se esperaba. La poca cantidad de paquetes que se registraron mostraron el mensaje

"host unreachable", como se muestra en la Figura 78, indicando que el dispositivo de destino no era accesible. Además, durante este intento de ataque, se recibió una alerta de XArp, indicando al usuario el intento de este ataque en la red.

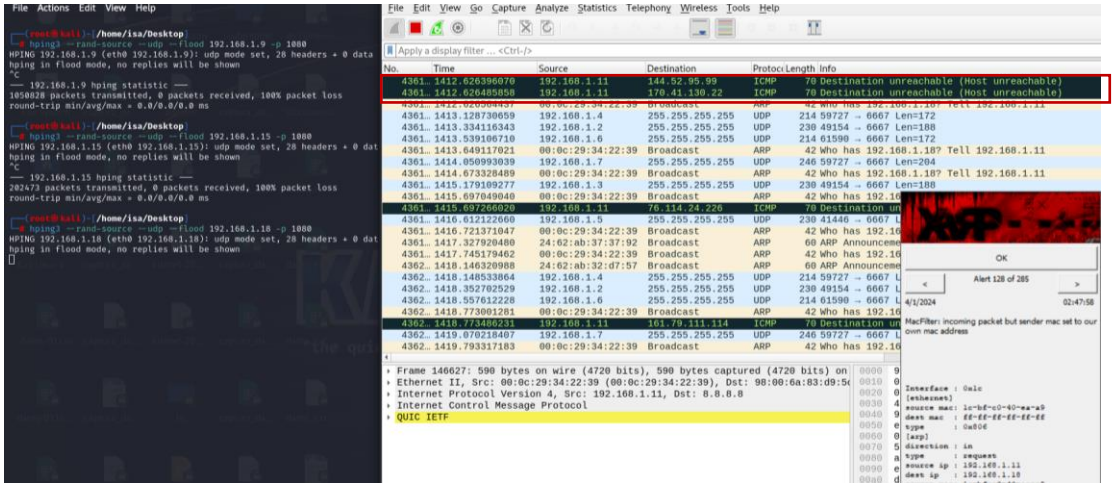


Figura 78. Resultados en el intento de ataque con hping3 y alerta de XArp

f. Elevación de privilegios

La utilización de RouterSploit para identificar y explotar vulnerabilidades en el sistema demandó más tiempo en comparación con la etapa de explotación previa a la implementación de las medidas de seguridad. Se inició la búsqueda de exploits que pudieran vulnerar el dispositivo con dirección IoT con dirección ip 192.168.1.3, como se identifica en la Figura 79.

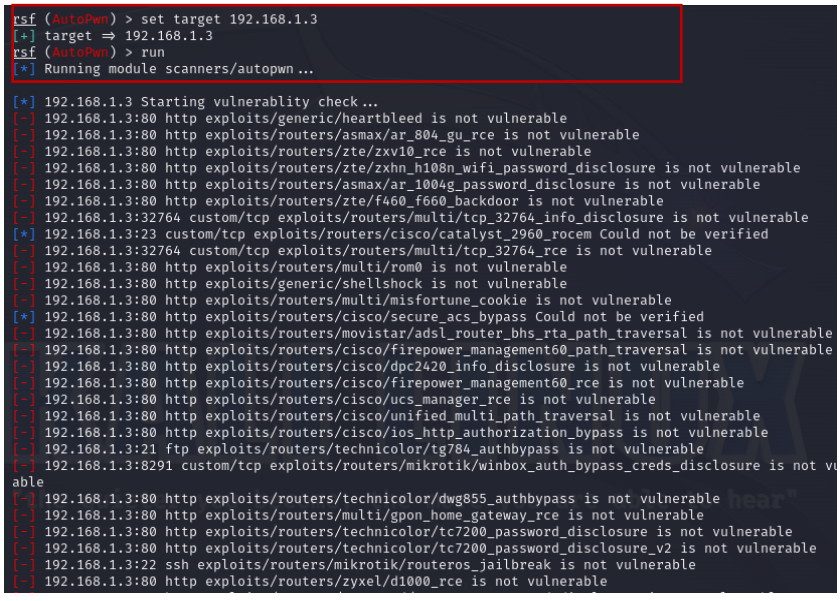


Figura 79. Búsqueda de exploits en el dispositivo IoT con dirección ip 192.168.1.3

Sin embargo, después de concluir la búsqueda de exploits en el dispositivo, no se lograron identificar vulnerabilidades que pudieran comprometer la seguridad del mismo. Este resultado muestra la robustez adquirida por los dispositivos IoT, destacando la efectividad del conjunto de medidas de seguridad implementadas. La visualización de este resultado, se muestra en la Figura 80.

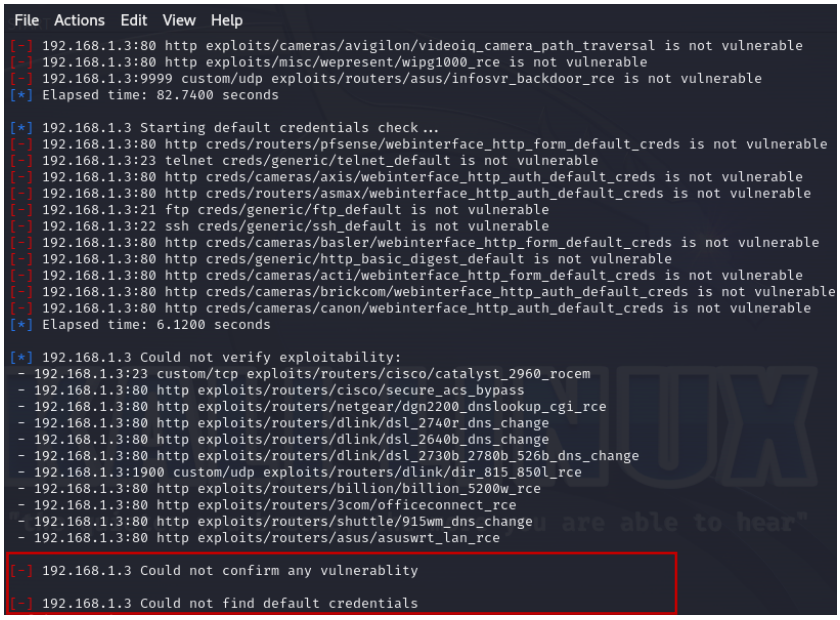


Figura 80. Resultados en la búsqueda de exploits en el dispositivo 192.168.1.3

3.7 Evaluación de la efectividad en las medidas de seguridad

Para la evaluación de la efectividad en las medidas de seguridad del sistema IoT, es necesario llevar a cabo un análisis de los resultados obtenidos tras la realización de pruebas de penetración. La revisión detallada de los registros de las pruebas, los informes de vulnerabilidades y los resultados de las evaluaciones de seguridad indican cómo las medidas de seguridad han respondido a los intentos de ataque al sistema.

3.7.1 Análisis de resultados en las pruebas de penetración

Las pruebas de penetración se llevaron a cabo con el objetivo de analizar la resistencia del sistema IoT frente a potenciales amenazas y ataques. La etapa de explotación permitió identificar vulnerabilidades y puntos débiles en el entorno IoT, mientras que la implementación de medidas de seguridad tuvo como objetivo mitigar estas vulnerabilidades y fortalecer la protección del sistema. La Tabla 31 presenta el análisis

de resultados para las pruebas de penetración realizadas en la etapa de explotación y en la etapa de explotación post - medidas de seguridad.

Tabla 31. Análisis de Resultados en las Pruebas de Penetración

Resultados en las pruebas de penetración			
	Etapa de Explotación	Etapa de Explotación Post-Medidas de Seguridad	Conclusiones
Suplantación de Identidad	A través de macchanger se cambió la dirección MAC del adaptador inalámbrico por las direcciones MAC de los dispositivos IoT.	El cambio de dirección MAC en el adaptador inalámbrico no se ejecutó, debido a las medidas implementadas para el control de acceso basado en la dirección MAC.	La implementación de medidas de control de acceso basadas en la dirección MAC restringieron los intentos de cambio de dirección MAC en el adaptador inalámbrico.
	A través de Bettercap, se engañó a los dispositivos IoT para que envíe creyeran que la dirección MAC del atacante era del router y así redirigir su tráfico de datos.	Se empezó la ejecución del ataque en los dispositivos IoT. Sin embargo, debido a la aplicación de Firewalls el análisis del tráfico de red no se completó adecuadamente.	La presencia y la acción de Firewalls limitaron la eficacia del ataque al dificultar el análisis completo del tráfico de red.
Manipulación de datos	La creación y manipulación de paquetes a través de Scapy, utilizando direcciones IP de los dispositivos IoT, se ejecutó exitosamente.	La generación de paquetes no se completó ya que el atacante no logró establecer la comunicación con el router. Esto como resultado del uso de Firewalls que restringieron esta conexión.	La presencia de Firewalls limitó la conexión del atacante y los paquetes de datos no se generaron adecuadamente debido a la falta de comunicación con el router.
Repudio	El tráfico de datos entre los dispositivos IoT y el atacante fue interceptado y modificado. Además, se consiguió acceso a las credenciales de usuario en los dispositivos IoT.	No fue posible la manipulación de tablas ARP para redirigir el tráfico de datos. La herramienta XArp emitió un mensaje de alerta al usuario sobre este intento de ataque.	La manipulación de las tablas ARP para redirigir el tráfico no tuvo éxito, debido al monitoreo y análisis ARP realizado por la herramienta XArp.
Divulgación de Información	El uso de contraseña débil posibilita que un atacante acceda a las credenciales de acceso al sistema en un tiempo estimado de alrededor de una hora.	El cambio de una contraseña por una más sólida y robusta muestra que el atacante podría estar accediendo a las credenciales de acceso al sistema en un tiempo estimado de alrededor de 17 horas.	El cambio de una contraseña débil a una más sólida y robusta representa un incremente significativo en la resistencia del sistema ante ataques.
Denegación de Servicios	La creación y envío masivo de paquetes utilizando Hping3 generó una interrupción en los servicios de los dispositivos IoT.	A pesar de la ausencia de mensajes de error o advertencias durante la ejecución de Hping3, el análisis del tráfico de red a través de Wireshark reveló la inadecuada de paquetes. Esto como resultado de la asignación de direcciones IP estáticas en los dispositivos.	La presencia de direcciones IP estáticas en los dispositivos, impidió este tipo de ataques y, además, permitió un seguimiento más minucioso al sistema.

Resultados en las pruebas de penetración			
	Etapa de Explotación	Etapa de Explotación Post-Medidas de Seguridad	Conclusiones
Elevación de Privilegios	La identificación y explotación de vulnerabilidades mediante Routersploit permitieron el acceso no autorizado al sistema.	La búsqueda de vulnerabilidades tomó más tiempo del requerido inicialmente debido a la presencia de firewalls en el sistema, además, no fue posible encontrar exploits que permitan vulnerar los dispositivos IoT.	La búsqueda de vulnerabilidades se vio obstaculizada por la presencia de firewalls, que incrementaron el tiempo requerido para esta acción. Además, no fue posible encontrar exploits que permitan vulnerar los dispositivos IoT.

3.7.2 Análisis de vulnerabilidades en el sistema IoT

Tras la implementación de las medidas de seguridad, se realizó un nuevo escaneo de vulnerabilidades en los dispositivos del sistema IoT, empleando la herramienta Nessus. Este proceso tiene como propósito validar la eficacia de las medidas implementadas en el fortalecimiento de la seguridad del sistema. A través de la utilización de Nessus, se busca obtener una evaluación actualizada y detallada del estado de las vulnerabilidades en el entorno de dispositivos IoT. Los resultados obtenidos en el nuevo escaneo de vulnerabilidades del sistema IoT indican la ausencia de las vulnerabilidades críticas, como se muestra en la Figura 81.

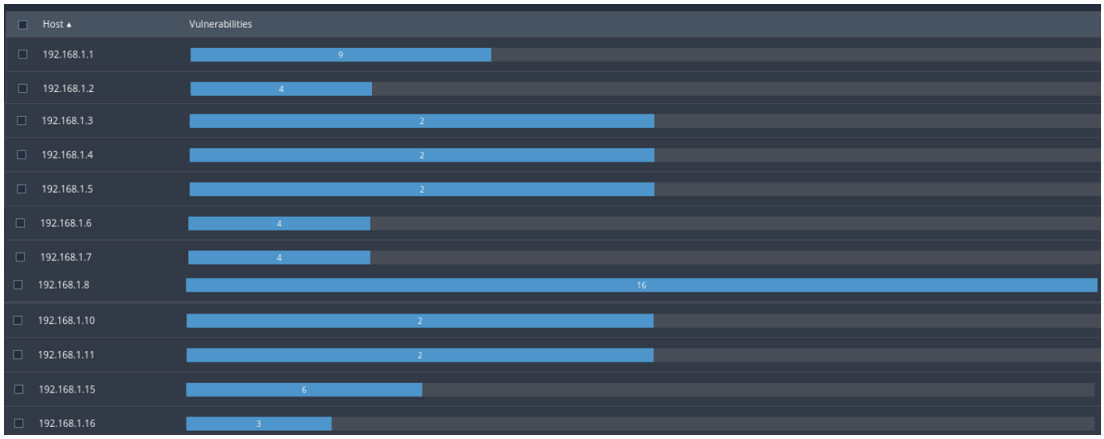


Figura 81. Escaneo de vulnerabilidades en el sistema IoT con Nessus

3.7.3 Efectividad en las medidas de seguridad del sistema IoT

A partir de la identificación de vulnerabilidades en el sistema IoT, se realizó un análisis para evaluar la efectividad de las medidas de mitigación aplicadas. La fórmula para calcular el porcentaje de efectividad, se muestra en la Ecuación 1

$$\% \text{ de efectividad} = ((\text{V. inicial} - \text{V. final})) / \text{V. inicial}) * 100\% \quad (1)$$

En donde:

V. inicial = Número de vulnerabilidades previo a las medidas de seguridad

V. final = Número de vulnerabilidades después de implementar las medidas de seguridad

% de efectividad = Porcentaje de la efectividad en la mitigación de vulnerabilidades.

El análisis correspondiente se detalla en la Tabla 32, donde se contrastan las vulnerabilidades identificadas inicialmente con las detectadas después implementar mediades de seguridad específicas, para una evaluación cuantitativa sobre la eficacia de las estrategias empleadas en la protección del sistema IoT.

Tabla 32. Comparativa entre las vulnerabilidades iniciales y finales en el sistema IoT

Dispositivo	**Dirección IP**	**Vulnerabilidades Iniciales**	**Vulnerabilidades Finales**
Router	192.168.1.1	29	9
Bombilla LED inteligente color blanco	192.168.1.2	6	4
Bombilla LED inteligente color blanco	192.168.1.3	11	2
Interruptor de luz inteligente	192.168.1.4	7	2
Cámara inteligente para interiores	192.168.1.5	5	2
Enchufe inteligente	192.168.1.6	7	4
Bombilla LED inteligente de colores	192.168.1.7	10	4
Parlante de voz Echo Dot Alexa	192.168.1.8	33	16
Sensor de contacto para puertas y ventanas	192.168.1.10	12	2
Dispositivo Móvil	192.168.1.11	4	2
Detector de movimiento PIR con alarma	192.168.1.15	10	4
Sensor de contacto para puertas y ventanas	192.168.1.16	7	2
Módulo regulador para luces	192.168.1.18	12	2
Total		153	55

El cálculo de la efectividad obtenida en la mitigación del sistema, se muestra en la Ecuación 2.

$$\% \text{ de efectividad} = ((153 - 55)) / 153) * 100\% \quad (2)$$

$$\% \text{ de efectividad} = 64{,}052$$

La reducción de vulnerabilidades es evidente en todos los dispositivos evaluados, destacándose principalmente en el interruptor de luz inteligente, las bombillas LED de colores y blanco, la cámara inteligente para interiores, el dispositivo móvil, los sensores de contacto para puertas y ventanas, y el modulador regulador para luces. Sin embargo, es importante señalar que el parlante de voz Echo Dot Alexa, y el router del sistema, aún conservan un nivel de vulnerabilidades ligeramente superior en comparación con los demás dispositivos evaluados. El cálculo de la efectividad, expresado como un porcentaje de reducción en las vulnerabilidades totales, alcanzó un 64,052 %, indicando una eficacia significativa en la mitigación de riesgos.

