

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TELECOMUNICACIONES

Tema:

HONEYNET PARA ANÁLISIS, EVALUACIÓN Y TRATAMIENTO DE RIESGOS CIBERNÉTICOS EN UN SISTEMA IOT

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: Yulisa Francisca Acosta Proaño

TUTOR: Ing. Andrea Patricia Sánchez Zumba, Mg.

Ambato - Ecuador

agosto – 2024

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: HONEYNET PARA ANÁLISIS, EVALUACIÓN Y TRATAMIENTO DE RIESGOS CIBERNÉTICOS EN UN SISTEMA IOT, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Yulisa Francisca Acosta Proaño, 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, agosto 2024.

Firmado electrónicamente por:
ANDREA PATRICIA SANCHEZ ZUMBA

Ing. Andrea Patricia Sánchez Zumba, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: HONEYNET PARA ANÁLISIS, EVALUACIÓN Y TRATAMIENTO DE RIESGOS CIBERNÉTICOS EN UN SISTEMA IOT 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, agosto 2024.



Yulisa Francisca Acosta Proaño

C.C. 0502965544

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, agosto 2024.

Yulisa Francisca Acosta Proaño

C.C. 0502965544

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por la señorita Yulisa Francisca Acosta Proaño, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado HONEYNET PARA ANÁLISIS, EVALUACIÓN Y TRATAMIENTO DE RIESGOS CIBERNÉTICOS EN UN SISTEMA IOT, 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, agosto 2024.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

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

Firmado electrónicamente por:
JOSE VICENTE MORALES LOZADA

Ing. José Vicente Morales Lozada, Mg.
PROFESOR CALIFICADOR

Firmado electrónicamente por:
EDGAR PATRICIO CORDOVA CORDOVA

Ing. Edgar Patricio Córdova Córdova, Mg.
PROFESOR CALIFICADOR

DEDICATORIA

A mi familia, especialmente a mis padres Carmen y Francisco, que con cuya sabiduría, paciencia, apoyo y amor incondicional me han guiado en cada paso de este camino

A mis amigos, por estar siempre ahí para brindarme su apoyo incondicional

A todos aquellos que han formado parte de mi vida y me han ayudado a alcanzar este logro.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por haberme acompañado y guiado a lo largo de mi carrera.

A mi tutora Ing. Andrea Patricia Sánchez Zumba, Mg. y profesores por su valiosa orientación, sus consejos y su disposición para compartir su conocimiento y experiencia. Su apoyo académico ha sido esencial para el desarrollo de esta investigación.

A mis hermanos Patricio y Santiago, por creer en mí incluso en los momentos más difíciles. Su apoyo ha sido una fuente inagotable de fuerza y determinación.

A mis amigos Evelyn, Jorge, Ariel y Santy, por su paciencia, comprensión y por brindarme momentos de alegría y distracción necesarios para mantenerme equilibrada durante este proceso, su amistad ha sido invaluable. Y a todas las personas que me acompañaron y contribuyeron para que el desarrollo de este proyecto sea más ameno, especialmente a William. Su colaboración y aporte han sido fundamentales para la culminación de este trabajo.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA ..... **i**

APROBACIÓN DEL TUTOR ..... **ii**

AUTORÍA ..... **iii**

DERECHOS DE AUTOR ..... **iv**

APROBACIÓN DEL TRIBUNAL DE GRADO ..... **v**

DEDICATORIA ..... **vi**

AGRADECIMIENTO ..... **vii**

ÍNDICE GENERAL DE CONTENIDOS ..... **viii**

ÍNDICE DE TABLAS ..... **xii**

ÍNDICE DE FIGURAS ..... **xv**

ÍNDICE DE ANEXOS ..... **xviii**

RESUMEN EJECUTIVO ..... **xix**

ABSTRACT ..... **xx**

CAPÍTULO I. MARCO TEÓRICO **1**

1.1 Tema de investigación 1

1.1.1 Planteamiento del problema 1

1.2 Antecedentes investigativos 3

1.3 Fundamentación teórica 5

1.3.1 Industria 4.0 5

1.3.2 Internet de las cosas 7

1.3.3 Riesgos cibernéticos 17

1.3.4 Honeynet 19

1.4 Objetivos 25

1.4.1 Objetivo general 25

1.4.2 Objetivos específicos 25

CAPÍTULO II. METODOLOGÍA 26

2.1 Materiales 26

2.2 Métodos 26

2.2.1 Modalidad de la investigación 26

2.2.2 Recolección de información 27

2.2.3 Procesamiento y análisis de datos 28

CAPÍTULO III. RESULTADOS Y DISCUSIÓN 29

3.1 Seguridad en sistemas IoT para el hogar 29

3.2 Esquema General del Sistema 30

3.3 Categorías de conexiones de redes en sistemas IoT 31

3.4 Infraestructura IoT para el hogar 32

3.5 Modelos de arquitectura por capas en IoT para el hogar 33

3.6 Diseño del sistema IoT para un hogar 35

3.6.1 Selección de Sensores y Dispositivos IoT para el hogar inteligente 35

3.6.2 Ubicación de Sensores y Dispositivos IoT en el hogar 37

3.6.3 Descripción de la red IoT implementada 39

3.7 Sistema integral para seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos home 40

3.7.1 Recopilación de Marcos de referencia 40

3.7.2 Modelo de línea base para seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos domésticos 41

3.8 Análisis GAP 44

3.9 Implementación del modelo de línea base creado 47

3.9.1 Política general de seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos home. 47

3.9.2 Determinación de herramientas especializadas para la detección de posibles vulnerabilidades existentes en el sistema IoT. 48

3.9.3 Identificación y valoración de Activos del sistema IOT doméstico 48

3.10 Análisis de Vulnerabilidades del sistema IoT para el hogar 50

3.10.1 Infraestructura de la red necesaria para la honeynet 50

3.10.2 Implementación de HONEYNET 51

3.10.3 Pruebas de penetración PENTESTING 60

3.10.4 Análisis de Vulnerabilidades 60

3.11 Resultados de la Honeynet 80

3.11.1 TPOT 80

3.11.2 Implementación de Honeypot de baja interacción para detección de ataque de DoS TCP SYN Flooding con Python 82

3.12 Gestión de riegos 85

3.12.1 Matriz de riesgos 85

3.12.2 Políticas y controles 89

3.13 Plan de tratamiento de riesgos..... 91

3.13.1 Proyectos del Plan de Tratamiento de Riesgos 92

3.13.2 Validez y Gestión de Documentos..... 95

3.14 Plan de acción de tratamiento de riesgos 96

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 97

4.1 Conclusiones 97

4.2 Recomendaciones..... 99

REFERENCIAS BIBLIOGRÁFICAS 101

ANEXOS 110

ÍNDICE DE TABLAS

Tabla 1. Elementos para funcionamiento efectivo de un sistema IoT. 8

Tabla 2. Elementos para funcionamiento efectivo de un sistema IoT. 9

Tabla 3. Descripción de las capas del modelo de arquitecturas de 3 capas (Survey). 10

Tabla 4. Descripción de las capas del modelo de arquitecturas de sincronización de reloj de un sistema de acceso IoT 10

Tabla 5. Descripción de las capas del modelo de arquitectura Biométrica Descentralizada 11

Tabla 6. Descripción de las capas del modelo de arquitectura IoT Bajo un Esquema Pregunta – Respuesta 11

Tabla 7. Descripción de las capas del modelo de arquitectura NFV IoT para un ambiente médico 12

Tabla 8. Descripción de las capas del modelo de arquitectura IoT basada en la teoría fractal 12

Tabla 9. Descripción de las capas del modelo de arquitectura WBAN 13

Tabla 10. Descripción de los modelos de arquitecturas Survey de 5 capas 13

Tabla 11. Descripción del modelo de arquitectura IoT Middleware 14

Tabla 12. Descripción del modelo de arquitectura 7 capas 14

Tabla 13. Descripción del modelo de arquitectura 7 capas de la ITU-T Y.4000 15

Tabla 14. Fases de estudio de seguridad y opciones a adoptar 17

Tabla 15. Principales riesgos y problemas de seguridad en IoT 19

Tabla 16. Ventajas y limitaciones de Honeynets 21

Tabla 17. Recolección de información..... 27

Tabla 18. Ventajas y Desafíos de las categorías de los sistemas IoT 32

Tabla 19. Análisis de las arquitecturas de 3 capas en IoT 33

Tabla 20. Análisis de las arquitecturas de 4 capas en IoT 34

Tabla 21. Análisis de las arquitecturas de 6 capas o más en IoT 34

Tabla 22. Dispositivos y sensores IoT del sistema 36

Tabla 23. Niveles de madurez en análisis para la mejora de la seguridad cibernética45

Tabla 24. Comparativa de herramientas para detección de vulnerabilidades 48

Tabla 25. Tipos de activos 49

Tabla 26. Análisis de cada uno de los activos del Hogar..... 50

Tabla 27. Comparativa de tipos de honeypots 52

Tabla 28. Honeypots de interacción baja y media especializados para IoT 52

Tabla 29. Comparativa para la creación de honeypot 56

Tabla 30. Comparativa de base de datos..... 58

Tabla 31. Detalle de vulnerabilidades detectadas en IPs 60

Tabla 32. Detalle de Remediación Vulnerabilidades – Activos Involucrados..... 61

Tabla 33. SSL Certificate Cannot Be Trusted..... 61

Tabla 34. SSL Self-Signed Certificate..... 63

Tabla 35. TLS Version 1.0 Protocol Detection..... 64

Tabla 36. SSL RC4 Cipher Suites Supported (Bar Mitzvah)..... 66

Tabla 37. TLS Version 1.1 Deprecated Protocol..... 67

Tabla 38. Comparativa de herramientas para identificación y análisis..... 74

Tabla 39. Catálogo de amenazas 86

Tabla 40. Probabilidad x Impacto/Consecuencia 87

Tabla 41. Matriz de Calificación, Evaluación y Respuesta de los Riesgos 87

Tabla 42. Identificación de riesgos 88

Tabla 43. Matriz de riesgos 89

Tabla 44. Resumen del Plan de Tratamiento de Riesgos 92

Tabla 45. Acceso no autorizado a la red 92

Tabla 46. Versiones desactualizadas de software/firmware 93

Tabla 47. Protocolos de comunicación no encriptados 94

Tabla 48. Protocolos de comunicación no encriptados 95

Tabla 49. Plan de acción de tratamiento de riesgos 96

ÍNDICE DE FIGURAS

Figura 1. Industria 4.0, tecnologías básicas 6

Figura 2. Arquitectura de funcionamiento de Tuya 16

Figura 3 Esquema Honeynet 19

Figura 4. Arquitectura de Honeyd 22

Figura 5. Honeypots en IoT 23

Figura 6. Arquitectura de Cowrie 24

Figura 7. Esquema general del Sistema 30

Figura 8. Modelo básico de la red para IoT 33

Figura 9. Modelo de arquitectura IoT (ITU-T Y.4000) 35

Figura 10. Ubicación de sensores y dispositivos IoT en la planta baja..... 37

Figura 11. Ubicación de sensores y dispositivos IoT en la planta alta 38

Figura 12. Esquema de red del sistema IoT 39

Figura 13. Madurez del análisis GAP inicial 46

Figura 14. Madurez del análisis GAP esperado 46

Figura 15. Diagrama de la infraestructura de la red..... 51

Figura 16. Diagrama de gestión de la red 53

Figura 17. Interfaz de inicio de TPOT 55

Figura 18. Visualización de funcionamiento de TPOT con Kibana 55

Figura 19. Captura de ataques en TPOT 56

Figura 20. Captura de datos en honeypot..... 57

Figura 21. Base de datos en Mongo 58

Figura 22. Evidencia de configuración y expedición del certificado SSL. 62

Figura 23. Evidencia de configuración y expedición del certificado SSL en TPOT . 62