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- La revisión de información en fuentes científicas identificó que los principales riesgos y vulnerabilidades de los sistemas IoT en hogares inteligentes, tales como intercepción de mensajes, contraseñas débiles y gestión inadecuada de los dispositivos. Para contrarrestar esto, se utilizan medidas como configuración adecuada de los routers, contraseñas fuertes, redes Wi-Fi separadas y actualizaciones regulares en los dispositivos. Además, se determinó que la metodología PTES es la más adecuada para llevar a cabo el proceso de evaluación mediante pruebas de penetración.

- La ejecución de las pruebas de penetración permitió al atacante utilizar la identidad de los dispositivos IoT y manipular la dirección MAC del router para redirigir el tráfico hacia él, empleando herramientas como macchanger y Bettercap; generar paquetes falsificados mediante Scapy; manipular las tablas del protocolo ARP con ettercap; descifrar la clave de la red utilizando diccionarios, a través de la suite Aircrack-ng. Además, se aumentó el tráfico de datos con información de direcciones aleatorias mediante hping3, y se accedió al sistema explotando vulnerabilidades con RouterSploit. Es importante destacar que, durante ese proceso, los dispositivos IoT perdieron su conexión al sistema y requirieron una reconfiguración.

- Las medidas de seguridad se implementaron en tres componentes esenciales del sistema: el router, la máquina del usuario y el dispositivo móvil. En cada uno de ellos, se llevaron a cabo configuraciones específicas para fortalecer la seguridad, tales como asignación de direcciones IP estáticas, control de acceso para las direcciones MAC y aplicación de contraseñas seguras. Se instalaron herramientas como XArp y CrowdSec para el monitoreo y control de la red. Por último, se activaron las actualizaciones automáticas en los dispositivos, para que se mantengan con las últimas correcciones de seguridad disponibles.

- Después de la implementación de las medidas de seguridad en el sistema, se llevaron a cabo nuevamente pruebas de penetración para evaluar su eficacia en el sistema, lo que demostró una reducción general de las vulnerabilidades y un fortalecimiento de la seguridad, principalmente en los dispositivos de iluminación, seguridad y vigilancia y el dispositivo móvil. Sin embargo, se observó que el parlante de voz Echo Dot Alexa y el router del sistema aún mantienen un nivel considerable de vulnerabilidades. Además, un análisis cuantitativo entre las vulnerabilidades iniciales y las posteriores a las medidas de seguridad, mostró una mitigación de 64,052% en el sistema IoT.

4.2 Recomendaciones

- Es recomendable realizar una investigación continua sobre las tendencias de seguridad en sitios web y fuentes reconocidas en ciberseguridad, páginas como Cisco y la revista “Security Today” proporcionan informes actualizados y análisis sobre amenazas emergentes en sistemas IoT. Además, sitios como la Fundación OWASP y el instituto NIST también ofrecen documentos y pautas importantes en la seguridad IoT. Se sugiere revisar estas fuentes al menos una vez al mes para mantenerse al tanto de desarrollos recientes.

- Para mejorar la amplitud y la profundidad de las pruebas de penetración en sistemas IoT, se sugiere adoptar un enfoque dinámico, realizando las pruebas desde diferentes ubicaciones geográficas y utilizando entornos de nubes. Este enfoque permitirá simular escenarios realistas y evaluar la resistencia del sistema IoT frente a amenazas potenciales desde diversas redes y ubicaciones.

- A medida que el entorno de sistemas IoT se amplía en el hogar, es recomendable explorar opciones adicionales para fortalecer su protección. La adquisición de antivirus reconocidos en este ámbito, como Norton o Bitdefender, puede brindar una capa adicional de protección contra amenazas; o firewalls avanzados, como el modelo Fortinet FortiGate o Cisco Meraki, permitiría un control más fuerte sobre el tráfico de red. Además, explorar ofertas de proveedores de internet que ofrezcan servicios de seguridad adicionales, también sería una solución para la protección del entorno IoT.

REFERENCIAS BIBLIOGRÁFICAS

[1] ARCOTEL, «Boletín Estadístico del sector de las Telecomunicaciones», Agencia de Regulación y Control de las Telecomunicaciones, abr. 2022. [En línea]. Disponible en: https://www.arcotel.gob.ec/wp-content/uploads/2022/06/Boletin-estadistico-mensual-actualizado-al-mes-de-abril-2022.pdf

[2] ARCOTEL, «Boletín Estadístico del sector de las Telecomunicaciones», Agencia de Regulación y Control de las Telecomunicaciones, dic. 2022. [En línea]. Disponible en: https://www.arcotel.gob.ec/abonados-y-usuarios/

[3] ARCOTEL, «Boletín Estadístico del sector de las Telecomunicaciones», Agencia de Regulación y Control de las Telecomunicaciones, may 2023. [En línea]. Disponible en: https://www.arcotel.gob.ec/lineas-activas/

[4] F. Cuzme Rodríguez, «El Internet de las Cosas y las consideraciones de seguridad», p. 179, abr. 2019.

[5] M. Barrio Andrés, *Internet Of ThingsInternet de las Cosas*. Editorial Reus, 2018. doi: 10.30462/9788429020380.

[6] G. M. García Villafuerte, «Análisis de vulnerabilidades en sistemas de automatización del hogar», masterThesis, Universidad Casa Grande. Departamento de Posgrado, 2023. Accedido: 8 de julio de 2023. [En línea]. Disponible en: http://dspace.casagrande.edu.ec:8080/handle/ucasagrande/3967

[7] A. Aldahmani, B. Ouni, T. Lestable, y M. Debbah, «Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends», *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 281-292, 2023, doi: 10.1109/OJVT.2023.3234069.

[8] A. Bhardwaj, K. Kaushik, M. Alshehri, A. A.-B. Mohamed, y I. Keshta, «ISF: Security Analysis and Assessment of Smart Home IoT-based Firmware», *ACM Trans. Sen. Netw.*, ene. 2023, doi: 10.1145/3578363.

[9] E. Anthi, «Detecting and defending against cyber attacks in a smart home Internet of Things ecosystem», phd, Cardiff University, 2022. Accedido: 25 de septiembre de 2023. [En línea]. Disponible en: https://orca.cardiff.ac.uk/id/eprint/148044/

[10] R. Akhilesh, O. Bills, N. Chilamkurti, y M. J. M. Chowdhury, «Automated Penetration Testing Framework for Smart-Home-Based IoT Devices», oct. 2022, doi: 10.26181/24041496.v1.

[11] C. B. Ynzunza Cortés, J. M. Izar Landeta, y J. G. Bocarando Chacón, «El Entorno de la Industria 4.0: Implicaciones y Perspectivas Futuras», 2017.

[12] J. L. del Val Román, «Industria 4.0: la transformación digital de la industria», en *Valencia: Conferencia de Directores y Decanos de Ingeniería Informática, Informes CODDII*, 2016.

[13] J. D. Déniz Cerpa, *Sistemas ciberfísicos (CPS) reconfigurables y su aplicación a técnicas de aprendizaje automático para la monitorización de actividades*. Universidad de Granada, 2023. Accedido: 7 de octubre de 2023. [En línea]. Disponible en: https://digibug.ugr.es/handle/10481/84503

[14] B. Nath, «La arquitectura de Internet de las cosas (IoT)», Geekflare. Accedido: 9 de julio de 2023. [En línea]. Disponible en: https://geekflare.com/es/iot-architecture/

[15] M. A. Angulo Tello y F. Cándelo Velásquez, «Diseño de un esquema de integración de tecnologías “IOT” de los sistemas de seguridad electrónica.», 2017, Accedido: 24 de septiembre de 2023. [En línea]. Disponible en: https://repositorio.unipacifico.edu.co/handle/unipacifico/379

[16] A. Tavizon, T. Guajardo, y C. I. Laines Alamina, «IOT, el internet de las cosas y la innovación de sus aplicaciones», vol. 2, may 2016.

[17] C. González Antúnez, «Internet de las cosas en el ámbito del hogar inteligente», *Internet of things in the field of smart home*, 2020, Accedido: 9 de julio de 2023. [En línea]. Disponible en: https://idus.us.es/handle/11441/114790

[18] F. J. Valencia, «Ciberseguridad», Studenta. [En línea]. Disponible en: https://es.studenta.com/content/116861778/9-francisco-javier-valencia

[19] S. Molinetti, «Descubre las principales medidas de seguridad en una red LAN», Think Big. Accedido: 8 de julio de 2023. [En línea]. Disponible en: https://empresas.blogthinkbig.com/medidas-de-seguridad-en-una-red-lan/

[20] «Seguridad WiFi: WEP, WPA, WPA2, WPA3 y sus diferencias», NetSpot. Accedido: 8 de julio de 2023. [En línea]. Disponible en: https://www.netspotapp.com/es/blog/wifi-security/wifi-encryption-and-security.html

[21] «Los riesgos de seguridad y las buenas prácticas de la Internet de las cosas», www.kaspersky.es. Accedido: 8 de julio de 2023. [En línea]. Disponible en: https://www.kaspersky.es/resource-center/preemptive-safety/best-practices-for-iot-security

[22] W. Ashford, «Las pruebas son clave para la seguridad IoT, dice investigador | Computer Weekly», ComputerWeekly.es. Accedido: 8 de julio de 2023. [En línea]. Disponible en: https://www.computerweekly.com/es/cronica/Las-pruebas-son-clave-para-la-seguridad-IoT-dice-investigador

[23] «(PDF) IoT Network Security in Smart Homes». Accedido: 26 de septiembre de 2023. [En línea]. Disponible en: https://www.researchgate.net/publication/361232264_IoT_Network_Security_in_Smart_Homes?enrichId=rgreq-7e5b84e9245c5a7fcbcbd67e6de10b8f-XXX&enrichSource=Y292ZXJQYWdlOzM2MTIzMjI2NDtBUzoxMTQzMTI4MTExNDE5NDA5N0AxNjc0MzA2Mzk2NDM2&el=1_x_2&_esc=publicationCoverPdf

[24] M. Appiah, «IoT-based smart home: benefits, risks, solutions, and the AI developments for cyber defense», dic. 2022.

[25] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, y M. Bilal, «Smart home security: challenges, issues and solutions at different IoT layers», *The Journal of Supercomputing*, vol. 77, dic. 2021, doi: 10.1007/s11227-021-03825-1.

[26] N. Thilakarathne *et al.*, «Internet of Things (IoT) Security: Status, Challenges and Countermeasures», vol. 3, pp. 5444-5454, dic. 2022, doi: 10.35444/IJANA.2022.14305.

[27] P. K. Sadhu, V. P. Yanambaka, y A. Abdelgawad, «Internet of Things: Security and Solutions Survey», *Sensors*, vol. 22, n.º 19, Art. n.º 19, ene. 2022, doi: 10.3390/s22197433.

[28] D. Singh, P. Pal, M. Mishra, A. Lamba, y S. Swagatika, *Security Issues In Different Layers Of Iot And Their Possible Mitigation*. 2020. doi: 10.13140/RG.2.2.32754.04803.

[29] «IoT: Communication protocols and security threats», *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1-13, ene. 2023, doi: 10.1016/j.iotcps.2022.12.003.

[30] L. L. Vargas Santana, «Análisis de vulnerabilidades críticas del sistema operativo móvil Android mediante Pentesting», Thesis, PUCESE – Escuela de ingeniería en tecnologías de la información, 2023. Accedido: 17 de octubre de 2023. [En línea]. Disponible en: http://localhost/xmlui/handle/123456789/3419

[31] B. Al-Sada, A. Sadighian, y G. Oligeri, «MITRE ATT&CK: State of the Art and Way Forward». arXiv, 27 de agosto de 2023. doi: 10.48550/arXiv.2308.14016.

[32] «(PDF) Standardised Penetration Testing? Examining the Usefulness of Current Penetration Testing Methodologies». Accedido: 17 de octubre de 2023. [En línea]. Disponible en: https://www.researchgate.net/publication/335652869_Standardised_Penetration_Testing_Examining_the_Usefulness_of_Current_Penetration_Testing_Methodologies

[33] M. J. Kraemer y I. Flechais, «Researching Privacy in Smart Homes: A Roadmap of Future Directions and Research Methods», en *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK: Institution of Engineering and Technology, 2018, p. 38 (10 pp.)-38 (10 pp.). doi: 10.1049/cp.2018.0038.

[34] H. A. Abdul-Ghani, D. Konstantas, y M. Mahyoub, «A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model», *International Journal of Advanced Computer Science and Applications (ijacsa)*, vol. 9, n.º 3, Art. n.º 3, 30 2018, doi: 10.14569/IJACSA.2018.090349.

[35] M. Hossain, M. Fotouhi, y R. Hasan, *Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things*. 2015. doi: 10.1109/SERVICES.2015.12.

[36]«A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) | SpringerLink». Accedido: 1 de octubre de 2023. [En línea]. Disponible en: https://link.springer.com/article/10.1007/s11276-018-1712-5

[37] «OWASP Internet of Things | OWASP Foundation». Accedido: 4 de octubre de 2023. [En línea]. Disponible en: https://owasp.org/www-project-internet-of-things/

[38] S. Gómez Sempere, «Análisis de vulnerabilidades en la Internet de las Cosas», oct. 2023, Accedido: 15 de enero de 2024. [En línea]. Disponible en: http://rua.ua.es/dspace/handle/10045/137983

[39] N. Alsharabi, M. Alqunun, y B. Murshed, «Detecting Unusual Activities in Local Network Using Snort and Wireshark Tools», *Journal of Advances in Information Technology*, vol. 14, pp. 616-624, ene. 2023, doi: 10.12720/jait.14.4.616-624.

[40] P. Pandit, *A Study of Security Tools for Wireless Networks*. 2021. doi: 10.13140/RG.2.2.34511.20640.

[41] J.-P. A. Yaacoub, H. N. Noura, O. Salman, y A. Chehab, «Ethical hacking for IoT: Security issues, challenges, solutions and recommendations», *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280-308, ene. 2023, doi: 10.1016/j.iotcps.2023.04.002.

[42] BreachLock_Labs, «Top Vulnerability Scanners for Cybersecurity Professionals», BreachLock. Accedido: 6 de enero de 2024. [En línea]. Disponible en:

https://www.breachlock.com/resources/blog/top-vulnerability-scanners-for-cybersecurity-professionals/

[43] R. Sahay, D. A. S. Estay, W. Meng, C. D. Jensen, y M. B. Barfod, «A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS», *Computers & Security*, vol. 128, p. 103179, may 2023, doi: 10.1016/j.cose.2023.103179.

[44] R. Vyas, «How Do MAC Spoofing Attacks Work?», SecureW2. Accedido: 6 de enero de 2024. [En línea]. Disponible en: https://www.securew2.com/blog/how-do-mac-spoofing-attacks-work

[45] T. Ariyadi y M. R. Pohan, «Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators», *Jurnal Penelitian Pendidikan IPA*, vol. 9, n.º 12, Art. n.º 12, dic. 2023, doi: 10.29303/jppipa.v9i12.5551.

[46] P. Krishnan, A. V. Prabu, S. Loganathan, S. Routray, U. Ghosh, y M. AL-Numay, «Analyzing and Managing Various Energy-Related Environmental Factors for Providing Personalized IoT Services for Smart Buildings in Smart Environment», *Sustainability*, vol. 15, n.º 8, Art. n.º 8, ene. 2023, doi: 10.3390/su15086548.

[47] W. Schroeder, «Hacking With Your Nemesis», Medium. Accedido: 6 de enero de 2024. [En línea]. Disponible en: https://posts.specterops.io/hacking-with-your-nemesis-7861f75fcab4

[48] J. James, «Engineering the Human Mind: Social Engineering Attack Using Kali Linux», *SN Computer Science*, vol. 4, pp. 1-10, nov. 2023, doi: 10.1007/s42979-023-02321-y.

[49] H. Gebrye, Y. Wang, y F. Li, «Traffic data extraction and labeling for machine learning based attack detection in IoT networks», *International Journal of Machine Learning and Cybernetics*, vol. 14, pp. 1-16, ene. 2023, doi: 10.1007/s13042-022-01765-7.

[50] J. Cathcart y T. Khan Mohd, *Password Hacking Analysis of Kali Linux Applications*. 2023.

[51] M. Goel, S. Singh, A. Garg, y N. R. Roy, «Comparative Study of DDoS Attacks & Tools and Their Analysis», en *2023 International Conference on IoT, Communication and Automation Technology (ICICAT)*, jun. 2023, pp. 1-8. doi: 10.1109/ICICAT57735.2023.10263744.

[52] A. Kumar, G. Ghinea, y S. Merugu, *Proceedings of the 2nd International Conference on Cognitive and Intelligent Computing: ICCIC 2022, 27–28 December, Hyderabad, India; Volume 1*. Springer Nature, 2023.

[53] D. Collins, «Pen Testing Framework for IoT Devices», masters, Dublin, National College of Ireland, 2021. Accedido: 6 de enero de 2024. [En línea]. Disponible en: https://norma.ncirl.ie/5094/

[54] T. Admassu, «Comparative Study on Methods Used in Prevention and Detection Against Adress Resolution Protocol Spoofing Attack», ene. 2020, Accedido: 6 de enero de 2024. [En línea]. Disponible en: https://www.academia.edu/70242615/Comparative_Study_on_Methods_Used_in_Prevention_and_Detection_Against_Adress_Resolution_Protocol_Spoofing_Attack

[55] T. Joos, «Security with CrowdSec » ADMIN Magazine», ADMIN Magazine. Accedido: 7 de enero de 2024. [En línea]. Disponible en: http://www.admin-magazine.com/Archive/2023/73/CrowdSec-crowd-security-service

[56] C. López y E. Cankaya, «A Comprehensive Analysis of Security Tools for Network Forensics», *Journal of Medical - Clinical Research & Reviews*, vol. 1, pp. 1-9, dic. 2017, doi: 10.33425/2639-944X.1021.

ANEXOS

Anexo A. Datasheet de los dispositivitos IoT

De La Figura A1 a la Figura A5 se muestra la información técnica de los dispositivos IoT de la marca Tuya.

INTERRUPTOR WIFI SMART 3 BOTONES

Referencia MER04929

$20,16 ~~$22.40~~ -10%

Impuestos incluidos

Stock: 20 Articulos

Tiempo restante | 16 d. 15 : 28 : 20

¿Estás buscando una manera fácil y conveniente de controlar tus luces desde cualquier lugar? Entonces, un interruptor WiFi inteligente para un botón puede ser la solución perfecta para ti. Este dispositivo te permite controlar la iluminación y de manera rápida y sencilla, todo desde la palma de tu mano.

1 Añadir al carrito

Descripción | Detalles del producto | Comentarios

Material	CRISTAL TEMPLADO
Temperatura funcionamiento	-10°c to +60°c
Botón	3
Modo de trabajo	TACTIL / CELULAR MOVIL
Modelo	PST-WF-U3
Color	BLANCO
Peso	0.2KG
Protocolo Wifi	IEEE 802.11 B/N/G 2.4G Hz
Voltaje	AC 110V-240V
Plataforma de soporte	Tuyasmart/Smartlife
Control de Voz	Amazon Alexa/Google Assistance/Ifttt

Figura A1. Especificaciones técnicas del Interruptor de luz inteligente

Figura A2. Especificaciones técnicas de la bombilla LED inteligente de colores

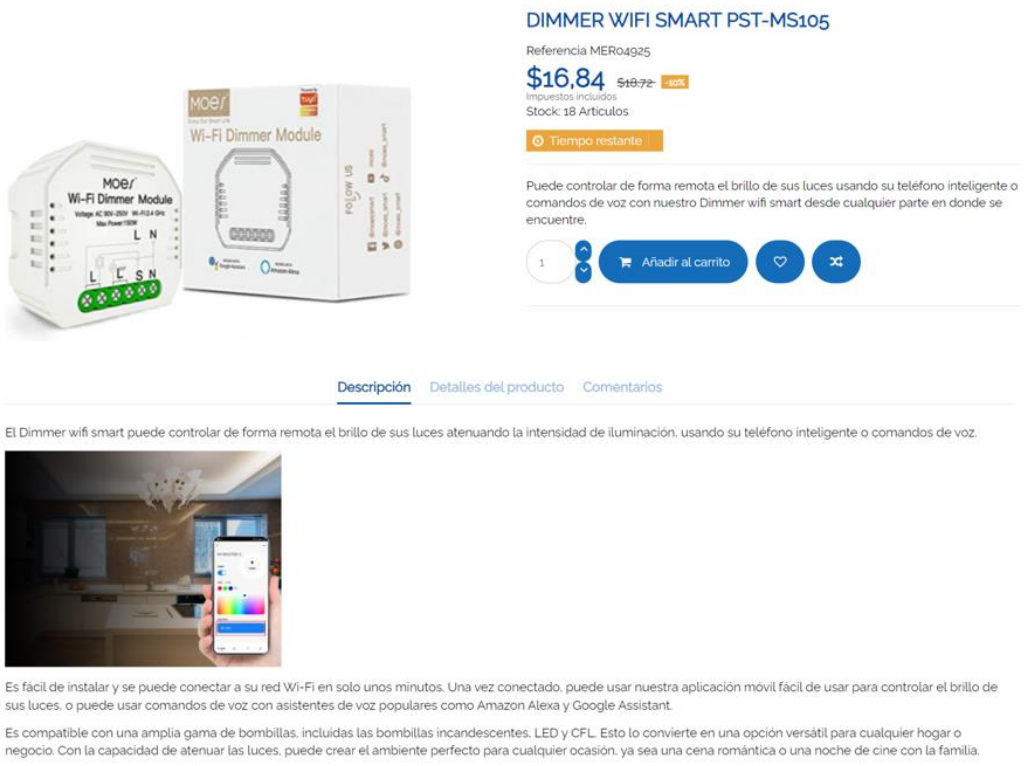
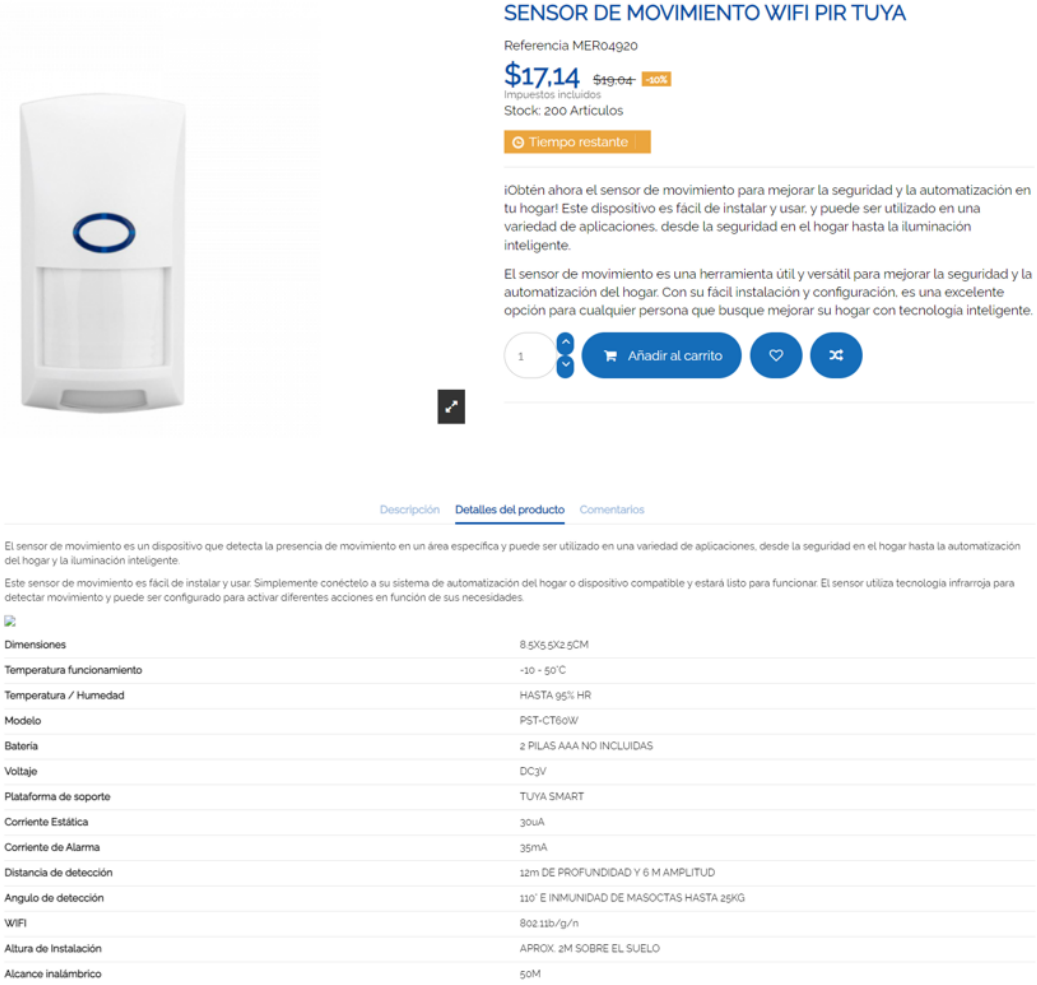


Figura A3. Detalles y especificaciones del módulo WiFi regulador para luces



SENSOR DE MOVIMIENTO WIFI PIR TUYA

Referencia MER04920

$17,14 ~~$19.04~~ -10%

Impuestos incluidos

Stock: 200 Artículos

Tiempo restante

¡Obtén ahora el sensor de movimiento para mejorar la seguridad y la automatización en tu hogar! Este dispositivo es fácil de instalar y usar, y puede ser utilizado en una variedad de aplicaciones, desde la seguridad en el hogar hasta la iluminación inteligente.

El sensor de movimiento es una herramienta útil y versátil para mejorar la seguridad y la automatización del hogar. Con su fácil instalación y configuración, es una excelente opción para cualquier persona que busque mejorar su hogar con tecnología inteligente.

1 Añadir al carrito

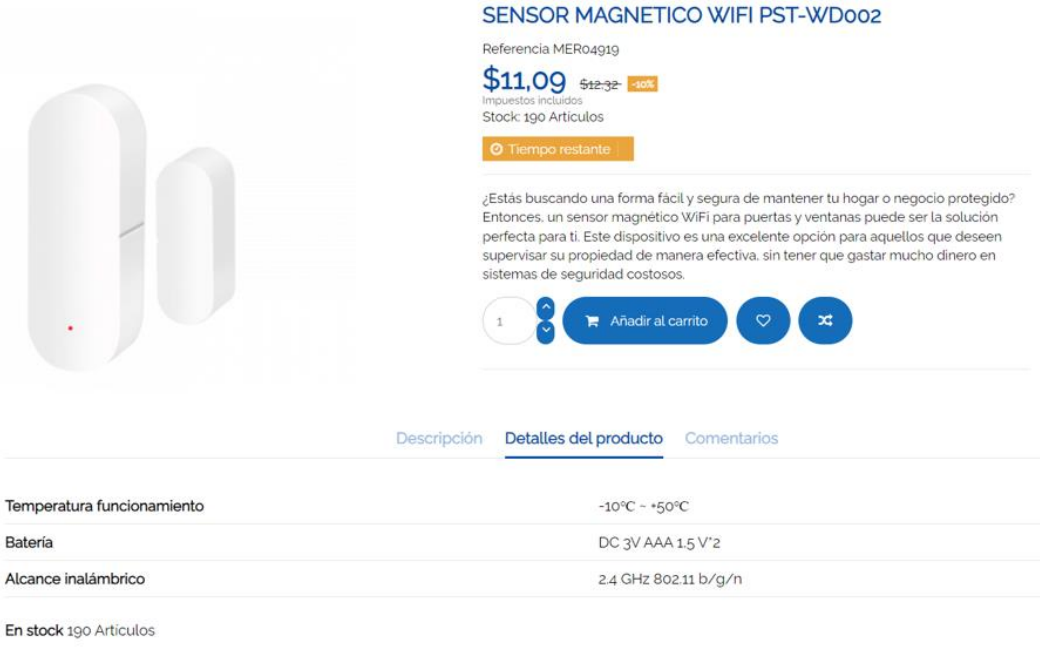
Descripción | Detalles del producto | Comentarios

El sensor de movimiento es un dispositivo que detecta la presencia de movimiento en un área específica y puede ser utilizado en una variedad de aplicaciones, desde la seguridad en el hogar hasta la automatización del hogar y la iluminación inteligente.

Este sensor de movimiento es fácil de instalar y usar. Simplemente conéctelo a su sistema de automatización del hogar o dispositivo compatible y estará listo para funcionar. El sensor utiliza tecnología infrarroja para detectar movimiento y puede ser configurado para activar diferentes acciones en función de sus necesidades.

Dimensiones	8.5X5.5X2.5CM
Temperatura funcionamiento	-10 ~ 50°C
Temperatura / Humedad	HASTA 95% HR
Modelo	PST-CT60W
Batería	2 PILAS AAA NO INCLUIDAS
Voltaje	DC3V
Plataforma de soporte	TUYA SMART
Corriente Estática	30uA
Corriente de Alarma	35mA
Distancia de detección	12m DE PROFUNDIDAD Y 6 M AMPLITUD
Angulo de detección	110° E INMUNIDAD DE MASOCTAS HASTA 25KG
WIFI	802.11b/g/n
Altura de Instalación	APROX. 2M SOBRE EL SUELO
Alcance inalámbrico	50M

Figura A4. Especificaciones técnicas del detector de movimiento con alarma PIR



SENSOR MAGNETICO WIFI PST-WD002

Referencia MER04919

$11,09 ~~$12.32~~ -10%

Impuestos incluidos

Stock: 190 Artículos

Tiempo restante

¿Estás buscando una forma fácil y segura de mantener tu hogar o negocio protegido? Entonces, un sensor magnético WiFi para puertas y ventanas puede ser la solución perfecta para ti. Este dispositivo es una excelente opción para aquellos que deseen supervisar su propiedad de manera efectiva, sin tener que gastar mucho dinero en sistemas de seguridad costosos.

1 Añadir al carrito

Descripción | Detalles del producto | Comentarios

Temperatura funcionamiento	-10°C ~ +50°C
Batería	DC 3V AAA 1.5 V*2
Alcance inalámbrico	2.4 GHz 802.11 b/g/n

En stock 190 Artículos

Figura A5. Especificaciones técnicas de sensores de contacto para puertas/ventanas

De La Figura A6 a la Figura A8 se muestra la información técnica de los dispositivos IoT de la marca Nexxt Solutions.