Figura 24. Evidencia de configuración y expedición del certificado SSL 64

Figura 25. Evidencia de configuración y expedición del certificado SSL en TPOT . 64

Figura 26. Evidencia de uso de cifrado TLSv1.0. 65

Figura 27. Evidencia de uso de cifrado TLSv1.0 en TPOT 65

Figura 28. Evidencia de suit de cifrado identificados 66

Figura 29. Evidencia de suit de cifrado identificados en TPOT 67

Figura 30. Evidencia de uso de cifrado TLSv1.1. 68

Figura 31. Evidencia de uso de cifrado TLSv1.1 en TPOT. 68

Figura 32. verificación de la tarjeta WiFi 69

Figura 33. Escaneo de redes cercanas para realizar ataque 71

Figura 34. verificación del ataque a la red 73

Figura 35. Mapeo de identificación 75

Figura 36. Acceso al dispositivo IoT con Hércules 75

Figura 37. Ataque dirigido 76

Figura 38. Captura del tráfico generado por el ataque 76

Figura 39. Captura de trama en IP 10.10.10.236 77

Figura 40. Resultado del ataque 77

Figura 41. Captura para análisis detallado de las comunicaciones del dispositivo 78

Figura 42. Script para tener el control del dispositivo 79

Figura 43. Verificación del control y monitoreo del dispositivo 80

Figura 44. Conexión SSL/TLS con el servidor en el puerto 443 81

Figura 45. Conexión SSL/TLS para inspección del certificado SSL 81

Figura 46. Captura de CVE en TPOT 82

Figura 47. Registro de ataques a TPOT 82

Figura 48. Ataque DoS TCP SYN Flooding desde Kali Linux 83

Figura 49. Captura y Registro de solicitudes maliciosas por medio del puerto 6668/TCP 83

Figura 50. Inundación TCP SYN en honeypot 84

Figura 51. Registro de solicitudes maliciosas por medio del puerto 6668/TCP 84

ÍNDICE DE ANEXOS

Anexo A. Política General de Seguridad de la Información 110

Anexo B. Criterios de valoración para los activos y Matriz de riesgos 116

Anexo C. Sniffer 119

Anexo D. Informe técnico a detalle de las pruebas de penetración 122

Anexo E. Análisis de red con la herramienta Nessus 153

Anexo F. Políticas 164

Anexo G. Controles 182

Anexo H. Plan de tratamiento de riesgos 194

Anexo I. Recopilación de tablas 202

RESUMEN EJECUTIVO

La seguridad de los sistemas IoT domésticos es crucial para proteger datos sensibles y garantizar la integridad, disponibilidad y confidencialidad de la información y de los dispositivos. Se utilizó Nessus para analizar las vulnerabilidades de los dispositivos inteligentes más comunes en el mercado. Con estos hallazgos, se diseñó una Honeynet que expone dichas vulnerabilidades para visibilizar los posibles ataques a los dispositivos IoT del hogar.

Se llevaron a cabo pruebas de penetración para evaluar la seguridad de los dispositivos del sistema IoT doméstico, y también pruebas a través de la Honeynet, que incluyeron hacking de la red WiFi y control de los dispositivos IoT desde la LAN. Los honeypots utilizados en el proyecto son ConPot y CitrixHoneypot, que registraron explotaciones de las vulnerabilidades CVE-2013-2566 y CVE-2015-2808. Además, se creó un honeypot específico en Python para capturar ataques DoS TCP SYN Flooding en el puerto 6668/TCP con el servicio IRC.

Los resultados de estas pruebas fueron fundamentales para desarrollar un plan de tratamiento de riesgos, que se basa en un modelo de línea base para la seguridad de los datos, la privacidad de las personas y los dispositivos IoT en entornos domésticos, se incluyó un análisis GAP para determinar el estado actual del sistema. El plan de tratamiento de riesgos propone controles y políticas específicas para mitigar los riesgos identificados y fortalecer la seguridad del sistema IoT, garantizando una protección continua y robusta para los dispositivos IoT en hogares inteligentes.

Palabras clave: Honeynet, IoT doméstico, seguridad, vulnerabilidad, riesgo, mitigación, pruebas de penetración.

ABSTRACT

The security of home IoT systems is critical for protecting sensitive data and ensuring the integrity, availability, and confidentiality of information and devices. Nessus was utilized to analyze the vulnerabilities of the most common smart devices on the market. Based on these findings, a Honeynet was designed to expose these vulnerabilities and illustrate potential attacks on home IoT devices.

Penetration tests were conducted to assess the security of devices within the home IoT system, as well as tests through the Honeynet, which included WiFi network hacking and control of IoT devices from the LAN. The honeypots deployed in the project are ConPot and CitrixHoneypot, which logged exploits of vulnerabilities CVE-2013-2566 and CVE-2015-2808. Additionally, a custom honeypot in Python was created to capture TCP SYN Flooding DoS attacks on port 6668/TCP utilizing the IRC service.

The results of these tests were crucial in developing a risk treatment plan, based on a baseline model for data security, privacy of individuals, and IoT devices in home environments. A GAP analysis was conducted to determine the current state of the system. The risk treatment plan proposes specific controls and policies to mitigate identified risks and enhance the security of the IoT system, ensuring continuous and robust protection for IoT devices in smart homes.

Keywords: Honeynet, home IoT, security, vulnerability, risk, mitigation, pentesting.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

HONEYNET PARA ANÁLISIS, EVALUACIÓN Y TRATAMIENTO DE RIESGOS CIBERNÉTICOS EN UN SISTEMA IOT

1.1.1 Planteamiento del problema

El uso de dispositivos IoT (Internet de las cosas) ha crecido exponencialmente en la última década, convirtiéndose en un nuevo objetivo de los ciber atacantes, porque estos dispositivos no cuentan con software antispam y antivirus como lo hacen las tabletas, computadoras o smartphones. En 2021, las organizaciones en los Estados Unidos experimentaron un promedio de 443 ataques semanales, lo que representa un aumento del 17% en comparación con el inicio de este año. En la región de Europa, Oriente Medio y África (EMEA), el promedio semanal de ataques por organización fue de 777, lo que supone un incremento del 36%. Las organizaciones en la región de Asia-Pacífico (APAC) sufrieron 1338 ataques semanales, un aumento del 13% [1].

En el mismo año, el análisis de los datos recogidos en los honeypots de Kaspersky revela que existe una tendencia constante al aumento del número de ataques en contra de dispositivos IoT. En el primer semestre de 2021, el número de intentos de infección totales alcanzó los 1.515.714.259, mientras que durante los seis meses anteriores fueron 639.155.942, en la mayoría de los casos, los intentos de conexión usaron el protocolo telnet (utilizado para acceder y gestionar un dispositivo de forma remota); el resto utilizó SSH y web. Además, según el Informe de Riesgos Globales 2023 del Foro Económico Mundial, en diciembre de 2022, se descubrió una falla crítica de seguridad pues los datos reflejan que más de 100 intentos de explotar vulnerabilidades fueron detectados cada minuto [2-3].

Es importante mencionar que la aplicación threat map de Check Point resalta los ataques cibernéticos de todo el mundo, se puede visualizar el país origen, de destino y el tipo de ataque, así como su estadística diaria individual, su análisis se centra en contabilizar la mayor cantidad de ataques, como secuestro de datos a entidades

bancarias y a dispositivos móviles. Los datos revelan que en 2023, al realizar el análisis de los tipos de malware, secuestro de datos o ransomware y su accionar en Sudamérica, los países Bolivia (11,2%) y Ecuador (9,6%) tienen un alto porcentaje de ataques cibernéticos, los dispositivos móviles, sistemas IoT y computadoras son un claro ejemplo de estos ataques, pues son vulnerados por una variedad de troyanos disfrazados en aplicaciones móviles normales que una vez instaladas en el dispositivo móvil, inundan de anuncios publicitarios, los países que tienen más ataques de este tipo son: Brasil (5,3%), Ecuador (3,9%) y Colombia (1,8%) [4].

Tanto a nivel mundial como en Ecuador, los delitos informáticos se visibilizan fuertemente en los últimos años, durante y después de la pandemia, la tecnología y los sistemas IoT forman parte de la vida de cada persona. Un informe estadístico de la Unidad de Ciberdelitos de la Policía Nacional del Ecuador muestra que, desde el 2017 hasta junio del 2023, se han registrado 2863 denuncias por delitos informáticos por acceso no consentido a un sistema informático, telemático o de telecomunicaciones, apropiación fraudulenta por medios electrónicos y ataque a la integridad de sistemas informáticos. Pichincha, Guayas, Imbabura, Manabí, Carchi y Azuay son las provincias con más casos registrados en este tiempo [5].

Las estadísticas presentadas por EcuCERT de ARCOTEL, revelan el número de IPs notificadas por vulnerabilidad, el reporte más reciente se da en agosto del 2023 con 4.819 direcciones IP y 14.267 direcciones IP notificadas por incidente en el país, por otra parte, de acuerdo con las denuncias presentadas en la fiscalía general del Estado, los delitos cibernéticos se encuentran en el top cinco a nivel de delitos denunciados en Ecuador hasta mediados del año 2023, ocupando el puesto número dos con 3.962 denuncias por apropiación fraudulenta por medios electrónicos, y en el puesto número cuatro con 274 denuncias, por acceso no consentido a un sistema informático [6-7].

Cabe mencionar que el promedio anual de denuncias en Tungurahua es 1.609, y presenta una tasa de variación, también promedio de 3.6%, recalcando que en la provincia de Tungurahua existen varios casos por delitos cibernéticos según el análisis de delincuencia e inseguridad ciudadana en Ambato. Los sistemas IoT han crecido de manera significativa, por lo que, se hace necesario implementar actividades que cooperen con la identificación de las prácticas de seguridad, con el fin de salvaguardar

la información personal e institucional de los principales ataques como: DoS, robo de identidad, ataques tipo Man-in-the-Middle, ataques de ingeniería social y otros [8].

El vertiginoso aumento de dispositivos IoT no seguros o mal configurados, ha emergido como una causa primordial detrás del crecimiento exponencial de amenazas cibernéticas en sistemas IoT, pues la proliferación de estos dispositivos, caracterizada por deficiencias en seguridad y configuraciones inadecuadas, ha creado una brecha significativa en la infraestructura digital. Esta vulnerabilidad ha permitido a actores malintencionados infiltrarse y comprometer la integridad de sistemas previamente considerados seguros. La falta de estándares de seguridad uniformes y la escasa conciencia sobre las medidas preventivas han contribuido a un escenario inseguro por el aumento descontrolado de dispositivos IoT, lo que se traduce en un incremento alarmante en las amenazas cibernéticas, planteando desafíos significativos para la confidencialidad, la integridad, y la disponibilidad de la información en entornos IoT.

Por otro lado, la existencia de vectores de ataque sofisticados en el ciberespacio ha desencadenado una serie de consecuencias negativas, la primera a considerar es la pérdida de datos confidenciales. Las organizaciones, a menudo, se encuentran luchando para mantenerse a la par con estas tácticas de ataques avanzadas, sin embargo, se plantean interrogantes sobre la capacidad de las actuales defensas cibernéticas para enfrentar la constante evolución de las ciberamenazas.

La carencia de soluciones de seguridad adecuadas para el IoT ha generado interrupciones en las operaciones de sistemas IoT críticos, porque existe una brecha insegura que los crackers explotan con facilidad, y han conseguido afectar sectores importantes como los de la salud, la energía y el transporte, por lo que plantear soluciones robustas para la seguridad, resulta un desafío inmediato para la estabilidad operativa, económica, política y social.

1.2 Antecedentes investigativos

Concluida la revisión bibliográfica en repositorios universitarios y diversas bases de datos especializadas en artículos científicos, se pueden detallar los antecedentes que emergen de esta investigación.

En 2021, Santiago Manzano y Rubén Terán, de la Universidad Técnica de Ambato, realizaron un "DESPLIEGUE DE UN HONEYNET BASADO EN REDES DEFINIDAS POR SOFTWARE PARA UN ISP". El proyecto aborda la preocupación de los proveedores de servicios de Internet (ISPs) por el tráfico de datos en su infraestructura. Debido al incremento de suscriptores y la necesidad de ampliar el ancho de banda a menor costo, se implementó el protocolo OpenFlow en dispositivos Mikrotik y una red definida por software (SDN) con HPE VAN SDN como orquestador. Se realizaron pruebas de velocidad y rendimiento de ancho de banda, y se mejoró la seguridad perimetral con honeypots configurados en distribuciones como Honeydrive y T-Pot para crear una honeynet. Los resultados muestran que la honeynet puede anticipar ataques frecuentes, identificando puertos vulnerables, direcciones IP y dominios de origen [9].

Por otro lado, en 2021, Diego Ordóñez de la Universidad Técnica Equinoccial publicó el artículo "REDUCIENDO LA BRECHA DE SEGURIDAD DEL IOT CON UNA ARQUITECTURA DE MICROSERVICIOS BASADA EN TLS Y OAUTH2". Analizó la seguridad en entornos de hogar inteligente, donde la heterogeneidad tecnológica genera problemas de autenticación y confidencialidad de datos. Para abordar estos problemas, se usaron tecnologías de vanguardia como OAuth2 y TLS junto a una arquitectura de microservicios. La división en capas funcionales permite la integración transparente de dispositivos fijos y móviles. El esquema de seguridad en tres niveles facilita la adaptación según los recursos computacionales y el tipo de información. Los resultados destacan la flexibilidad y solidez de la arquitectura IoT segura propuesta [10].

En 2021, Ibai Castañón de la Universidad de León presentó el "ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA HONEYNET PARA EL ESTUDIO DE MALWARE EN ENTORNOS INDUSTRIALES IOT". El proyecto propuso una honeynet en un entorno industrial IoT utilizando honeypots de código abierto como Honeyd para monitorear la red y recoger muestras de malware. Estas muestras se envían al sistema de análisis Cowrie - IoT Device para su evaluación y generación de informes. Los resultados muestran que una tarea cron se activa cada cinco minutos para copiar el primer elemento del directorio de muestras, moverlo y borrar el original. La copia se analiza y se guarda un reporte con los datos obtenidos [11].

De igual manera, en 2022, Andrade, Ortiz, Cazares, Navas, y Sánchez publicaron "DEFINING CYBER RISK SCENARIOS TO EVALUATE IOT SYSTEMS". El estudio propone una metodología para el análisis de riesgos de seguridad en dispositivos IoT, utilizando escenarios basados en factores de riesgo. Para gestionar la incertidumbre en el comportamiento de IoT, se emplean redes bayesianas junto con el Best Worst Method (BWM) para la toma de decisiones multicriterio y obtener un valor cuantitativo de riesgo. Los resultados muestran un riesgo de ataque del 65% en la simulación, indicando que la superficie de ataque se expande con el aumento de dispositivos IoT, ya que se generan más puntos de entrada y salida. El modelo de red bayesiana (BN) se seleccionó como la solución adecuada para evaluar eficazmente la seguridad en sistemas IoT [12].

En 2023, Rabzelj, Južnič, Volk, Kos, Kren, y Sedlar de la Universidad de Liubliana publicaron el artículo "Designing and Evaluating a Flexible and Scalable HTTP Honeypot Platform: Architecture, Implementation, and Applications". El estudio aborda el aumento de ciberataques debido a la digitalización y la proliferación de dispositivos IoT y servicios en la nube sin medidas de seguridad adecuadas. Proponen y evalúan un sistema honeypot flexible basado en HTTP que puede imitar cualquier servicio y aplicación HTTP. Implementaron 14 servicios y realizaron un experimento de 4 meses, recopilando datos de atacantes. Los resultados muestran que los honeypots seleccionan dinámicamente la tecnología emulada y bloquean respuestas a direcciones IP específicas. De esta forma, una única dirección IP podría aparecer como varios dispositivos para varios atacantes al mismo tiempo, y se podría servir un mayor número de respuestas dinámicas y probar su atractivo, ofreciendo respuestas dinámicas para aumentar el realismo y efectividad de los honeypots [13].

1.3 Fundamentación teórica

1.3.1 Industria 4.0

El término Industria 4.0 surgió en 2011 durante la Feria de Hannover con el objetivo de impulsar la economía alemana. Su propósito es automatizar la producción y liberar los procesos productivos de la intervención humana. Los principales aportes de la

Industria 4.0 al mundo empresarial incluyen la digitalización de los sistemas de producción e información para la gestión y planificación de la producción, la automatización de sistemas para la adquisición de datos de las líneas de producción y las máquinas, y el uso de sistemas ciberfísicos como el IoT, IoS y la fábrica inteligente [14-15].

Un gran número de avances tecnológicos que forman la base de la industria 4.0 han producido una transformación significativa en la producción. Las celdas aisladas y poco optimizadas han evolucionado para convertirse en un flujo de producción completamente integrado, automatizado y optimizado, lo que se traduce en una mayor eficiencia y productividad [16].

a. Tecnologías de la Industria 4.0

Las Tecnologías de la Industria 4.0 son similares a las utilizadas para la Transformación digital y experimentan cambios importantes en las interrelaciones entre humanos y máquinas. La Figura 1 muestra las nueve tecnologías básicas de la Industria 4.0 [16].

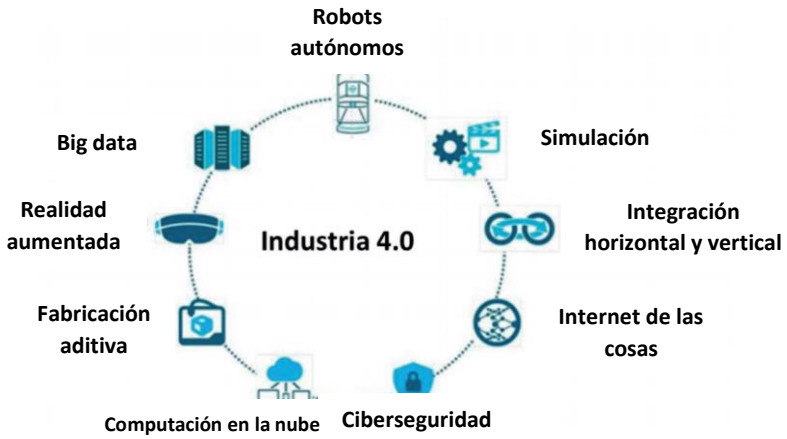


Figura 1. Industria 4.0, tecnologías básicas [16].

A continuación, se describen las tecnologías básicas de la Industria 4.0 [16-18].

- ***Robots autónomos.*** Se implementan para minimizar errores en tareas sencillas, aumentar la eficiencia de las líneas de producción y optimizar el sistema.

- ***Simulación.*** Se utiliza en el sistema productivo para programar la producción a través de un entorno ciberfísico que tiene en cuenta las redes de suministro.

- ***Integración horizontal y vertical.*** Analiza los sistemas como un todo y propone cambios estructurales en los objetos físicos y su conexión

- ***Internet de las cosas.*** Se refiere a escenarios en los que la conectividad de la red y la capacidad se extienden a objetos, sensores y artículos de uso diario.

- ***Ciberseguridad.*** Es un conjunto de prácticas, procesos y tecnologías diseñadas para gestionar el riesgo del ciberespacio.

- ***Computación en la nube.*** Es un modelo que permite el acceso ubicuo y bajo demanda a un conjunto compartido de recursos informáticos configurables**.**

- ***Fabricación auditiva.*** Se caracteriza por la flexibilidad en la fabricación, apoyado en el uso de prototipos e impresión 3D.

- ***Realidad aumentada.*** Es una pantalla interactiva que usa la capacidad de las computadoras para crear una experiencia similar al mundo real.

- ***Big data:*** Se refiere a la gran cantidad de datos, tanto estructurados como no estructurados, disponibles en internet, pueden proporcionar información útil.

1.3.2 Internet de las cosas

El concepto de Internet de las Cosas se refiere a situaciones en las que la conectividad de red y la capacidad de procesamiento se extienden a objetos, sensores y artículos cotidianos que tradicionalmente no se consideran computadoras. Esto permite que estos dispositivos produzcan, intercambien y utilicen datos con una intervención humana mínima. El primer dispositivo para IoT fue una tostadora conectada a través de IP que se podía encender y apagar a través de internet [19].

a. Infraestructura

La infraestructura de un sistema de IoT se refiere a la combinación de tecnologías, dispositivos, redes y plataformas que permiten la conexión, recopilación, procesamiento y gestión de datos generados por los dispositivos IoT. Esta

infraestructura es fundamental para el funcionamiento efectivo de los sistemas de IoT y puede incluir los siguientes elementos que se muestran en la Tabla 1 [20]:

Tabla 1. Elementos para funcionamiento efectivo de un sistema IoT [20].