Bombilla LED inteligente Wi-Fi 110V - A19 - NHB-W110

V1 V3

Color blanco regulable, empaque individual

MPN: NHB-W110

- **Tipo de bombilla:** A19
- **Watts:** 9W (equivalente a 60 watts)
- **Color:** No
- **Material:** Plástico
- **Garantía:** 2 years

Especificaciones técnicas

MPN	NHB-W110 V3
General	
Color	Luz blanca (fría a cálida)
Brillo	800 lúmenes
Watts	9W
Luz de color	2700-6500k
Intensidad regulable	Sí
Factor de forma	Bombilla A19, casquillo E26/E27
Voltaje	110VCA, 60Hz
Frecuencia inalámbrica	IEEE 802.11N, 2.4GHz (no compatible con redes Wi-Fi de 5GHz)
Requisitos de instalación	No se necesita concentrador
Vida útil	Hasta 25.000 horas
Información adicional	
Requisitos del sistema	• Aparato inalámbrico con sistema operativo iOS 10 o superior, o Android 5.0 o superior • Aplicación Nexxt Home • Red Wi-Fi existente
Atributos especiales	Capacidad para crear horarios, escenas, numerosos horarios, grupos
Asistentes virtuales compatibles	Amazon Alexa, Google Assistant y Siri
Aplicación	Interiores
Garantía	2 años
Certificado	FCC
Apariencia física	
Dimensiones	10,5 x 5,9 cm
Peso	30 g
Armazón	Plástico
Color	Blanco
Contenido del empaque	Bombilla inteligente (1) Guía rápida de instalación (1)
Condiciones ambientales	
Temperatura de funcionamiento	-10 °C - 40 °C
Temperatura de almacenaje	-40 °C - 70 °C
Humedad relativa	< 95% no condensada

Figura A6. Especificaciones técnicas de las bombillas LED inteligentes color blanco

Enchufe inteligente Wi-Fi 110V

Enchufe inteligente Wi-Fi

MPN: AHIWPSO4U1

- No necesita concentrador
- Emparejamiento fácil
- Aplicación compatible con iOS y Android™
- Configuración de horarios
- Programación de múltiples temporizadores
- Acceso compartido

Especificaciones técnicas

MPN	AHIWPSO4U1
Entrada	
Tensión	100 -240VCA
Frecuencia	50/60Hz
Corriente máxima de carga	10A máx
Frecuencia inalámbrica	IEEE 801.11N, 2.4GHz (no es compatible con redes Wi-Fi de 5GHz)
Tipo de enchufe	NEMA 5-15P
Salida	
Tensión	120-240VCA
Frecuencia	50/60Hz
Potencia máxima	1250W
Tomacorriente	NEMA 5-15R
Características físicas	
Dimensiones	6,5x4,5x3,2cm
Cubierta	Plástico retardador de llama
Color	Blanco
Peso	65g
Condiciones ambientales	
Temperatura de funcionamiento	0 - 40ºC
Temperatura de almacenamiento	-10 - 60ºC
Humedad relativa	Humedad de funcionamiento: 10%-90% no condensada Humedad de almacenamiento: 5%-90% no condensada
Aplicación	Uso en interior
Información adicional	
Requisitos del sistema	- Dispositivo móvil con plataforma iOS8 o superior, Android™ 4.1 o superior - Aplicación Nexxt Home - Red Wi-Fi existente
Garantía	Dos años
Certificado	FCC (Comisión Federal de Comunicaciones)

Figura A7. Especificaciones técnicas del enchufe inteligente

Cámara de 2K para interior

Cámara inteligente Wi-Fi para interior

MPN: NHC-I710

- Resolución total de 2K garantiza una calidad de imagen y precisión cromática impresionantes
- La captura imágenes a 20fps permite grabar en tiempo real objetos en movimiento sin degradar su nitidez
- Óptima visualización de cada escena gracias a la definición ultraalta y amplio ángulo de visión de 100°
- Algoritmo inteligente para la detección del cuerpo humano minimiza las alertas falsas
- Detección de movimiento con un alcance efectivo de hasta 10m
- La visión nocturna, gracias a los seis LEDs infrarrojos de gran alcance, capta imágenes con claridad, incluso en condiciones mínimas de iluminación
- Almacenamiento local mediante una tarjeta microSD™ de hasta 128GB*
- Opciones de montaje flexibles: es posible colocar la cámara sobre un estante o montarla en la pared o en el techo

Especificaciones técnicas

MPN	NHC-I710
Aspectos generales	
Resolución	2K QHD (2304x1296p) 3MP
Sensor de imagen	CMOS a color de 1/2,8 de pulgada
Tipo de lente	Fijo de 4mm
Ángulo de visión	100 grados
Compresión de video	H.265
Compresión de audio	G.711
Audio bidireccional	Micrófono y parlante integrados
Botón de reposición	Incluido
Frecuencia de imagen	20fps
Modo IR	Conjunto de luces LED (6) con filtro de corte infrarrojo para conmutación automática
Captura de imagen estática	Incluida
Alcance del detector de movimiento	Hasta 10m
Visión nocturna	Hasta 10m
Ranura para memoria local	Tarjeta microSD™ de hasta 128GB*
Frecuencia inalámbrica	IEEE 802.11N, 2.4GHz (no es compatible con redes Wi-Fi de 5GHz)
Requisitos de configuración	No requiere concentrador
Características de vídeo	Detección de movimiento, filtro para reconocimiento de la figura humana
Alimentación	
Tensión de entrada	5V 1A
Consumo total	5W (máx.)
Aspectos físicos	
Dimensiones	8,5x3,3x4,9cm
Peso	12g
Longitud del cable	Cable Tipo C de 2m
Cubierta	Plástico
Color	Blanco
Aspectos ambientales	
Temperatura de funcionamiento	-10°C - 50°C
Temperatura de almacenamiento	-20°C - 60°C
Humedad relativa	< 95% no condensada
Información adicional	
Requisitos del sistema	- Dispositivo móvil con plataforma iOS8 o superior, Android™ 4.1 o superior - Aplicación Nexxt Home - Red Wi-Fi existente
Funciones especiales	Notificaciones.
Aplicación	Para uso interior
Contenido del empaque	•Cámara inteligente Wi-Fi de 2K (1) • Cable USB Tipo-C (1) • Adaptador de corriente (1) • Herrajes de montaje (1 set) • Almohadilla autoadhesiva 3M (1) • Plantilla de perforación (1) • Guía de configuración rápida (1)
Certificación	FCC (Comisión Federal de Comunicaciones)
Garantía	Dos años

Figura A8. Especificaciones técnicas de la cámara inteligente para interiores

La Figura A9 muestra la información técnia del parlante Echo Dot Alexa 5ta gen.

Tamaño	3.9" x 3.9" x 3.5" (100mm x 100mm x 89 mm)
Peso	10.7 oz (304 g) El tamaño y peso reales podrían variar en función del proceso de fabricación.
Audio	Parlante con proyección frontal de 1.73" (44 mm), alta definición sin pérdidas.
Conectividad wifi	El wifi de doble banda es compatible con redes 802.11a/b/g/n/ac (2.4 y 5 GHz). No admite la conexión con redes wifi ad hoc (peer-to-peer, también conocida como red de pares).
Amazon Sidewalk	Una red compartida que ayuda a que los dispositivos compatibles funcionen mejor en casa y más allá de la puerta. Si se pierde la conexión wifi, Sidewalk permite que determinados dispositivos sigan conectados. Además, Sidewalk ayuda a que dispositivos como aspersores de agua y localizadores de mascotas funcionen en distancias más largas. Sidewalk utiliza una pequeña parte de tu ancho de banda de Internet para brindarte estas ventajas tanto a ti como a tus vecinos a través de Sidewalk Bridges (dispositivos Echo y Ring participantes), y está activada en tu dispositivo a menos que hayas desactivado la configuración previamente. Puedes desactivar Sidewalk en cualquier momento. Obtener más información sobre Sidewalk.
Compatibilidad con Dispotivos de Smart Home	WiFi, Bluetooth Low Energy Mesh, y Matter
Conectividad Bluetooth	Compatibilidad con perfil de distribución de audio avanzado (A2DP, por sus siglas en inglés) para el streaming de audio desde tu dispositivo móvil al Echo Dot, o desde el Echo Dot a tu bocina Bluetooth. Perfil de control remoto para audio y video (AVRCP, por sus siglas en inglés) para controlar por voz los dispositivos móviles conectados. El control por voz no es compatible con dispositivos Mac OS X. Las bocinas Bluetooth que requieren códigos PIN no se admiten.
Integración de eero	Su red wifi debe usar un enrutador eero compatible y su dispositivo Echo debe permanecer dentro del alcance de un dispositivo eero compatible. Deberá vincular sus cuentas de eero y Amazon y administrar eero desde la aplicación móvil de eero para usar esta función. Los dispositivos Echo integrados compatibles de eero admiten hasta 1,000 pies cuadrados de cobertura adicional, velocidades de hasta 100 Mbps y 10 o menos dispositivos conectados en la banda de 5 GHz. El rendimiento real puede variar y es posible que algunas funcionalidades de eero, Echo o Alexa no sean compatibles con eero integrado. Obtén más información sobre el rendimiento, la disponibilidad y la compatibilidad de eero integrado. El uso de eero, así como el de productos y servicios relacionados con eero, incluyendo eero integrado, requieren crear una cuenta de eero y aceptar los términos de servicio de eero. Revisa el aviso de privacidad de eero.
Requisitos del sistema	El Echo Dot viene listo para conectarse a tu red wifi. La app de Alexa es compatible con dispositivos Fire OS, Android y iOS; además, puedes acceder a ella en un navegador web. Sistemas operativos compatibles. Es posible que algunos servicios y Skills requieran una suscripción u otras tarifas.

Figura A9. Especificaciones técnicas del parlante de voz Echo Dot Alexa 5ta gen.

Anexo B. Configuración del adaptador USB 802.11

La información técnica del A600 Adaptador USB inalámbrico utilizado en la etapa de explotación, se muestra en la Figura B1.

Archer T2U Plus

AC600 Adaptador USB Inalámbrico de Alta Ganancia Doble Banda

- **Wi-Fi Alta velocidad**: 256QAM incrementa el ancho de banda de 2,4 GHz de 150 Mbps a 200 Mbps, 200 Mbps en la banda de 2,4 GHz y 433 Mbps en la banda de 5 GHz, Wi-Fi AC, te asegura una conexión rápida
- **Doble Banda Inalámbrica**: Bandas de 2.4 GHz y 5 GHz proporcionan conectividad flexible, dando el acceso al dispositivos a la oble banda Wi-Fi del router para mayor velocidad y rango extendido
- **Antena Alta Ganancia**: Antena de 5dBi de alta ganancia mejora considerablemente la potencia de recepción y transmisión de señal del adaptador USB
- **Soporta los Últimos Sistemas Operativos**: Compatible con Windows 10/8.1/8/7/XP y Mac OS X

CARACTERÍSTICAS DE HARDWARE

Interface	USB 2.0
LED	Status
Dimensiones (W X D X H)	57.8 × 18 × 173.4 mm
Antena	5dBi

CARACTERÍSTICAS INALÁMBRICAS

Estándares Inalámbricos	IEEE 802.11b/g/n 2.4 GHz, IEEE 802.11a/n/ac 5 GHz
Velocidades Inalámbricas	600 Mbps (200 Mbps en 2.4 GHz, 433 Mbps en 5 GHz)
Frecuencia	2.4 GHz, 5 GHz
Modos Inalámbricos	Ad-Hoc / Modo Infraestructura
Seguridad Inalámbrica	WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
Tecnología de Modulación	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM, 256-QAM

Figura B1. Especificaciones técnicas del AC600 Adaptador USB inalámbrico

La Figura B2 muestra información sobre las interfaces inalámbricas en el entorno de pruebas mediante el comando `lusb`.

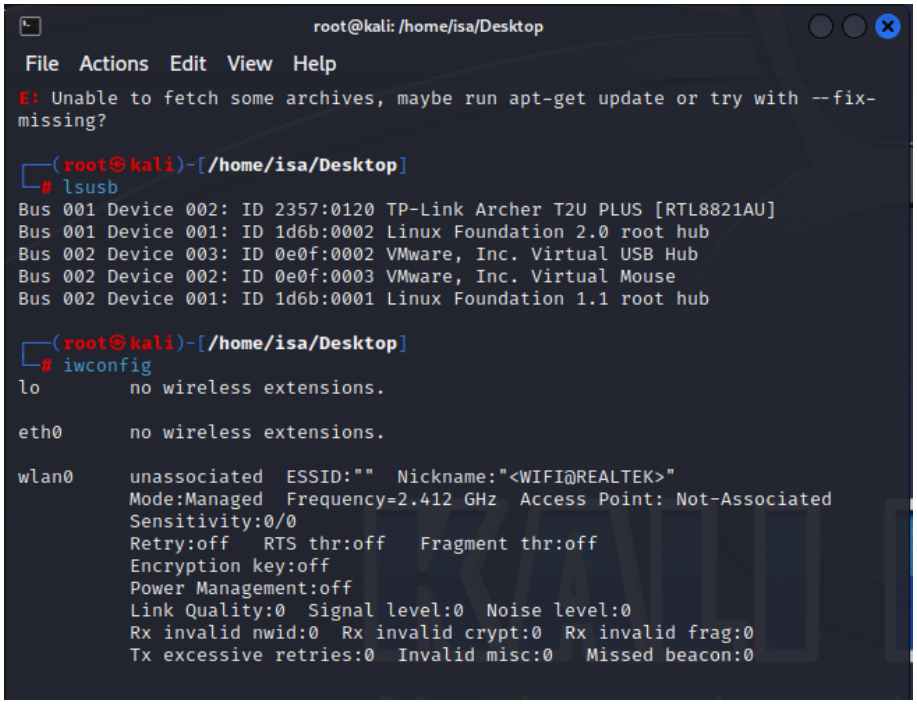


Figura B2. Interfaces inalámbricas

La activación del modo monitor en el adaptador USB 802.11 mediante el comando `airmon-ng start wlan0`, como se muestra en la Figura B3.

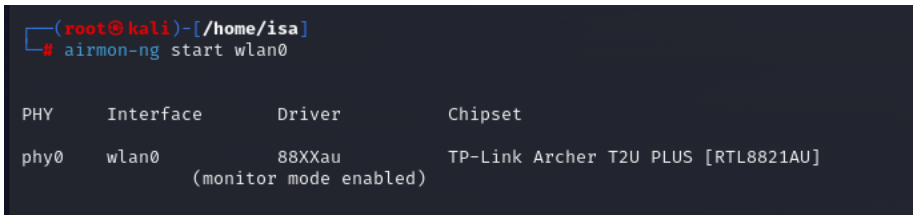


Figura B3. Activación del modo monitor en el adaptador USB 802.11

La Figura C1 presenta la descarga de la herramienta Advanced IP Scanner en el sistema Windows se realiza mediante su página oficial: Advanced IP Scanner

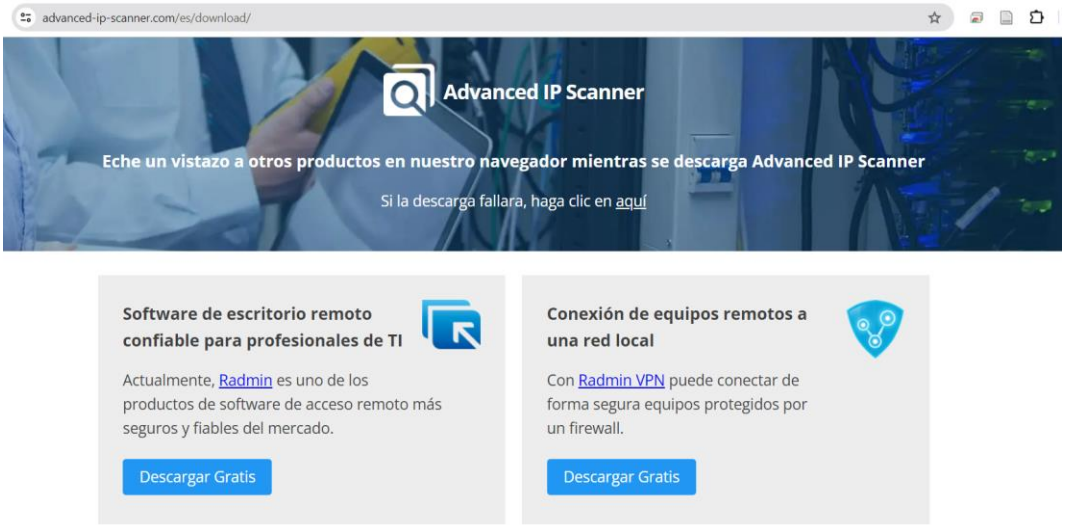


Figura C1. Descarga del software Advanced IP Scanner de la página oficial

Una vez descargado el software, se realiza su instalación en la máquina de Windows, como se muestra en la Figura C2.