Elemento	**Descripción**
Redes de comunicación	Incluyen tecnologías de conectividad que permiten la comunicación entre los dispositivos IoT y las plataformas de gestión.
Dispositivos IoT	Comprenden sensores, actuadores, y otros dispositivos conectados que recopilan información del entorno físico y la transmiten a la infraestructura de IoT.
Plataformas de gestión de IoT	Son sistemas de software que permiten la administración, procesamiento, análisis y visualización de los datos generados por los dispositivos IoT.
Sistemas de procesamiento de datos	Permiten el procesamiento y la gestión eficiente de grandes volúmenes de datos generados por los dispositivos IoT.

La ITU-T Y.4113 en sus recomendaciones de infraestructura, propone un modelo básico de la red para IoT. El dispositivo es un equipo con capacidades obligatorias de comunicación y capacidades opcionales de detección, actuación, captura de datos, almacenamiento de datos y procesamiento de datos con respecto a la IoT [21].

El gateway es una unidad con respecto al IoT que interconecta los dispositivos con la red central realiza la traducción necesaria entre los protocolos utilizados en la red central y los utilizados por los dispositivos [21].

La red central es una parte del sistema de prestación compuesta por redes, equipos e infraestructuras, conecta el dominio del proveedor de servicios a la red de acceso [21].

La red de área de IoT es una red de dispositivos para IoT y puertas de enlace que están interconectados. La conectividad se logra a través de conexiones locales, normalmente utilizando tecnologías de comunicación de corto alcance [21].

La plataforma IoT es una infraestructura técnica que proporciona integración de capacidades genéricas y específicas. Estas, junto con las capacidades de la red central, pueden estar expuestas a uno o más servidores de aplicaciones de IoT. La red central proporciona funcionalidades de comunicación para respaldar la transferencia de datos

a dispositivos y puertas de enlace a través de la red de acceso. El servidor de aplicaciones de IoT ejecuta aplicaciones y se comunica con dispositivos, puertas de enlace y plataformas de IoT a través de la red central directamente para brindar servicios de aplicaciones [21].

b. Arquitectura

Una arquitectura debe cumplir requerimientos para que sea viable, debe basarse en 5 pilares fundamentales que son: tecnología distribuida, arquitectura escalable, eficiencia energética, seguridad y conectar al mundo con la web. Los componentes de IoT, se categorizan acorde a la información de la Tabla 2 [22]:

Tabla 2. Elementos para funcionamiento efectivo de un sistema IoT [22].

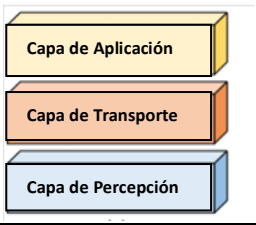
Elemento	**Servicio IoT**	**Gateway**	**Nodos receptores**
Función	Proporcionar servicios de autenticación, manejo de eventos, notificaciones, interfaz gráfica y análisis y almacenamiento de datos.	Proporcionar interconectividad, recopilar datos, transmitir instrucciones y actuar como broker de la red.	Electrodomésticos o sensores para monitorear el entorno físico en el que se encuentran
Requerimientos energéticos	El consumo es alto y requiere alimentación continua, refrigeración y una fuente de poder robusta	El consumo es moderado debido a la necesidad de permanecer alimentado de forma continua.	Bajo consumo, se puede alimentar con baterías.
Requerimientos Computacionales	Se necesita un procesamiento elevado de datos, almacenamiento continuo, manejo simultáneo de procesos y conectividad.	Moderados, se requieren realizar procesos en paralelo y en tiempo real sin incurrir en fallos y bloqueos.	Se requiere un procesamiento mínimo, solo para procesar las entradas y salidas de los sensores y actuadores.
Requerimientos de comunicación	Se requieren recursos de comunicación robustos	Se necesitan recursos de comunicación robustos.	Los recursos de comunicación son limitados

Existen varias propuestas de modelos de arquitecturas IoT por capas, entre ellas, de 3, 4, 5 y 7 capas. A continuación, se detalla la clasificación de estas arquitecturas:

- ***Arquitecturas de 3 capas.*** Entre las más importantes se mencionan cuatro de ellas, las cuales son: Survey de 3 capas, de sincronización de reloj de un sistema de acceso IoT, biométrica descentralizada, IoT bajo un esquema pregunta – respuesta [23-26].

La arquitectura Survey de 3 capas fue propuesta en los inicios de la investigación de sistemas loT, por lo que es considerada como una de las arquitecturas básicas, en la Tabla 3. se describen cada una de las capas de esta arquitectura [23].

Tabla 3. Descripción de las capas del modelo de arquitecturas de 3 capas (Survey)[23].

Arquitectura de 3 capas (Survey)	
	**Percepción.** Formada por un conjunto de objetos, el objetivo principal de esta capa es la de capturar datos del entorno mediante sensores. **Transporte.** Responsable de permitir la comunicación entre Internet y los dispositivos loT, puede ser vista como la infraestructura que da soporte. **Aplicación.** Representa una abstracción de los servicios loT, estos son solicitados por un usuario mediante un API.

Para la arquitectura de sincronización de reloj de un sistema de acceso IoT, se plantea un sistema de acceso que permite que dispositivos con recursos limitados puedan ser considerados para formar parte de un sistema loT. Esta arquitectura asegura escalabilidad gracias a su sistema de acceso, y permite solucionar el problema de sincronización de reloj de manera precisa en varios dispositivos heterogéneos. Las capas se describen en la Tabla 4 [24].

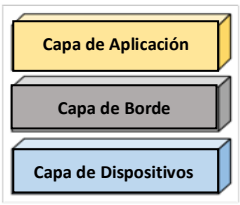
Tabla 4. Descripción de las capas del modelo de arquitecturas de sincronización de reloj de un sistema de acceso IoT [24].

Arquitectura de sincronización de reloj de un sistema de acceso IoT	
	**Distribución.** Encargada de sincronizar el reloj de todo el sistema loT, tomando como referencia el reloj del kemel. **Mantenimiento.** Encargada de mantener el reloj del kernel de cada sistema operativo para otorgar un reloj a la capa de distribución. **Adquisición.** Encargada de iniciar y sincronizar el reloj de referencia del sistema, este puede ser RTC, GPS, NTP.

Se propone una arquitectura descentralizada formada por 3 capas, la cual asegura escalabilidad y administración completa del sistema, esta es la arquitectura Biométrica Descentralizada. Puede verse como una versión mejorada de la arquitectura tradicional de 3 capas, la descripción de estas capas se detalla en la Tabla 5. Esta propuesta se

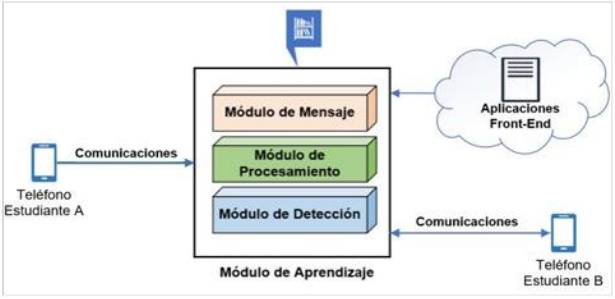
encuentra orientada a la detección de rostros, con el propósito de controlar la cantidad de personas que salen de sus hogares durante las cuarentenas provocadas por el COVID-19 [25].

Tabla 5. Descripción de las capas del modelo de arquitectura Biométrica Descentralizada [25].

Arquitectura Biométrica Descentralizada	
	**Dispositivo.** Encargada de recolectar los datos provistos por las cámaras de seguridad y dispositivos de detección. **Borde.** Capa principal de la arquitectura, encargada del procesamiento, almacenamiento v transmisión de los datos a ser manejados por la capa de Aplicación. **Aplicación.** Reside el servicio y aplicación de detección e identificación facial

Se puede observar cómo la arquitectura de 3 capas IoT Bajo un Esquema Pregunta - Respuesta es orientada para aplicaciones de ciudad inteligente, al emplear módulos con sensores embebidos que tengan la capacidad de intercambiar preguntas con diferentes usuarios que se encuentren cerca de estos módulos, creando así un sistema de aprendizaje ubicuo y accesible a una gran cantidad de personas. En la Tabla 6, se describen las tres capas de este modelo de arquitectura [26].

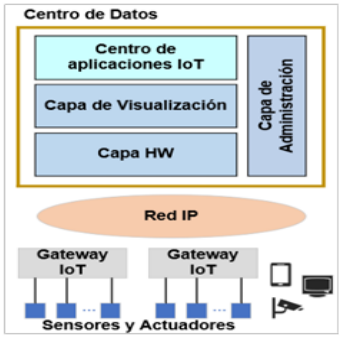
Tabla 6. Descripción de las capas del modelo de arquitectura IoT Bajo un Esquema Pregunta – Respuesta [26].

Arquitectura IoT Bajo un Esquema Pregunta - Respuesta	
	**Aplicaciones de Front-end.** contienen la aplicación, en donde personas puedan recibir y postear preguntas. **Módulo de Aprendizaje.** está compuesto de 3 partes: 1. Detección 2. Procesamiento 3. Mensaje **Comunicaciones.** permite la comunicación entre un dispositivo final (celular) y un módulo de aprendizaje.

- ***Arquitecturas de 4 capas.*** A continuación, se presentan algunas de las arquitecturas de 4 capas, las cuales son: NFV IoT para un ambiente médico, IoT basada en la teoría fractal, WBAN para sistemas IoT [27-29].

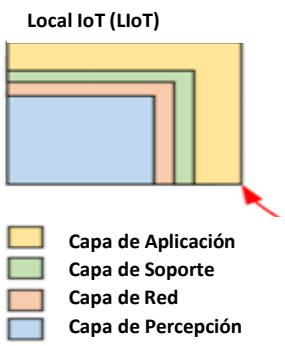
La arquitectura de 4 capas NFV IoT para un ambiente médico, emplea funciones NFV (Network Functions Virtualization) en una arquitectura tradicional para sistemas loT, gracias a dichas funciones la arquitectura asegura ser escalable, flexible y rápida. En la Tabla 7 se describe cada una de sus capas [27].

Tabla 7. Descripción de las capas del modelo de arquitectura NFV IoT para un ambiente médico [27].

Arquitectura NFV IoT para un ambiente médico	
	**Sensores y Actuadores.** dispositivos encargados de sensorizar y recolectar datos. **Gateway loT.** provee compatibilidad entre los protocolos de capa 2 y el protocolo IP manejado en la red del sistema. **Red IP.** encargada de intercambiar información entre el Centro de Datos y el Gateway IoT **Centro de Datos.** encargado de soportar las aplicaciones IoT.