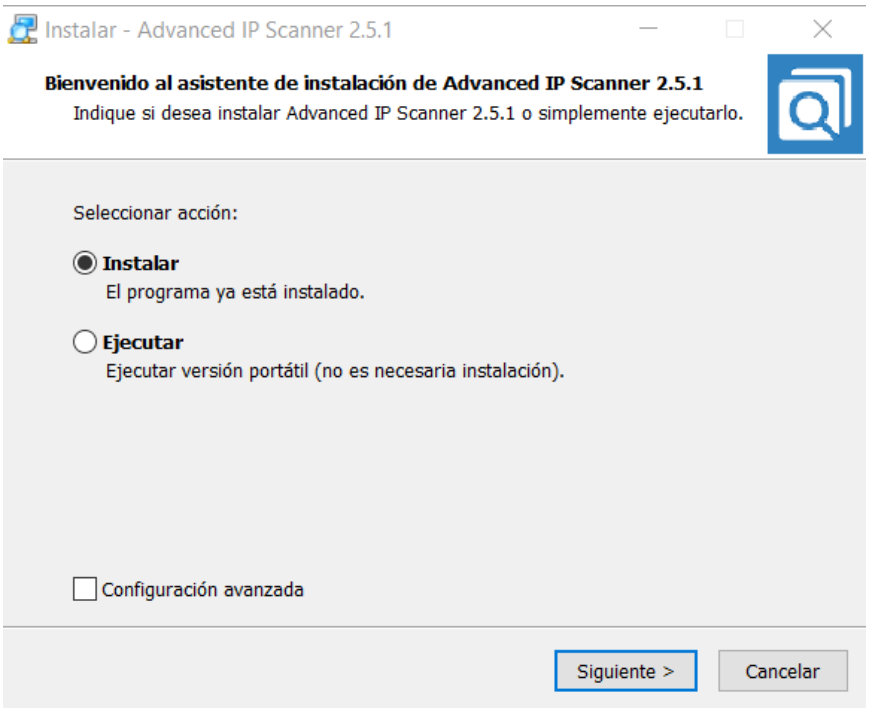


Figura C2. Instalación del software Advanced IP Scanner en la máquina Windows

En pocos minutos, la instalación de la herramienta se completó y se encuentra lista para realizar escaneos de detección en la red, como muestra la Figura C3.

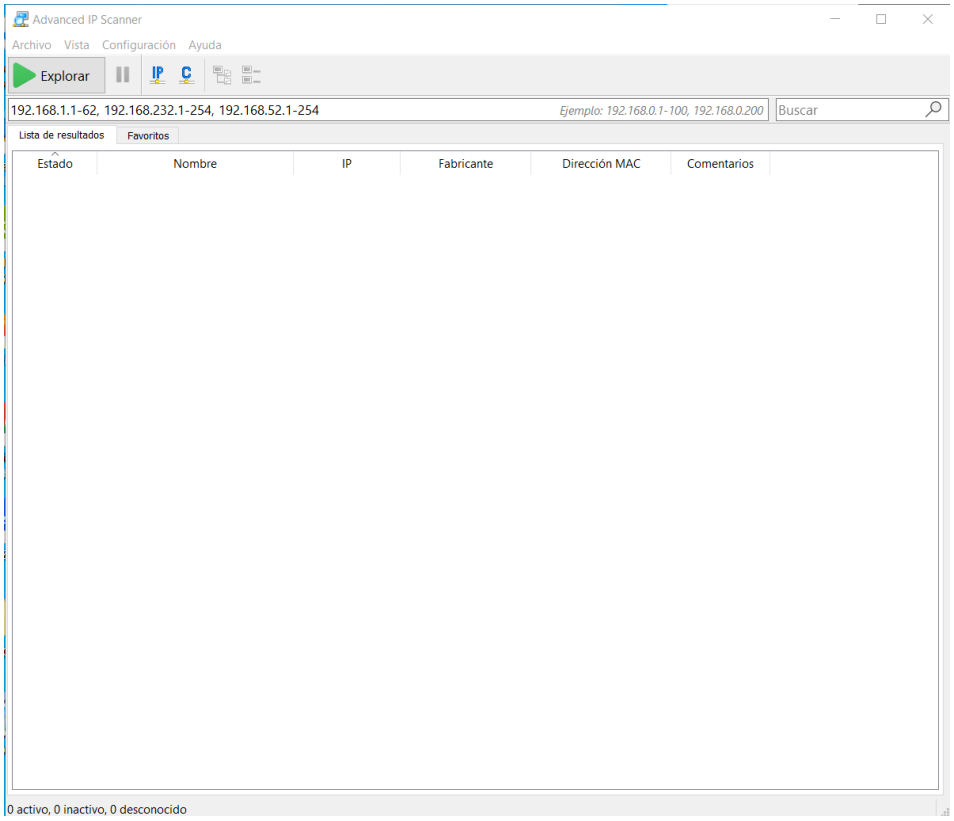


Figura C3. Interfaz de inicio en el software de Advanced IP Scanner

La Figura C4 muestra la inicialización de la herramienta Kismet en Kali Linux mediante el comando `kismet -c wlan0`, debido a que esta es la interfaz en la cual se encuentra el adaptador inalámbrico.

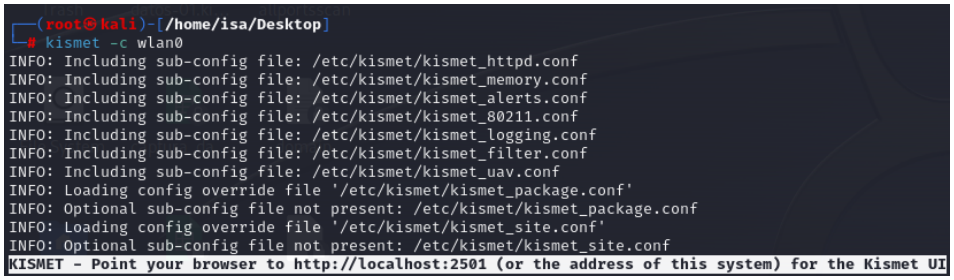


Figura C4. Inicialización de la Herramienta Kismet en Kali Linux

La Figura D1 descarga de la herramienta Angry IP Scanner se la realizó a través de su página oficial: AngryIp.

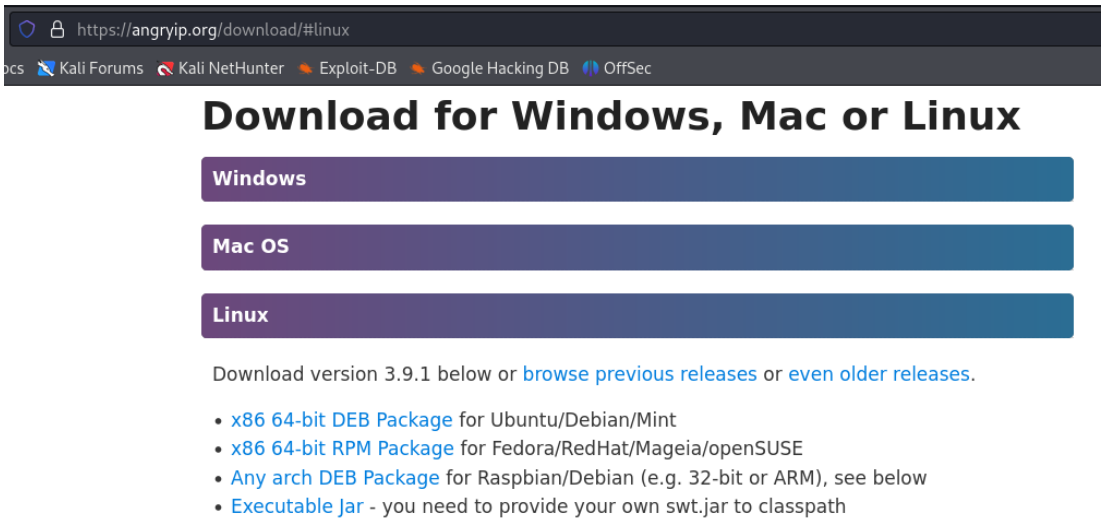


Figura D1. Descarga de la herramienta Angry IP Scanner a través de u página oficial

Una vez descargada en el sistema operativo correspondiente, en este caso Linux, se realiza la instalación en la máquina mediante el comando `sudo dpkg -i pscan_3.9. 1 _ amd 64.deb`, como se muestra en la Figura D2.

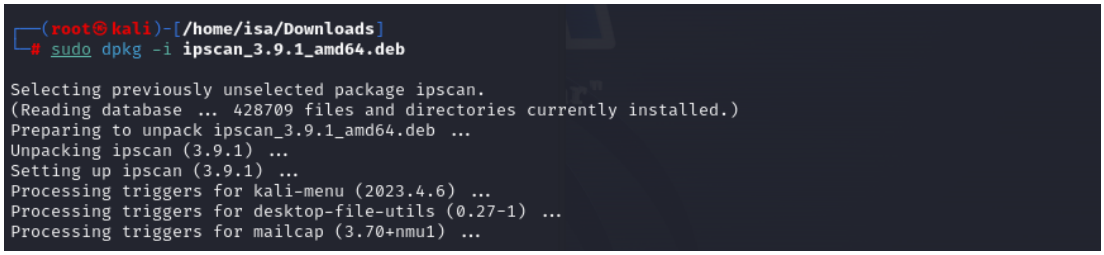


Figura D2. Instalación de la herramienta Angry IP Scanner en la máquina Kali Linux

Después de pocos minutos para la instalación, la herramienta pueda ser ejecutada en la máquina virtual de Kali Linux, como se muestra en la Figura D3.

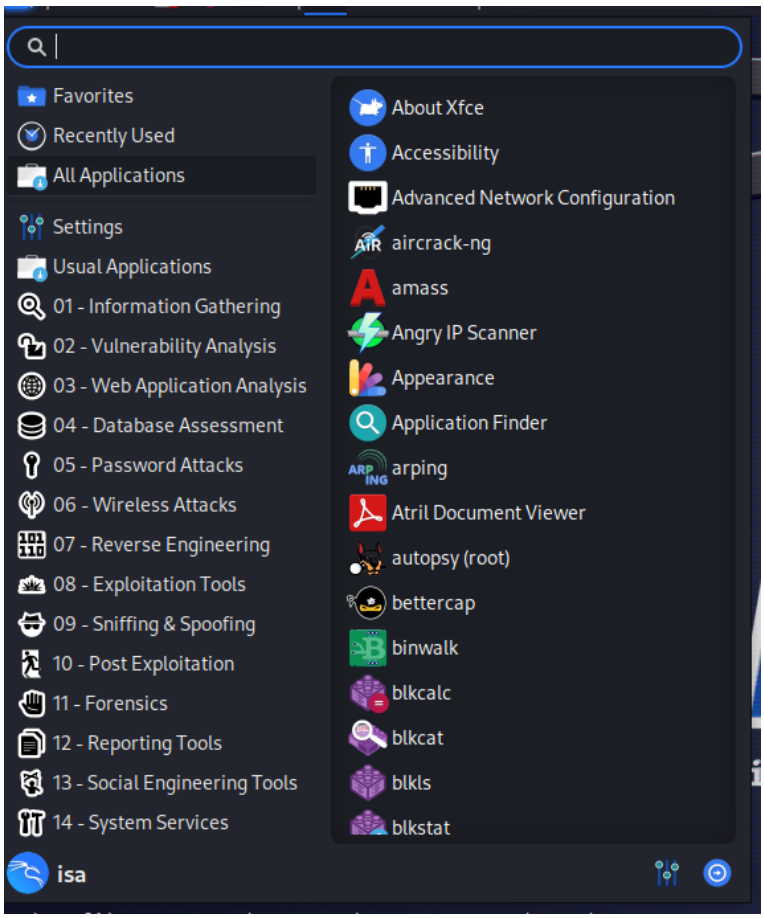


Figura D3. Acceso a la herramienta Angry IP Scanner en la máquina Kali Linux

La descarga de la herramienta Nessus a través de su página oficial Tenable, como se muestra en la Figura D4.

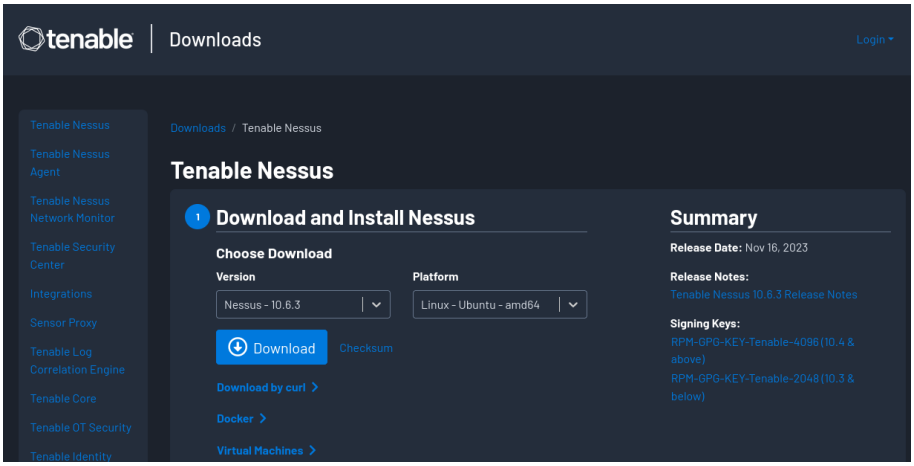


Figura D4. Descarga de la herramienta Nessus a través de su página oficial

El proceso de instalación de la herramienta Nessus a través de la línea de comandos de Kali Linux, como se muestra la Figura D5.

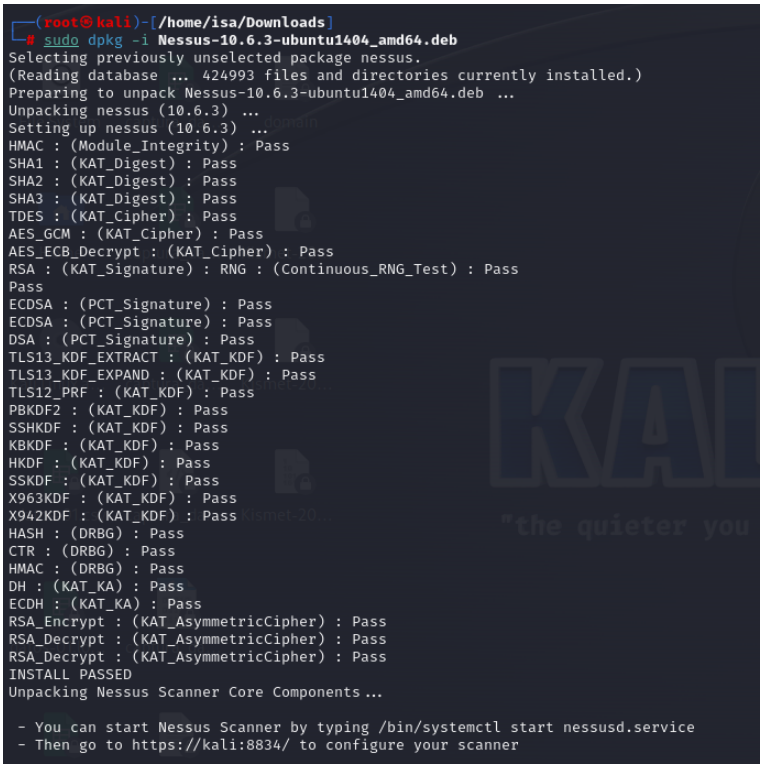


Figura D5. Instalación de la herramienta Nessus a través de la línea de comandos de Kali Linux

La Figura D6 muestra la inicialización de la herramienta Nessus en la máquina virtual instalada.

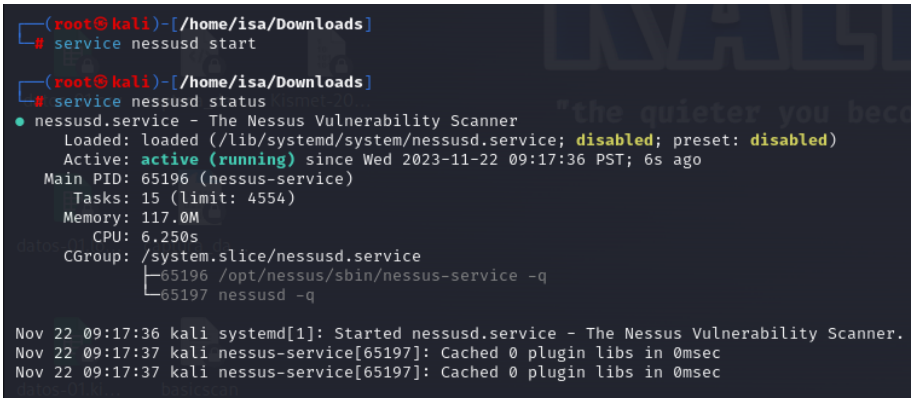


Figura D6. Inicialización de la herramienta Nessus

Se ingresa a la interfaz gráfica de la herramienta Nessus mediante el puerto 8834, como se muestra en la Figura D7.

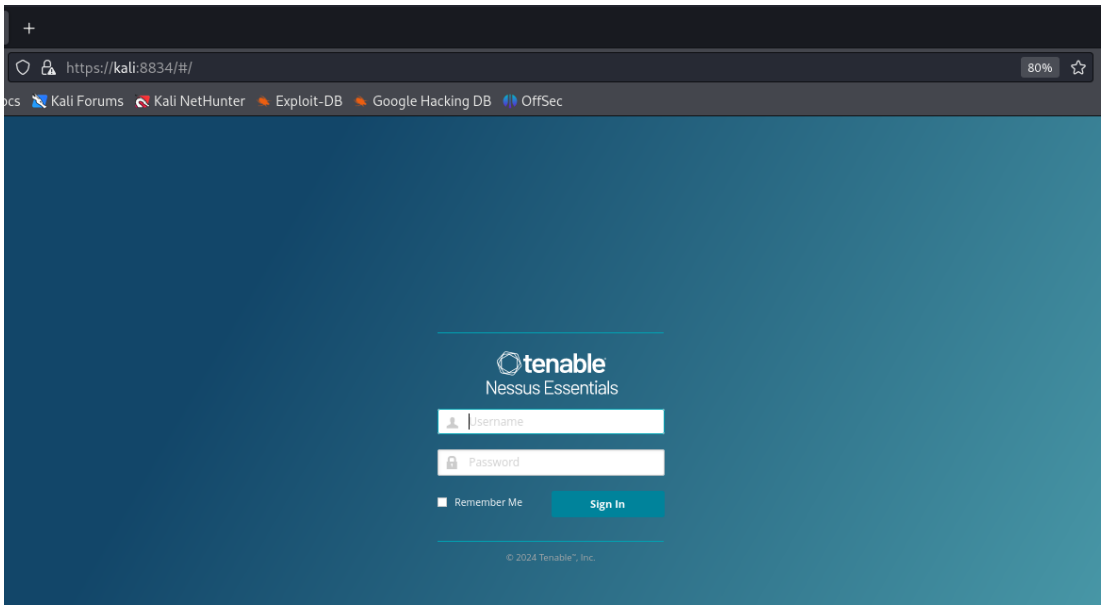


Figura D7. Ingreso a la interfaz gráfica de la herramienta Nessus

Una vez dentro de la herramienta Nessus, se pueden realizar diferentes tipos de escaneos según los requerimientos del usuario, en la página principal de la herramienta, como se muestra en la Figura D8.

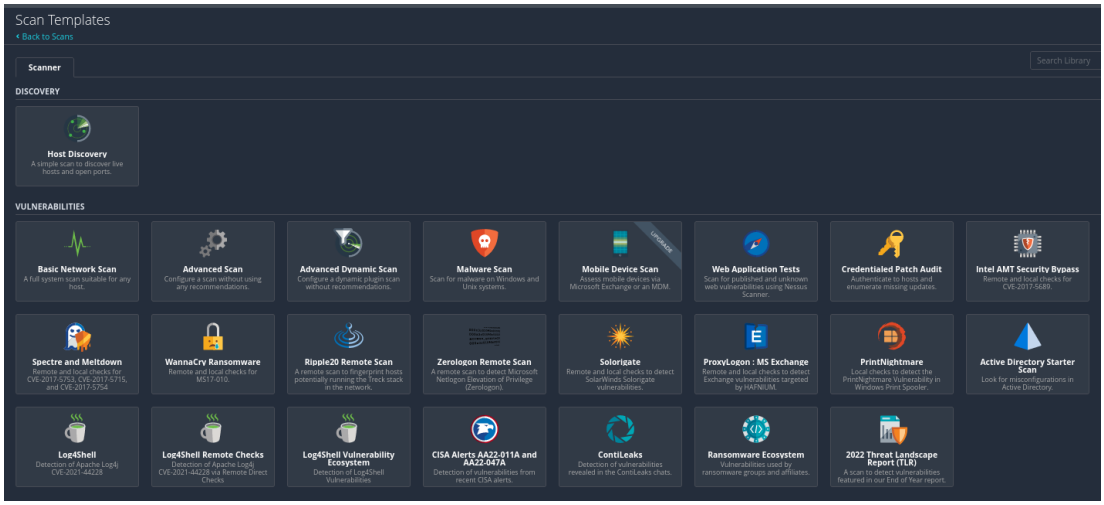


Figura D8. Opciones de escaneo en la herramienta Nessus

Para realizar un nuevo escaneo de la red, se accede a la opción de Advanced Scan y se delimita el rango para el escaneo de dispositivos, como se muestra en la Figura D9.

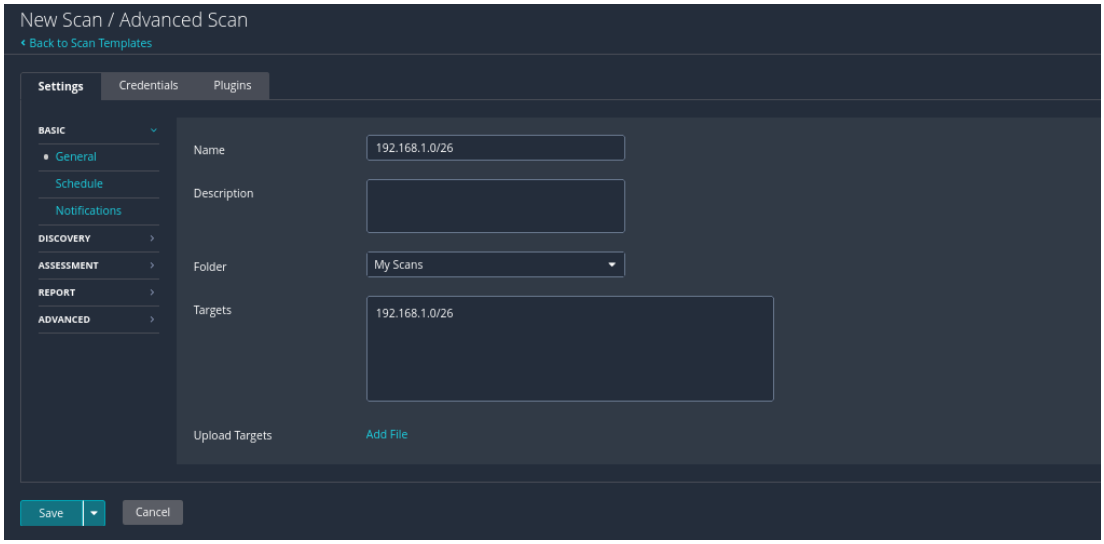
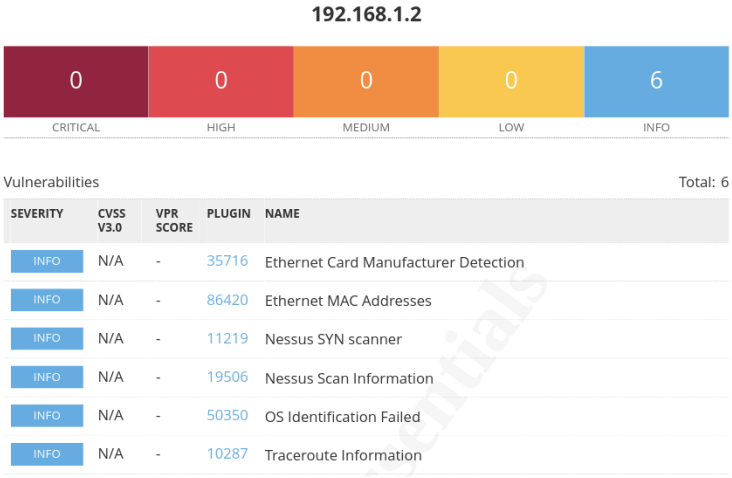


Figura D9. Selección de los dispositivos para el escaneo de vulnerabilidades

La Figura D10 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.2.



192.168.1.2

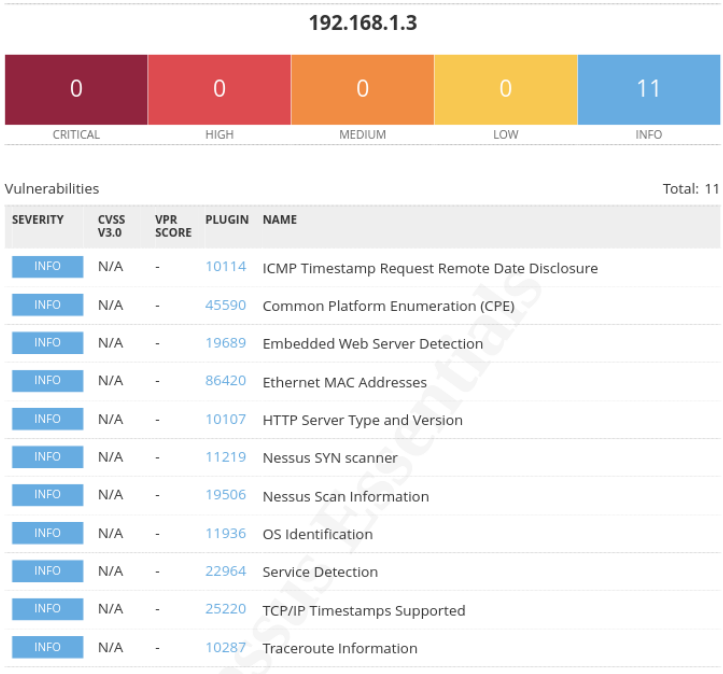
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	6

Vulnerabilities — Total: 6

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	50350	OS Identification Failed
INFO	N/A	-	10287	Traceroute Information

Figura D10. Escaneo de vulnerabilidades en el dispositivo 192.168.1.2

La Figura D11 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.3.



192.168.1.3

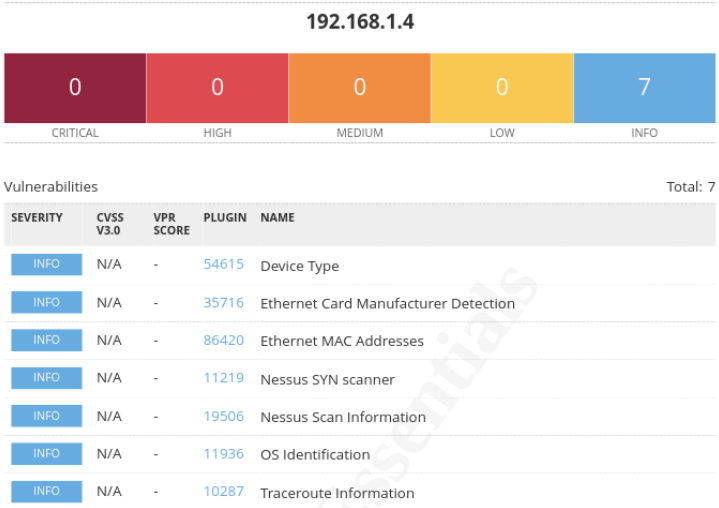
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	11

Vulnerabilities — Total: 11

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	19689	Embedded Web Server Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

Figura D11. Escaneo de vulnerabilidades en el dispositivo 192.168.1.3

La Figura D12 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.4.



192.168.1.4

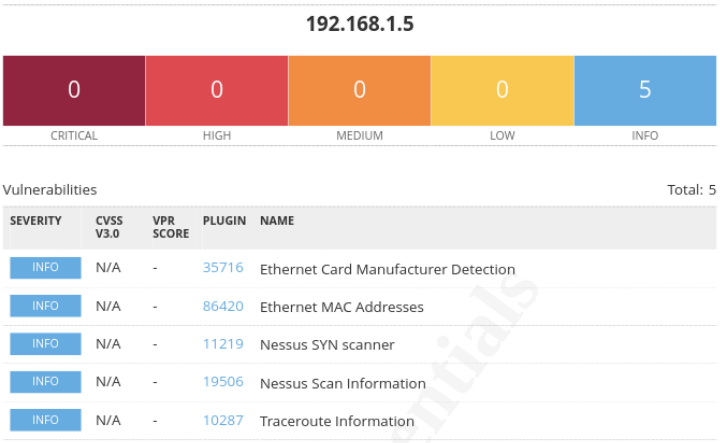
0	0	0	0	7
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10287	Traceroute Information

Figura D12. Escaneo de vulnerabilidades en el dispositivo 192.168.1.4

La Figura D13 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.5.



192.168.1.5

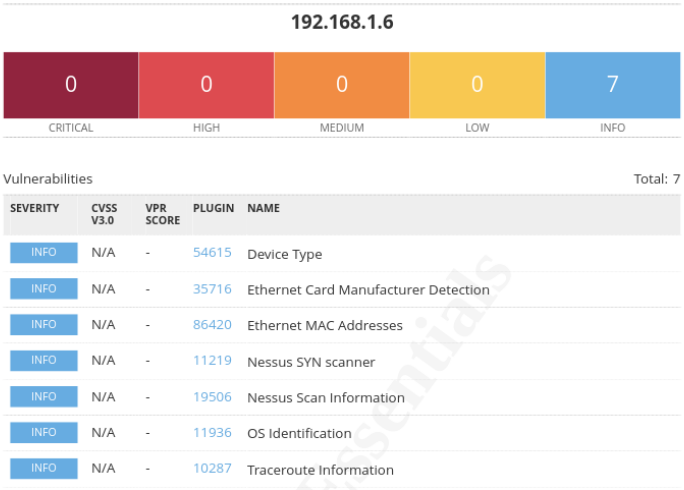
0	0	0	0	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

Figura D13. Escaneo de vulnerabilidades en el dispositivo 192.168.1.5

La Figura D14 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.6.