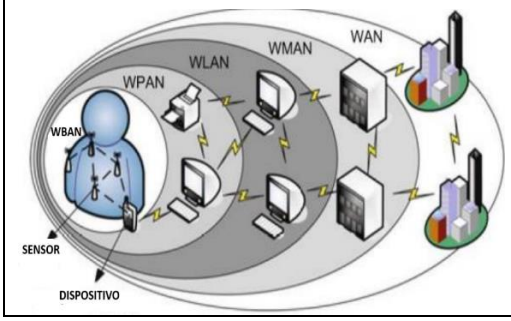
La arquitectura IoT basada en la teoría fractal considera a GloT (Global loT) y LIoT (Local loT), mencionando que GloT (Sistema loT más grande del mundo) se encuentra formada recurrentemente por LIoT (Sistema IoT de aplicación especifica). La descripción de cada una de sus capas se encuentra en la Tabla 8 [28].

Tabla 8. Descripción de las capas del modelo de arquitectura IoT basada en la teoría fractal [28].

Arquitectura IoT basada en la teoría fractal	
	**Capa de Percepción.** esta capa es la responsable de recopilar datos relevantes. **Capa de Red.** se encarga de la transmisión de los datos recolectados por la capa de percepción. **Capa de Soporte.** constituida por un middleware, se encarga de la depuración masiva de datos heterogéneos, del análisis de múltiples protocolos. **Capa de Aplicación.** en esta capa se realiza el análisis de Big Data y la Inteligencia Artificial, para obtener conocimiento de los datos.

La arquitectura WBAN para sistemas IoT emplea la tecnología WBAN (Wireless Body Area Network), la cual es una tecnología que permite interconectar diferentes sensores colocados en el cuerpo o humano o cerca de este. La Tabla 9, muestra la descripción de cada una de sus capas [29].

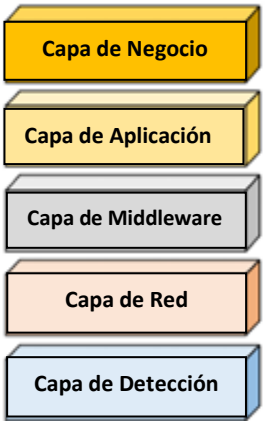
Tabla 9. Descripción de las capas del modelo de arquitectura WBAN [29].

Arquitectura WBAN para sistemas IoT	
	**Percepción.** compuesta de sensores, actuadores y controladores **Red:** define los diferentes protocolos de comunicación a ser usados en el sistema. **Nube/Middleware.** provee una infraestructura distribuida para el procesamiento y análisis de los datos. **Aplicación.** encargada de presentar la información procesada para cumplir con los servicios presentados por la aplicación.

- ***Arquitecturas de 5 capas.*** A continuación, se presenta la arquitectura de 5 capas (Survey) [30].

Debido a que la arquitectura de 3 capas presentada en la Tabla 3, no posee las suficientes funcionalidades para la implementación de un sistema loT moderno, se ha planteado una arquitectura de 5 capas las cuales se describen en la Tabla 10 [30].

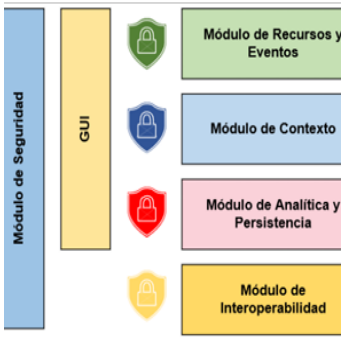
Tabla 10. Descripción de los modelos de arquitecturas Survey de 5 capas [30].

Arquitectura de 5 capas (Survey)	
	**Detección.** Esta capa es responsable de la conexión de estos dispositivos, recolección de información y el intercambio de ésta con la capa superior. **Red.** se encarga de la transmisión de la información. **Middleware.** debido a la gran cantidad de dispositivos heterogéneos usados en los sistemas loT **Aplicación.** representa una abstracción de los servicios loT, estos son solicitados por un usuario mediante un API. **Negocio.** permite realizar análisis de datos, gráficos, modelos de negocio que ayuden a los desarrolladores o stakeholders de los sistemas loT en la toma de decisiones.

- ***Arquitecturas de 7 capas.*** Se pueden mencionar la arquitectura IoT Middleware, de 7 capas, y la de 7 capas de la ITU-T Y.4000 [31-32].

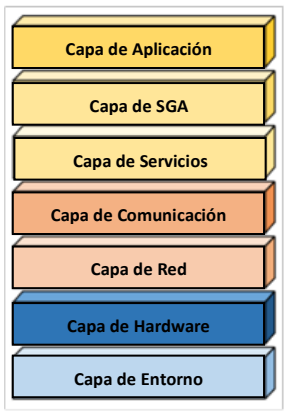
La Arquitectura IoT Middleware puede acoplarse a sistemas IoT, asegurando escalabilidad e Interoperabilidad. Esta consta de 7 capas las cuales se describen en la Tabla 11 [32].

Tabla 11. Descripción del modelo de arquitectura IoT Middleware [32].

Arquitectura IoT Middleware	
	**Módulo de Interoperabilidad.** permite integrar diversos dispositivos heterogéneos mediante un API. **Módulo de Analítica y Persistencia.** proporciona un procesamiento básico de los datos recolectados, al igual que un almacenamiento limitado. **Módulo de Contexto.** el contexto de un sistema loT puede entenderse como la capacidad de proveer información relevante acorde a la tarea demandada por un usuario. **Módulo de Recursos y Eventos.** administra y optimiza las interacciones entre dispositivos IoT. **Interfaz Gráfica de Usuario (GUI).** visto como un dominio transversal, permite al middleware **Red IP.** encargada de intercambiar información entre el Centro de Datos y el Gateway IoT **Módulo de Seguridad.** es un dominio transversal aplicado en todos los módulos del middleware.

Se propone una arquitectura de 7 capas que considera las dificultades existentes en los dispositivos encargados de la recolección de datos al estar expuestos a un entorno dinámico. En la Tabla 12, se describe cada una de estas 7 capas [31].

Tabla 12. Descripción del modelo de arquitectura 7 capas [31].

Arquitectura de 7 capas	
	**Capa de Entorno.** permite realizar la detección de objetos, personas o diferentes parámetros del entorno en el cual se encuentran colocados los dispositivos loT **Capa de Hardware**. encargada de integrar todos los componentes de hardware necesarios para la implementación de un sistema IoT. **Capa de Red.** permite la transmisión y procesamiento de la información por medio del Internet. **Capa de Comunicación.** actúa como un puente de información, encargado de comunicar la capa donde se recolectan datos **Capa de Servicios.** proporciona ayuda en la ejecución de las actividades requeridas por el cliente. **Capa de Soporte y Gestión de Aplicación (SGA):** otorga un control gerencial completo y seguridad en todo el sistema loT. **Capa de Aplicación.** recolecta información sobre las tareas a ser realizadas en base a los requisitos del cliente.

Esta arquitectura está estandarizada por la UIT-T, proporciona una estructura robusta y bien definida para implementaciones de IoT en el hogar, garantizando la interoperabilidad y la seguridad a través de capas bien definidas. En la Tabla 13, se describe cada una de las capas [33].

Tabla 13. Descripción del modelo de arquitectura 7 capas de la ITU-T Y.4000 [33].

Arquitectura de 7 capas de la ITU-T Y.4000	
	**Capa fisica.** Esta capa se encarga de la transmisión de bits a través de un medio de comunicación físico. **Capa de enlace de datos.** Aquí se establece la comunicación punto a punto entre dispositivos. **Capa de red.** Es responsable del enrutamiento de datos a través de la red. **Capa de transporte.** Proporciona servicios de transporte confiable y eficiente **Capa de sesión.** Establece, administra y termina sesiones entre aplicaciones en dispositivos finales. **Capa de presentación.** Se ocupa de la representación y la conversión de datos para garantizar la interoperabilidad**.** **Capa de aplicación.** Es la capa más alta del modelo y proporciona servicios de red.

c. Componentes

En términos sencillos, una arquitectura IoT contiene los siguientes componentes [22]:

- ***Arreglo de sensores.*** para recoger datos y actuadores para realizar comandos recibidos desde la nube.

- ***Gateways.*** para filtrar, preprocesar y mover datos a la nube y viceversa, recibir comandos desde la nube.

- ***Cloud Gateways.*** para garantizar la transición de datos entre las pasarelas sobre el terreno y los servidores centrales de IoT.

- ***Procesadores de datos.*** en tiempo real para distribuir los datos procedentes de los sensores entre los componentes de las soluciones de IoT pertinentes.

- ***Bases de Datos.*** para almacenar todos los datos de valor definido e indefinido.

- ***Big Data Warehouse.*** para la recogida de datos valiosos.

- ***Aplicaciones de control.*** para enviar comandos a los actuadores.

- ***Machine Learning.*** para generar los modelos que luego son utilizados por las aplicaciones de control.

- ***Aplicaciones de usuario.*** que permiten a los usuarios monitorizar el control de sus cosas conectadas.

- ***Análisis de datos.*** para el procesamiento manual de datos

d. Conexión a la nube de dispositivos IoT

El mayor fabricante de dispositivos IoT es Tuya, los dispositivos Tuya están diseñados para comunicarse con TuyaCloud, pero la mayoría también expone una API de red de área local. La Figura 2, muestra que los dispositivos se conectan hacia la nube de Tuya por medio del puerto 6668/TCP [34].

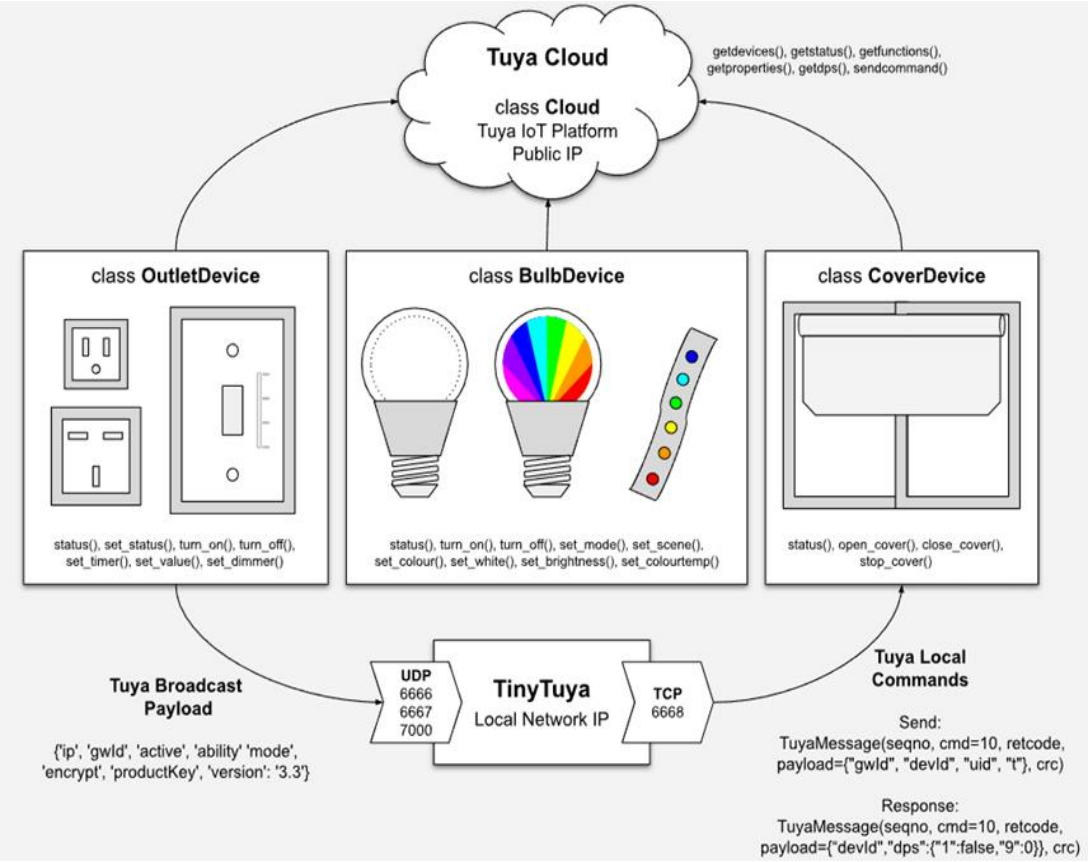


Figura 2. Arquitectura de funcionamiento de Tuya [34].

1.3.3 Riesgos cibernéticos

Existen múltiples puntos de vista con los que se puede abordar el estudio de la seguridad en los entornos informáticos, así como una gran variedad de intereses, elementos afectados y tipos de medidas a adoptar. En general se adopta el punto de vista del usuario final, que es el que resulta más afectado por cualquier fallo en la seguridad del sistema [35].

a. Fases del estudio de seguridad

Para abarcar todos los aspectos de la seguridad, hay que tomar en cuenta las fases, a más de las actitudes que se puede optar frente al problema de la Seguridad Informática que se muestran en la Tabla 14 [35]:

Tabla 14. Fases de estudio de seguridad y opciones a adoptar [35].

Fases del estudio de seguridad	La identificación de las amenazas que puedan afectar al sistema; en especial las de mayor riesgo e impacto.
	Las defensas o medidas de prevención a implantar para dificultar o evitar los incidentes de seguridad.
	Los medios de detección de indicios de situaciones no deseadas.
	Los recursos de recuperación y acciones de contingencia necesarias para reducir los trastornos y/o repercusiones económicas de los incidentes de seguridad.
Opciones para adoptar frente a un problema de seguridad informática	Aceptar el riesgo, bien por su baja probabilidad de ocurrencia, bien por su bajo impacto
	Transferir el riesgo, mediante la contratación del correspondiente seguro, aunque pueden existir pérdidas irreparables como la del recurso información.
	Evitar el riesgo, mediante la elaboración y puesta en marcha de un Plan de Seguridad Informática que contengan medidas preventivas y de recuperación.

b. Riesgos a los sistemas lógicos

Este tipo de riesgo suele ser uno de los más peligrosos y difíciles de detectar, ya que al alterar el funcionamiento normal del sistema y no detectarse a tiempo puede provocar daños irreparables a la información, a los usuarios e incluso al sistema físico, entre ellos están [18]:

- Ciberplagas
- Copias ilegales
- Denegación de servicios

c. Riesgos a la información

La información es el elemento más sensible de todo el sistema informático, porque es susceptible a accesos no autorizados, a modificación de la información, resultando una gran amenaza, entre ellos están [35]:

- Captura de emisiones electromagnéticas.
- Interceptación de líneas de datos.
- Acceso no autorizado a las bases de datos.

d. Riesgos a las personas

Los riesgos a las personas en el contexto de los sistemas IoT domésticos son amenazas que pueden comprometer la privacidad, seguridad y bienestar de los individuos, entre ellos están [35]:

- Hackers y cracker.
- Ciberterrorismo.
- Pornografía y pornografía infantil.
- Apologías de grupos violentos o partidos ilegales.
- Perdidas de la intimidad.
- Fraude electrónico.

e. Riesgos cibernéticos en un sistema IoT

La IoT no abarca solo las computadoras o los teléfonos inteligentes, sino casi cualquier dispositivo que tenga un interruptor de encendido y apagado y que pueda

potencialmente conectarse a Internet, para formar parte del Internet de las cosas. El enorme volumen y la gran diversidad de "cosas" que componen la IoT implican que allí se albergue una cantidad considerable de datos de usuario, que están propensos a ser robados o pirateados por cibercriminales. Mientras más dispositivos conectados existan, más oportunidades tienen los cibercriminales de poner en riesgo la seguridad de los datos. En la Tabla 15, se observan los riesgos y los principales problemas de seguridad de IoT [36]:

Tabla 15. Principales riesgos y problemas de seguridad en IoT [36].

Riesgo/Problemas	Descripción
Falta de pruebas y desarrollo	Algunos fabricantes de IoT han dejado de lado la seguridad en su prisa por lanzar sus productos al mercado.
Contraseñas por defecto que propician los ataques de fuerza bruta	Muchos dispositivos de IoT vienen con contraseñas por defecto que no suelen ser seguras.
Malware y ransomware de IoT	El malware botnet de IoT ha estado entre las variantes más comunes.
Inquietudes sobre la privacidad de los datos	Los dispositivos de IoT recopilan, transmiten, almacenan y procesan una enorme cantidad de datos de usuarios.
Aumento de ciberataques	Los dispositivos de IoT infectados pueden utilizarse para realizar ataques de denegación de servicio distribuido (DoS, por sus siglas en inglés).
Interfaces no seguras	Entre los problemas comunes de interfaz es el cifrado frágil o nulo o la autenticación de datos insuficiente.
Entornos complejos	Un estudio revela que, en 2020, un hogar promedio en Estados Unidos menciona que basta con pasar por alto una mala configuración de seguridad en un solo dispositivo para poner en peligro toda la red doméstica.

1.3.4 Honeynet

Las honeynet son redes de honeypot que son capaces de emular una infraestructura completa para dotar de más realismo y realizar una recogida de información lo más completa posible, la Figura 3, muestra un esquema de honeynet [37].

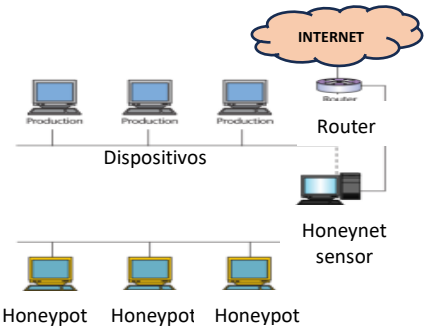


Figura 3 Esquema Honeynet [37].

a. Honeypot

Una honeypot es un sistema trampa creado con la intención de atraer a los atacantes y así evitar ataques contra infraestructuras o sistemas. Además, se utilizan para recoger información sobre cualquier actividad maliciosa. Esta información puede ir desde hora y fecha del ataque, dirección IP o sistema operativo del atacante, hasta diccionarios utilizados para fuerza bruta. También se pueden extraer exploits, que son piezas de código que se aprovechan de vulnerabilidades para provocar un comportamiento no deseado. Las honeypots se pueden clasificar en base a los siguientes aspectos: nivel de interacción, tipo de honeypot e implementación de la honeypot. La clasificación por nivel de interacción con el usuario tiene tres posibles diferenciaciones [37]:

- ***Baja interacción***. Son aquellas en las que la honeypot tiene poca interacción con el usuario. Básicamente trata de ofrecer servicios emulados como SSH, FTP, Telnet, HTTP, etc. Los atacantes lanzan sus ataques contra estos servicios y la honeypot recoge toda la información posible de sus acciones [37].

- ***Media interacción.*** Las honeypot de interacción media tienen un comportamiento limitado de cara al atacante. Sin embargo, en éstas se da más funcionalidad a los servicios para que los atacantes encuentren un entorno más realista [37].

- ***Alta interacción.*** Son las más complicadas de diseñar e implementar. Su nivel de sofisticación es alto, ya que todo lo que hay en ella es simulado y permite interacción plena por parte del atacante. Son excelentes para recoger mucha información e información completa. Como desventaja, estas honeypots aportan riesgos a la infraestructura real si no se controlan [37].

Cada tipo de Honeynet tiene sus propias ventajas y limitaciones en términos de detección de riesgos en sistemas IoT. La selección del tipo adecuado dependerá de los recursos disponibles, el nivel de interacción deseado con los atacantes y los objetivos específicos de seguridad de la red IoT en cuestión. La Tabla 16, proporciona una visión general de las ventajas y limitaciones de cada tipo de Honeynet en relación con la detección de riesgos en sistemas IoT [38].

Tabla 16. Ventajas y limitaciones de Honeynets [38].

Tipo de Honeynet	Ventajas	Limitaciones
Honeynets de alta-interacción	- Ofrecen interacción profunda con los atacantes, recopilando información detallada. - Útiles para comprender tácticas de ataques dirigidos a dispositivos IoT.	-Requieren mantenimiento y recursos significativos. - Difíciles de escalar para redes IoT domésticas.
Honeynets de bajo-interacción	- Fáciles de implementar y mantener. - Útiles para detectar amenazas genéricas en sistemas IoT.	- Pueden no capturar tanta información sobre atacantes como las Honeynets de alto-interacción.
Honeynets basadas en sensores	- Menos intrusivas, centradas en la monitorización de tráfico y actividad en red. - Integración sencilla en entornos IoT existentes.	- Detección basada en patrones de comportamiento, lo que puede generar falsos positivos. - Pueden no detectar amenazas más avanzadas que no se ajusten a patrones conocidos.
Honeynets de simulación de firmware	- Detectan ataques dirigidos al firmware de dispositivos IoT. - Críticas para la seguridad de dispositivos IoT que ejecutan firmware propietario.	- Requieren conocimiento profundo de la arquitectura y funcionamiento de dispositivos específicos. - Difíciles de implementar y mantener debido a la complejidad y variabilidad de los firmwares.

Además de los niveles de interacción, existen dos tipos de honeypot clasificadas según el tipo de uso [37]:

- ***Honeypot virtual.*** Como su propio nombre indica, es una honeypot virtualizada mediante software de virtualización y alojada dentro de un host físico. Esta honeypot está perfectamente integrada dentro de la propia red de la infraestructura contando con su propia configuración de red. Estas honeypot son sencillas de implementar y más económicas que las físicas [37].