192.168.1.6

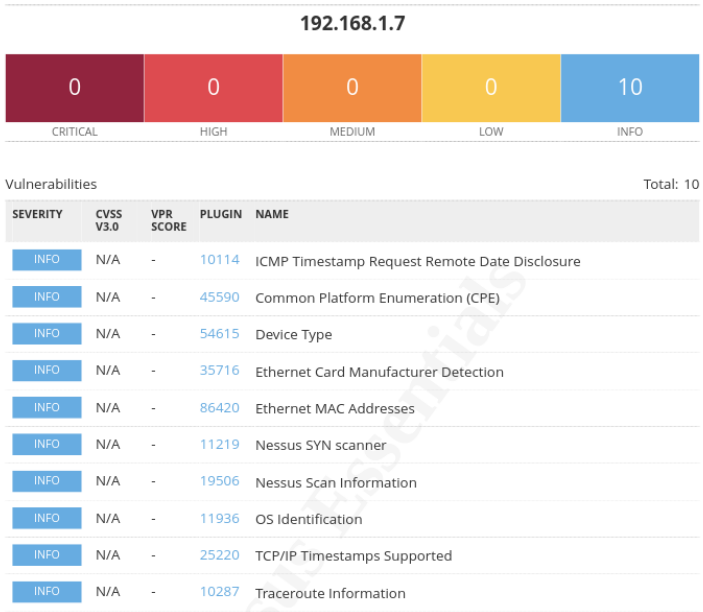
0	0	0	0	7
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10287	Traceroute Information

Figura D14. Escaneo de vulnerabilidades en el dispositivo 192.168.1.6

La Figura D15 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.7.



192.168.1.7

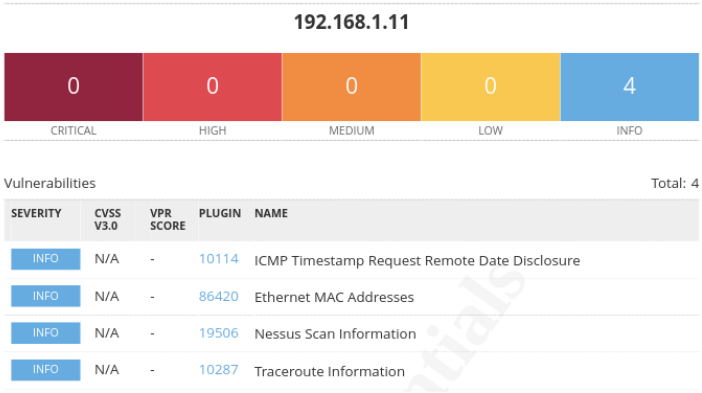
0	0	0	0	10
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 10

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

Figura D15. Escaneo de vulnerabilidades en el dispositivo 192.168.1.7

La Figura D16 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.11.



192.168.1.11

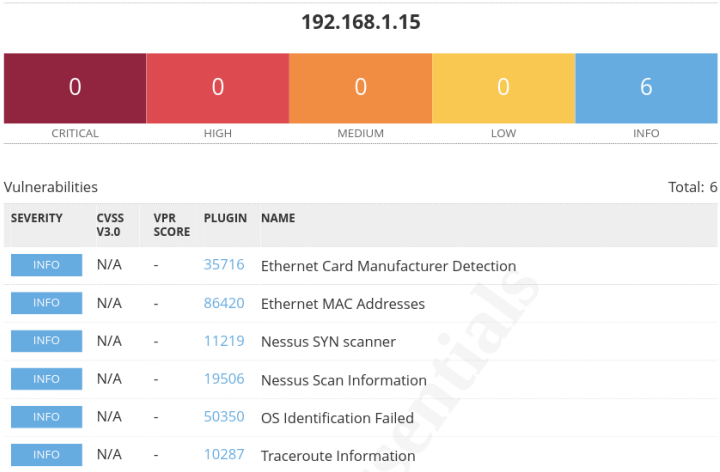
0	0	0	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

Figura D16. Escaneo de vulnerabilidades en el dispositivo 192.168.1.11

La Figura D17 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.15.



192.168.1.15

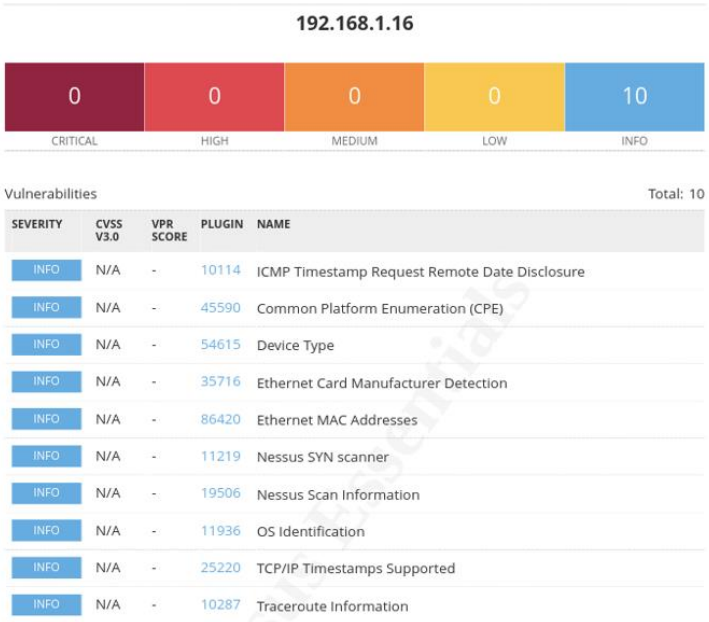
0	0	0	0	6
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 6

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	50350	OS Identification Failed
INFO	N/A	-	10287	Traceroute Information

Figura D17. Escaneo de vulnerabilidades en el dispositivo 192.168.1.15

La Figura D18 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.16.



192.168.1.16

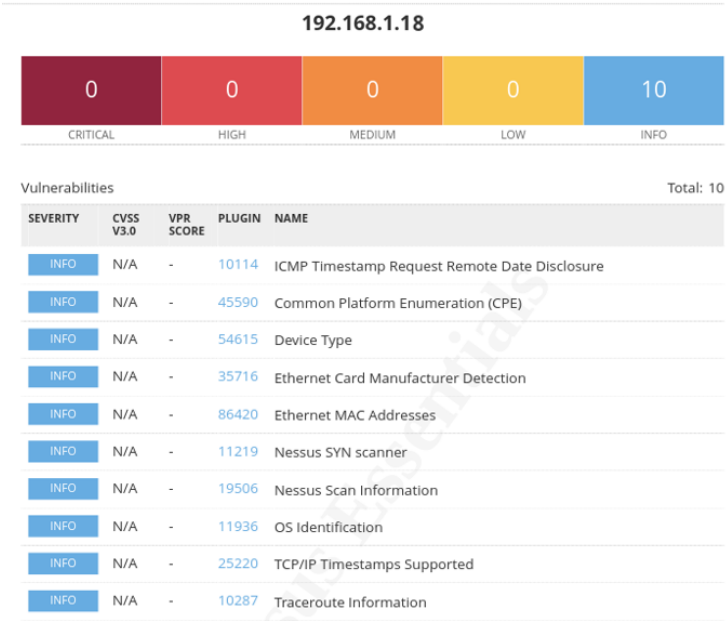
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	10

Vulnerabilities — Total: 10

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

Figura D18. Escaneo de vulnerabilidades en el dispositivo 192.168.1.16

La Figura D19 muestra el resultado del escaneo de vulnerabilidades en el dispositivo 192.168.1.18.



192.168.1.18

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	10

Vulnerabilities — Total: 10

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

Figura D19. Escaneo de vulnerabilidades en el dispositivo 192.168.1.18

La Figura E1 muestra la instalación de la herramienta Crunch en Kali Linux, utilizada para la generación de diccionarios.

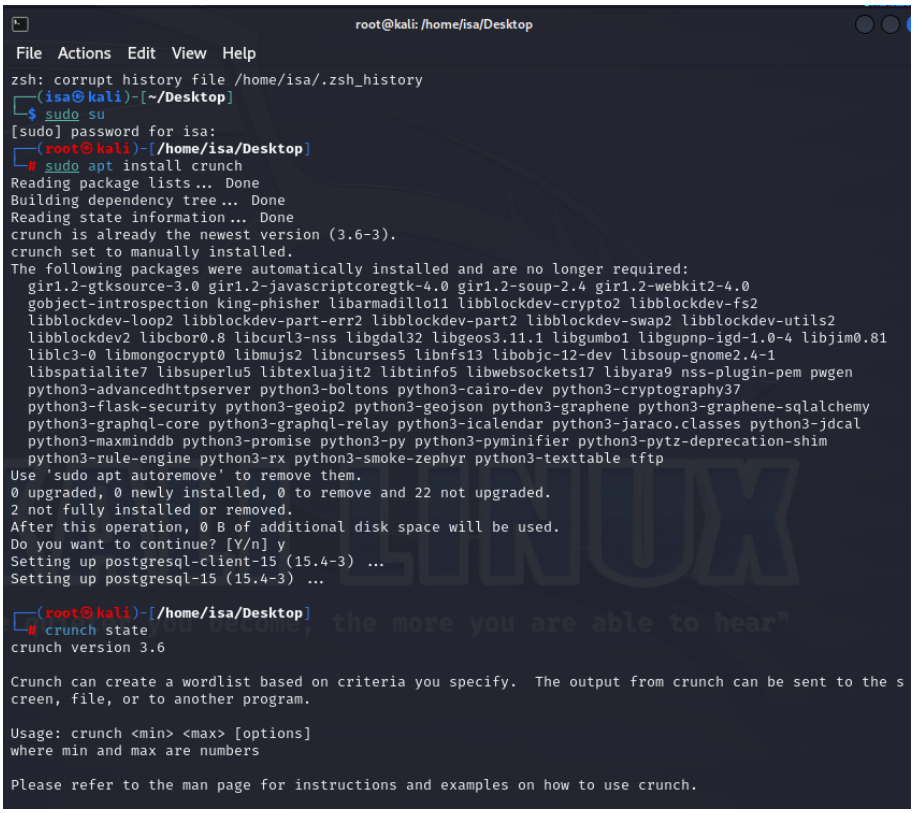


Figura E1. Instalación de la herramienta Crunch

La Figura E2 muestra el comando de instalación hping3 en la máquina virtual de Kali Linux.

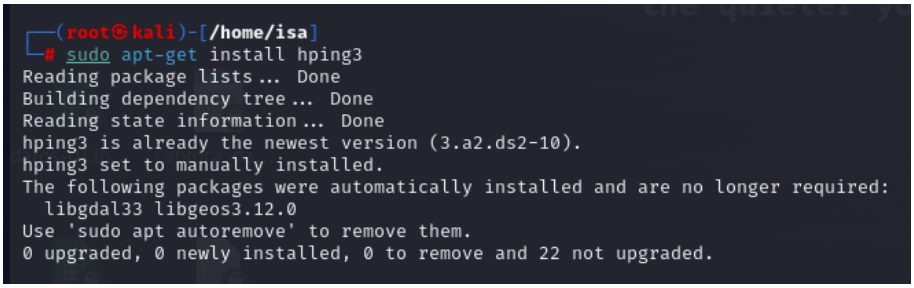


Figura E2. Instalación de Hping3

La Figura E3 muestra el comando de instalación Bettercap en la máquina virtual de Kali Linux.

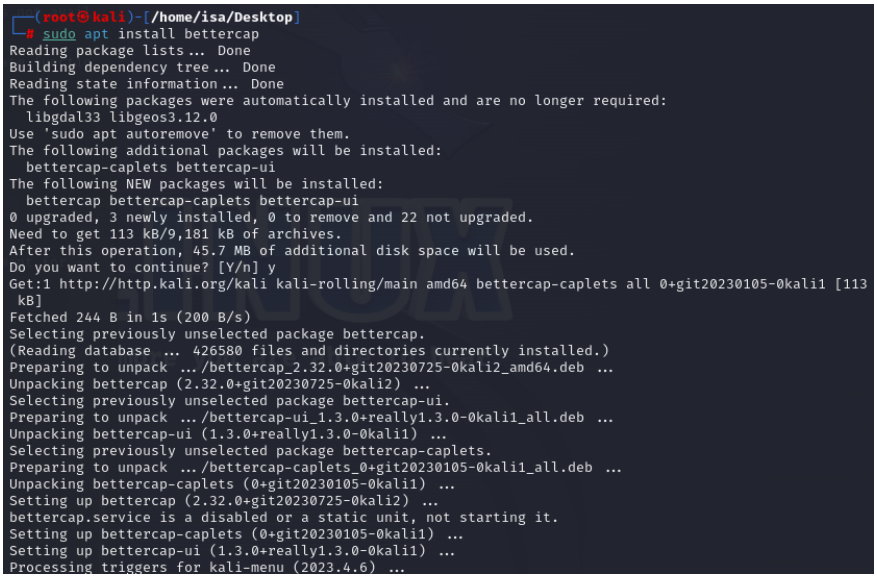


Figura E3. Instalación de Bettercap en Kali Linux

Para ingresar a la herramienta Scapy, se ingresa su nombre en el sistema, como indica la Figura E4.

Figura E4. Instalación de la herramienta Scapy en Kali Linux

El proceso de instalación y configuración de RouterSploit en la máquina virtual requiere de una serie de pasos, identificados en la Figura E5.

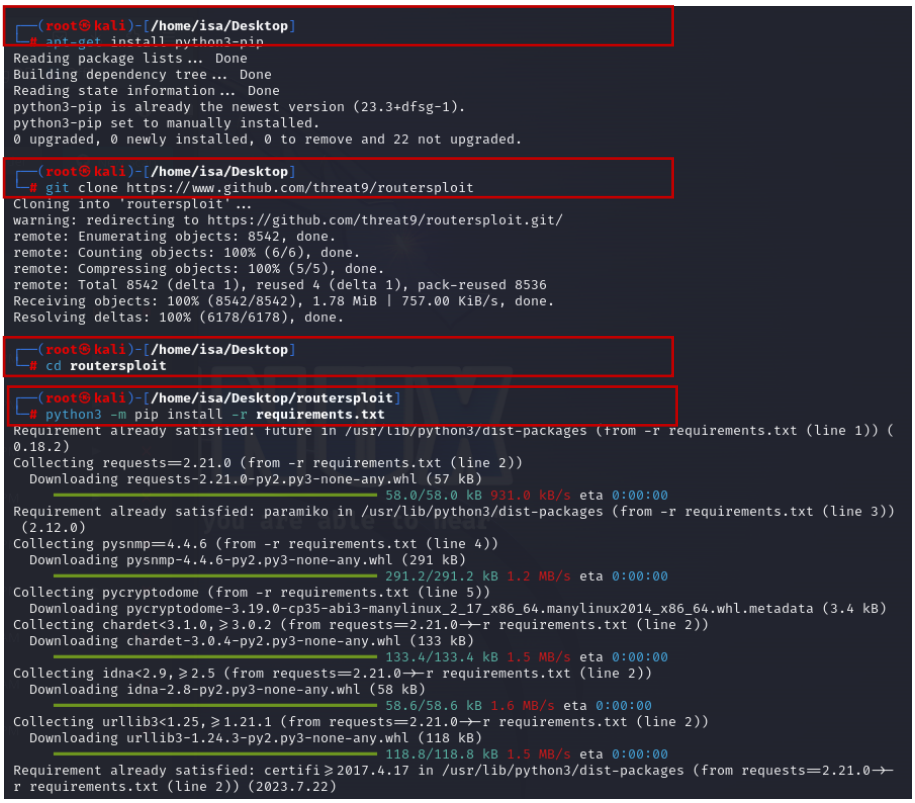


Figura E5. Proceso de instalación de RouterSploit en Kali Linux

Para ejecutar la herramienta de RouterSploit, se ejecuta el comando `rsf. py`, como se muestra en la Figura E6.