- ***Honeypot física.*** A diferencia de la honeypot virtual, esta honeypot cuenta con un equipo específico para su cometido y al igual que la virtual, se encuentra perfectamente integrada dentro de la red. La ventaja que aporta esta honeypot es que es lo más realista posible, sin embargo, el coste de mantenimiento es más elevado que una honeypot virtual [37].

- ***Honeypot de investigación.*** Utilizadas por instituciones educativas y de investigación. La información recogida de los ataques viene motivada ante la posibilidad de descubrir nuevos ataques o las motivaciones que llevan al atacante a cometer estos actos [37].

b. Honeypots en IoT

Los Honeypot de baja interacción, interacción hibrida-media cumplen con las características que permiten trabajar en el mundo del IoT, entre ellos se tiene [39]:

- ***Dionaea.*** Presentado al mundo por primera vez en 2009 como una evolución de Nepenhes. Dionaea es un honeypot de baja interacción que originalmente estaba orientado a capturar el comportamiento del malware al interactuar con los servicios de red de los sistemas Windows. Pero su funcionalidad fue extendida hasta llegar a cubrir otros servicios orientados a bases de datos o servidores web, entre los cuales destacan MySQL y MSSQL. En cuanto a conectividad web, se puede simular el protocolo HTTP, HTTPS o FTP en otro tipo de servicios [39].

- ***Honeyd.*** Debido a su capacidad de simular fingerprints es sencillo adaptarlo para que simule cualquier servicio si se implementa en el puerto correspondiente, puede utilizarse para simular dispositivos IoT expuestos. Una de las capacidades más destacables de esta herramienta es la de simular rutas de red, pudiendo crear así topologías de red complejas e incluso simular routers. Esta característica permite implementar incluso latencias en la red o perdidas de paquetes, generando al atacante la experiencia de que se encuentra ante un entorno real, en la Figura 4 se observa la arquitectura básica de Honeyd [39].

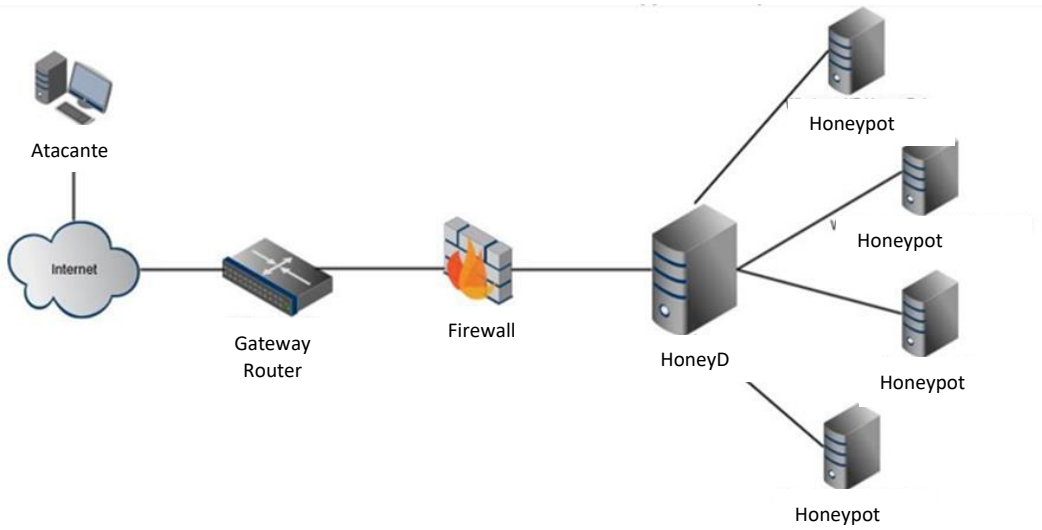


Figura 4. Arquitectura de Honeyd [39].

- ***ConPot.*** Es una herramienta de código abierto diseñada como un honeypot de alto interacción para sistemas de control industrial (ICS). Su propósito es emular servicios y dispositivos típicos de infraestructuras críticas, atrayendo y registrando las actividades de los atacantes para el análisis de amenazas y la mejora de la ciberseguridad en entornos industriales [40].

- ***Telnet IoT HoneyPot.*** Uno de los últimos desarrollos honeypot liberado en 2016 fue "Telnet IoT Honeypot", diseñado especialmente para capturar binarios en este ámbito tras el ataque de Mirai y la posterior publicación de su código fuente. Como implementación de interacción baja, este honeypot no implementa el entorno y comportamiento completo de un sistema Linux, sino que se limita a recoger estadísticas de los patrones de ataque. Para ello basta con registrar los dominios a los que, tras logearse exitosamente, tratan de alcanzar los atacantes [39].

- ***IoTPot.*** En la Figura 5, se analiza una honeypot de características híbridas llamada IoTPOT centrada en ataques contra el servicio Telnet. El incremento disparado de ataques llevados a cabo contra dispositivos IoT durante el año 2014 sirve de motivación para este sistema. Se estudia una honeypot un tanto sofisticada motivada por la heterogeneidad de los dispositivos IoT. En concreto, se describe la forma de buscar una honeypot de interacción inteligente de tal forma que sea capaz de aprender el funcionamiento de varios tipos de dispositivos mediante técnicas de aprendizaje máquina [41].

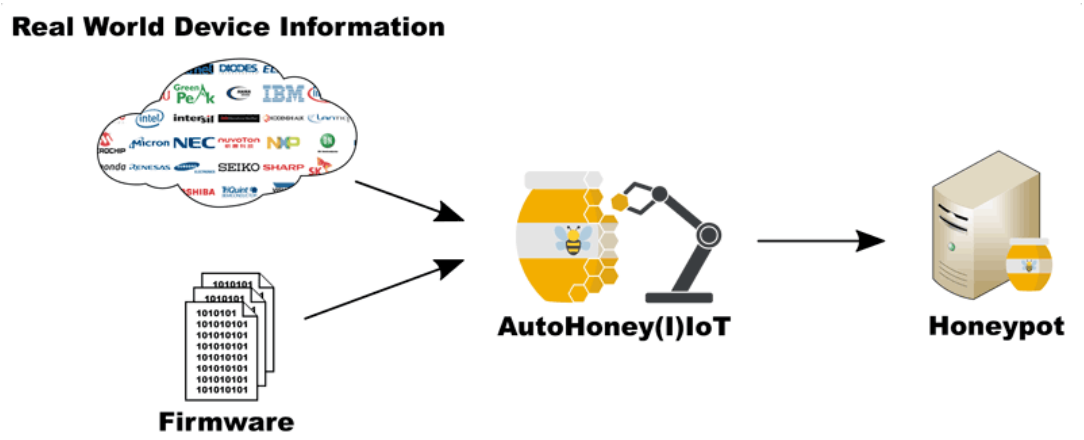


Figura 5. Honeypots en IoT [41].

- ***Kippo.*** Kippo fue inicialmente presentado al mundo en 2009 como un sistema de interacción media para detectar ataques SSH de fuerza bruta fuera del mundo IoT, pero debido a su versatilidad y a que es una herramienta de código libre fue adaptado rápidamente para cubrir nuevas necesidades. Actualmente, permite capturar las interacciones que el atacante tiene con el sistema, pero deben tenerse en cuenta que estas interacciones están limitadas a una serie de instrucciones y sistema de ficheros falso [39].

- ***CitrixHoneypot.*** Es un honeypot especializado diseñado para emular servicios y dispositivos específicos de Citrix, con el fin de atraer y registrar actividades de posibles atacantes. Esta herramienta es utilizada en entornos de investigación de seguridad cibernética para estudiar tácticas de intrusión dirigidas a sistemas Citrix y mejorar las estrategias de defensa contra amenazas en redes [40].

- ***Cowrie.*** Es la nueva versión del Honeypot Kippo, en la Figura 6, se observa cómo trabaja Cowrie, esta es un fork del código desde el punto de vista de los programadores. Se ha actualizado con nuevas características y proporciona una emulación que registra la sesión de un atacante. Con esta grabación de la sesión, se puede comprender mejor las herramientas, tácticas y procedimientos (TTPs) de los atacantes [39].

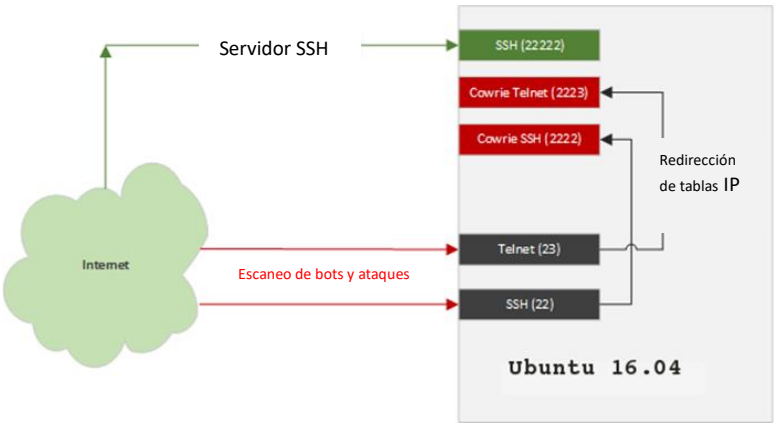


Figura 6. Arquitectura de Cowrie [39].

Este honeypot permite emular los servicios de los dos anteriores, Telnet y SSH, permite registrar todos los movimientos de cada sesión de manera individual almacenándolos en una base de datos y, además proporciona un nivel de interacción con el sistema operativo bastante completo [39].

Recientemente, ha surgido un nuevo interés en esta área, donde algunos proyectos se han inspirado en trabajos anteriores para su desarrollo, mientras que otros han observado de cerca las tendencias de los ataques a IoT y se han enfocado en problemáticas específicas. Entre estos últimos se destaca HoneyThing, el cual se centra en la vulnerabilidad del protocolo TR-064, que afecta a ciertos modelos de routers. Algunas variantes de la botnet Mirai han explotado implementaciones vulnerables de este protocolo, eliminando y simplificando las tareas de mantenimiento [42].

Además, es importante mencionar la presencia de proyectos más enfocados en simular dispositivos IoT completos, como cámaras, incorporando funciones como movimientos, rotaciones y zoom. Ejemplos notables de tales implementaciones son Wificam y Honeypot Camera. Otros proyectos se centran en ataques o vulnerabilidades específicas, como MTPot, desarrollado especialmente para abordar las amenazas de Mirai [38-40].

1.4 Objetivos

1.4.1 Objetivo general

Implementar una Honeynet para análisis, evaluación y tratamiento de riesgos cibernéticos en un sistema IoT.