Figura E6. Ejecución de RouterSploit en Kali Linux

Anexo F. Instalación de XArp

La descarga de la herramienta XArp se realiza a través de su página oficial en XArp, como se muestra se muestra en la Figura F1.

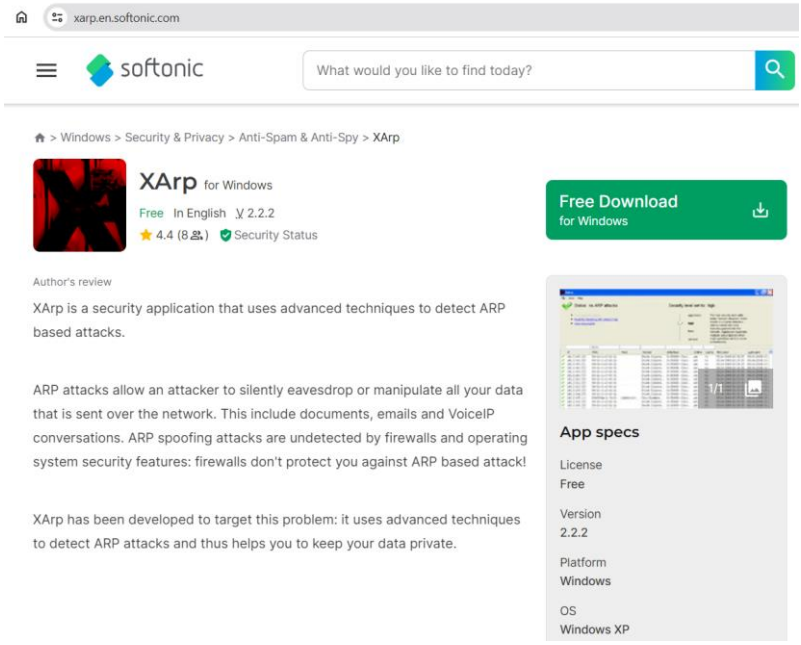


Figura F1. Descarga de la herramienta XArp mediante su página oficial

Una vez descargado el instalador del programa, se realiza su ejecución en la máquina del usuario, como muestra la Figura F2.

Figura F2. Instalación de la herramienta XArp en la máquina del usuario

Anexo G. Instalación de CrowdSec

Se ingresa a la página oficial de la herramienta, en CrowdSec , como se muestra en la Figura G1.

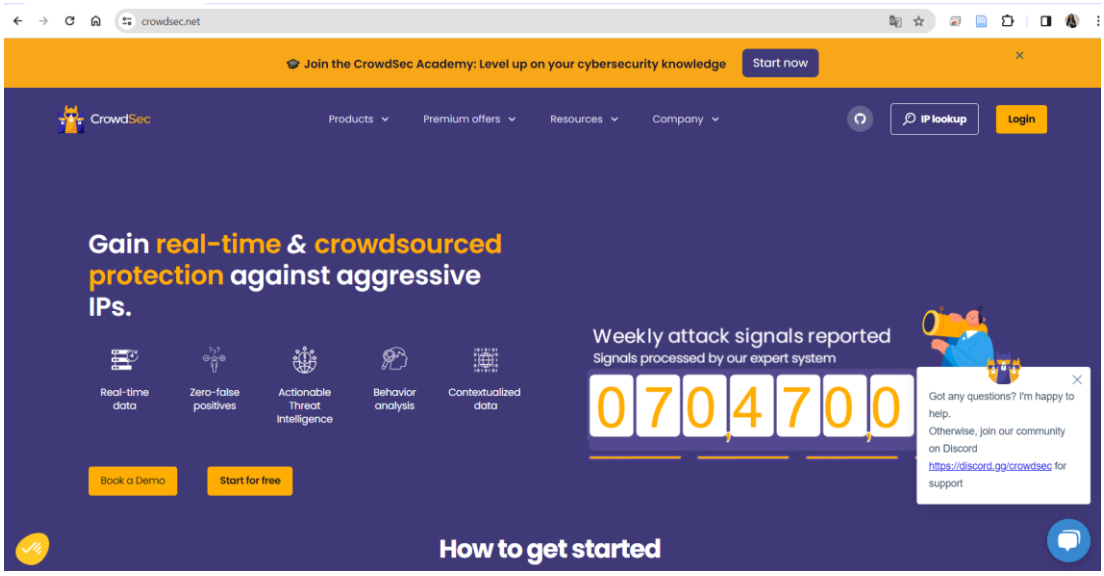


Figura G1. Página de inicio de CrowdSec

Se ingresa a la opción “Start for free” y se elige el sistema operativo en el cual se va instalar el Firewall, como se indica en la Figura G2.

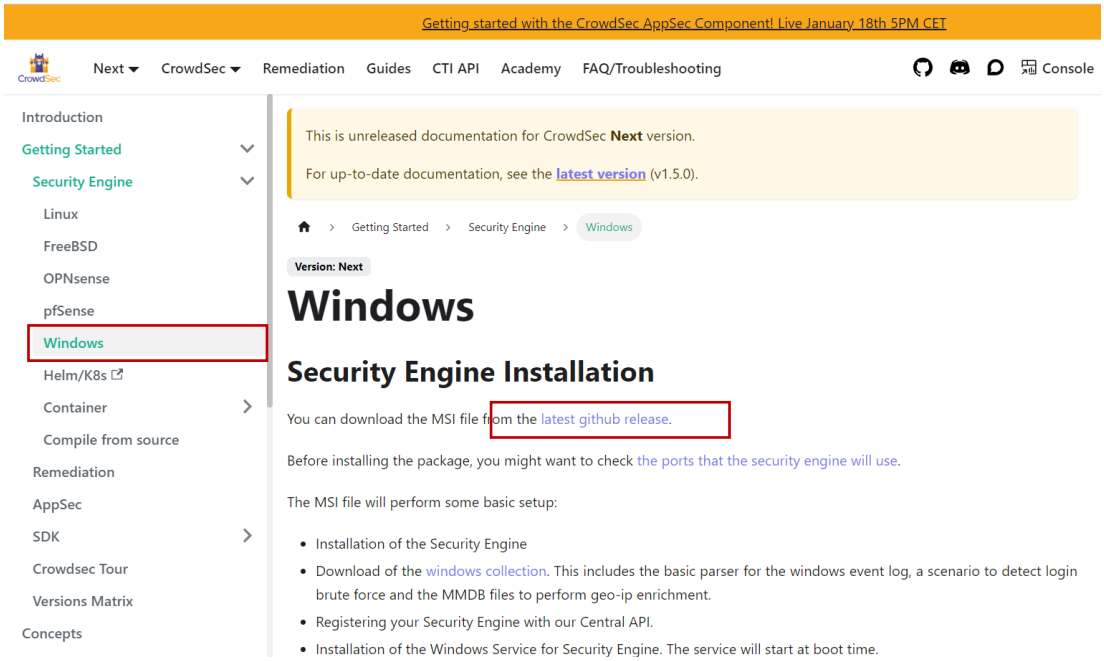


Figura G2. Elección del sistema operativo para la descarga de CrowdSec

Al ingresar a los repositorios proporcionados por la página de CrowdSec, se accede a la versión más reciente de estos y se realiza la descarga de la herramienta, como se indica en la Figura G3.

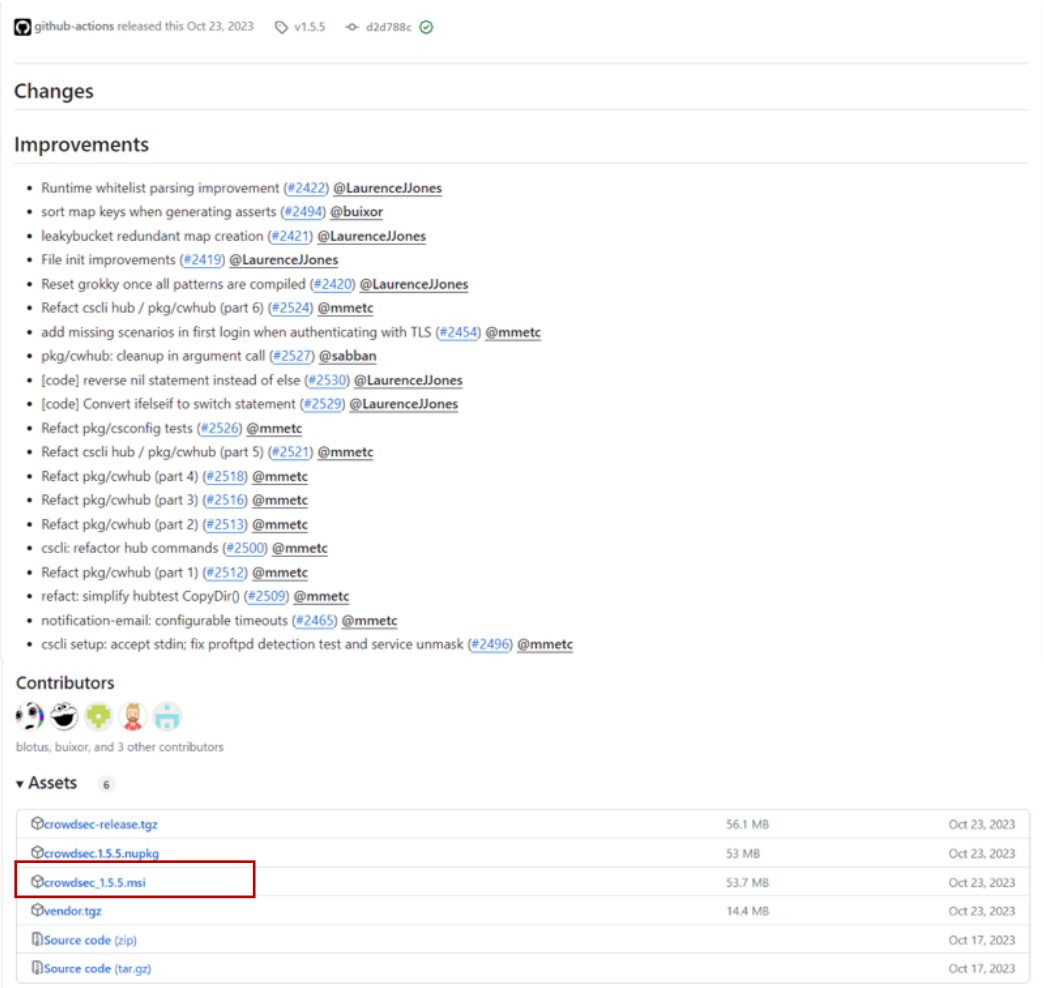


Figura G3. Descarga de la herramienta CrowdSec en la máquina

Además, también es necesario la descarga del firewall-bouncer para el funcionamiento de la herramienta, como se muestra en la Figura G4.

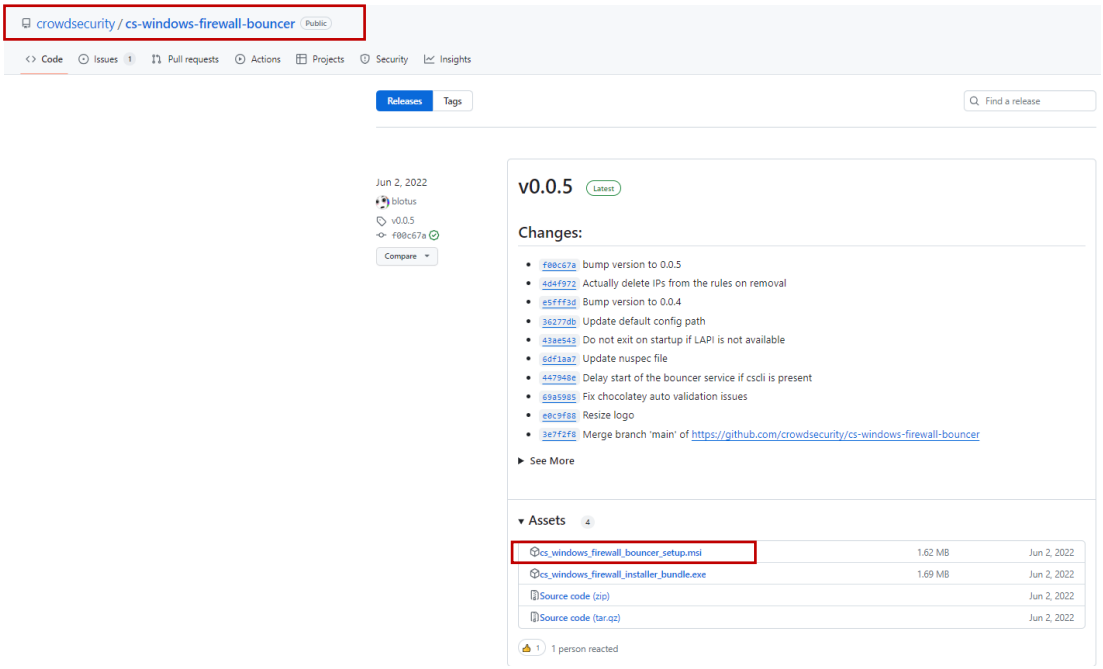


Figura G4. Descarga del firewall bouncer en la máquina

Una vez descargadas estas dos herramientas, se realiza la ejecución correspondiente del CrowdSec Setup y del Firewall Bouncer,

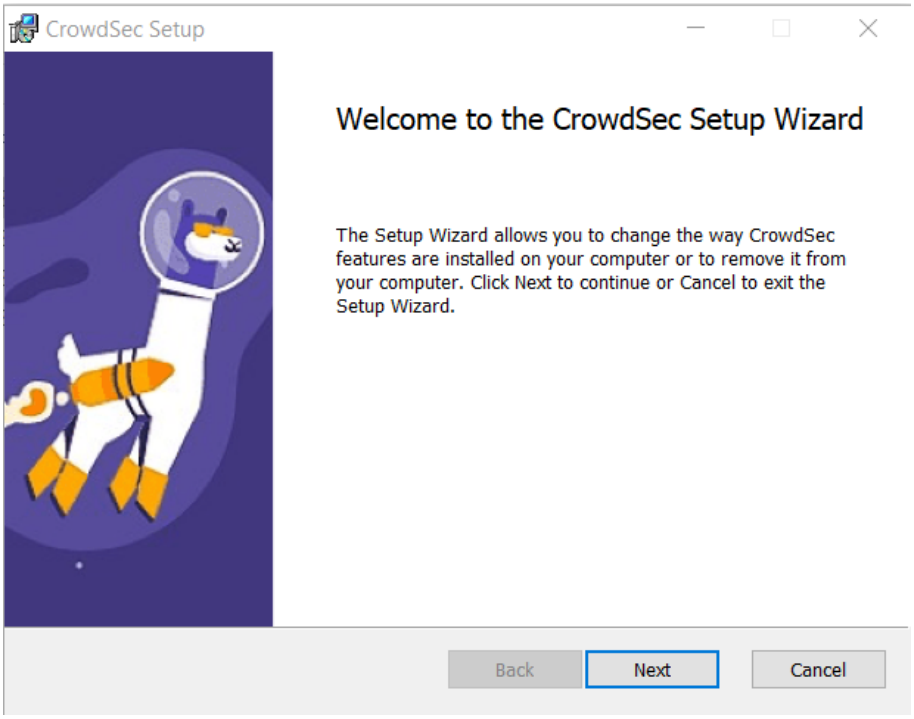


Figura G5. Ejecución del CrowdSec Setup

Figura G6. Ejecución del Firewall Bouncer