1.4.2 Objetivos específicos

- Analizar los tipos de Honeynet y las arquitecturas de los sistemas IoT que mejor se adaptan a los sistemas de detección de riesgos cibernéticos.
- Desarrollar una Honeynet para identificar los riesgos, vulnerabilidades y amenazas existentes en el sistema IoT.
- Elaborar una propuesta de plan de Tratamiento de riesgos cibernéticos para garantizar la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas en el sistema IoT.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para la investigación, se seleccionaron dispositivos IoT típicos de hogares inteligentes como luces, interruptores, enchufes, cámaras de seguridad, asistentes de voz y sensores de movimiento. Los dispositivos fueron evaluados para determinar su resistencia ante riesgos potenciales mediante pruebas de penetración utilizando Nessus Essentials para el análisis de vulnerabilidades. Además, se implementó una honeynet con TPOT y un honeypot desarrollado en Python para simular ataques DoS por inundación de paquetes SYN, permitiendo la detección y monitorización de actividades maliciosas. La honeynet proporcionó datos sobre las tácticas de posibles atacantes, evaluando las amenazas a la seguridad del sistema IoT.

La virtualización se realizó con VMware Workstation para crear entornos controlados en una única estación de trabajo. Las pruebas de penetración y evaluaciones de vulnerabilidad se llevaron a cabo con Kali Linux, que incluye herramientas especializadas como Wireshark, Hercules, Zenmap y Jupyter. Además, se empleó un adaptador USB 802.11 TP-Link AC600 T2U Nano para habilitar la conectividad inalámbrica en el entorno de pruebas con Kali Linux y evaluar la seguridad de los dispositivos IoT, proporcionando un marco robusto para realizar un análisis exhaustivo de la seguridad en entornos de IoT domésticos.

2.2 Métodos

2.2.1 Modalidad de la investigación

El presente proyecto es una investigación aplicada, ya que aprovecha los conocimientos previamente adquiridos durante el transcurso académico para abordar de manera concreta y efectiva los desafíos específicos asociados con la seguridad en entornos de Internet de las cosas, además se utilizó una Honeynet como herramienta de análisis y evaluación que permite simular ambientes cibernéticos reales, identificando vulnerabilidades y amenazas potenciales en el sistema IoT. Asimismo,

la aplicación de estas técnicas orientó a desarrollar estrategias de tratamiento de riesgos adaptadas a la dinámica y complejidad de los entornos IoT, contribuyó así a la mejora de la seguridad y a la mitigación de posibles amenazas en este contexto tecnológico en constante evolución.

La investigación fue bibliográfica, debido a que se respaldó en la recopilación de datos provenientes de diversas fuentes confiables, como revistas técnicas, libros, artículos científicos, publicaciones en línea y tesis. Se focalizó en temas vinculados a sistemas IoT, honeynets y análisis, evaluación y tratamiento de riesgos cibernéticos. La revisión bibliográfica permitió obtener una comprensión profunda de las teorías, prácticas y enfoques previamente propuestos por expertos en el campo, sirviendo como base para la formulación de estrategias efectivas en la gestión de riesgos cibernéticos específicamente adaptadas a entornos IoT.

Es una investigación experimental, dada la necesidad se implementó y evaluó la eficacia del sistema Honeynet para el análisis, evaluación y tratamiento de riesgos cibernéticos en un entorno de Sistema de Internet de las Cosas. La elección de un enfoque experimental se sustentó en la naturaleza dinámica y en la constante evolución de las amenazas cibernéticas que afectaron a los dispositivos IoT, así como en la falta de soluciones para abordar estas vulnerabilidades.

2.2.2 Recolección de información

Con el propósito de lograr la recolección de información, se utilizó libros, revistas, recursos en línea y proyectos desarrollados, así como también manuales de construcción y guías prácticas. En el proceso, se consideraron bases de datos fidedignas que faciliten el avance del proyecto.

Tabla 17. Recolección de información

Criterio	**Descripción**
¿Para qué?	Para analizar evaluar y tratar los riesgos cibernéticos.
¿De qué personas u objetos?	De Sistemas IoT.
¿Cómo?	Por medio de una Honeynet.
¿Con qué?	Con herramientas que permitieron la creación de una honeynet para analizar evaluar y tratar los riesgos cibernéticos en un sistema IoT.
¿Cuándo?	Durante el período académico marzo 2024 a agosto 2024.
¿Dónde?	En la ciudad de Ambato.

2.2.3 Procesamiento y análisis de datos

Para el procesamiento y análisis de datos se procederá de la siguiente manera:

- Revisión de la información recopilada.
- Análisis de los registros generados por Honeynet.
- Estudio de las propuestas de solución planteadas para mitigar riesgos existentes.
- Documentación de todos los procesos, hallazgos y propuestas elaboradas.
- Planteamiento de la propuesta de solución.
- Interpretación de la información relevante que contribuya al desarrollo del proyecto de investigación que lleve a la solución de la propuesta.
- Validación del plan y tratamiento de los riesgos existentes.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Seguridad en sistemas IoT para el hogar

Los dispositivos interconectados en el hogar que forman parte de los sistemas IoT, como las cámaras de seguridad, los sistemas de iluminación automatizados o los altavoces inteligentes, brindan comodidad y eficiencia a los usuarios. Sin embargo, esta interconexión de dispositivos genera preocupaciones en materia de seguridad. Los sistemas IoT para el hogar están diseñados con un enfoque en la facilidad de uso y la accesibilidad, lo que los hace vulnerables a una serie de amenazas cibernéticas, desde ataques de denegación de servicio hasta intrusiones en la privacidad de los usuarios. A juzgar por el número cada vez mayor de ataques y la persistencia de los delincuentes, se puede afirmar que IoT es un área fructífera para los atacantes que utilizan incluso los métodos más primitivos, como adivinar combinaciones de contraseñas y nombres de usuario, ya que las combinaciones más comunes suelen ser "support/support", seguidas de "admin/admin" y "default/default" [46].

Una honeynet está compuesta por varios honeypots, los cuales son una buena forma de exponer las vulnerabilidades de los sistemas. Es decir, un honeypot muestra el alto nivel de amenazas que suponen los ataques a los dispositivos de IoT. Los honeypots son una opción eficiente debido a su bajo consumo de recursos y su baja tasa de falsos positivos, lo que los diferencian de los sistemas tradicionales de detección de intrusos, permitiendo priorizar los esfuerzos y mantener un bajo consumo de recursos en los honeypots [47].

El objetivo principal de implementar una honeynet es adquirir la mayor cantidad de información posible sobre los ataques para su posterior análisis. Para su desarrollo se utiliza máquinas virtuales que incluyen honeypots que pueden publicar distintos servicios, incluyendo aquellos utilizados por dispositivos IoT para el hogar, después de un análisis de estos dispositivos se descubre los servicios con los que trabajan los mismos, lo que contribuye en el desarrollo de la honeynet y un plan de tratamiento de riesgos adecuado para un entorno doméstico.

3.2 Esquema General del Sistema

La Figura 7, presenta el esquema general por etapas, relacionando cada uno de los componentes del sistema. La honeynet está ubicada en el interior de la red doméstica y utiliza un módem de fibra óptica con servicios de internet.



Figura 7. Esquema general del Sistema

Etapa 1. La primera etapa del Sistema IoT, se refiere a la interconexión de dispositivos inteligentes dentro del hogar. Esta integración abarca una amplia gama de elementos que trabajan en conjunto para brindar comodidad y eficiencia al usuario. Se incluyen dispositivos como bombillas, sensores y enchufes inteligentes, sistemas de seguridad con cámaras de vigilancia y altavoces inteligentes como "Alexa". Además de estos dispositivos, la red Wi-Fi con conexión a Internet es esencial para la comunicación y el control remoto desde dispositivos móviles o a través de comandos de voz.

Etapa 2. En esta etapa, se comprende el contexto de la implementación del sistema IoT en un entorno doméstico y se definen los elementos claves para proteger la seguridad de los dispositivos IoT, la privacidad de las personas y la seguridad de los datos. Entorno a estos elementos claves, se establecen diversas actividades que deben ejecutarse para garantizar la confidencialidad, integridad y disponibilidad de los dispositivos IoT y de la información.

Etapa 3. En esta etapa, se define una metodología que permite abarcar los elementos clave identificados en la Etapa 2. Para ello, se identifican claramente las vulnerabilidades críticas en base a la ubicación de los dispositivos IoT y la importancia de sus acciones y manipulaciones dentro del entorno doméstico. Además, se implementó una honeynet que permite identificar los tipos de ataques dentro de la red, utilizándose esta herramienta en la fase de análisis de vulnerabilidades. Se establece una metodología clara para gestionar los riesgos de los elementos críticos del sistema IoT. Esta metodología incluye la realización de diversas pruebas y análisis para determinar los vectores de ataque. Al final del proceso, se entrega una documentación detallada que explica el tratamiento de estos riesgos y proporciona recomendaciones sobre cómo deben ser gestionados y mitigados.

3.3 Categorías de conexiones de redes en sistemas IoT

Existen tres formas diferentes en las que los dispositivos IoT se conectan y procesan los datos para entregar la información al usuario final. Estas conexiones dependen de la respuesta de las funciones, tomando en cuenta la latencia. Algunas actividades y procesos que deben entregarse en tiempos muy reducidos, como por ejemplo, el manejo autónomo de un vehículo, controlados desde servidores descentralizado cercano al equipo IoT que interactúa con ellos. Otro ejemplo es una planta de tratamiento, donde se monitorean diferentes niveles para tomar una acción en base a estos datos [48].

Por otro lado, existen casos en los que no es necesario que la información se entregue de forma inmediata y pueden tener latencias más altas o tiempos de respuesta más lentos sin que se vea afectada la operación [48].

La Tabla 18, muestra las ventajas y desafíos de cada una de las tres categorías de conexiones, junto con sus respectivas descripciones. Esta tabla facilita el análisis de las ventajas y desafíos de las diferentes arquitecturas de conexiones de redes en sistemas IoT, para identificar que categoría utilizan los dispositivos IoT para entornos domésticos, considerando factores como la necesidad de análisis centralizado, la rapidez de respuesta a amenazas y la complejidad de implementación y mantenimiento.

Tabla 18. Ventajas y Desafíos de las categorías de los sistemas IoT [48].

Arquitectura	Descripción	Ventajas	Desafíos
Centralizada	Implica que todos los datos de los dispositivos IoT se recopilan y procesan en un punto central, como un servidor o una nube.	- Permite un análisis centralizado que identifica patrones de actividad sospechosa en toda la red. - Facilita la implementación de algoritmos de detección de anomalías y análisis de comportamiento a gran escala.	- Tiene una dependencia significativa de la conectividad de red hacia el punto central. - Existe un riesgo de cuellos de botella o puntos únicos de fallo.
Distribuida	Implica que la detección de riesgos cibernéticos se realiza de manera distribuida en varios nodos dentro de la red IoT.	- Permite una respuesta rápida a amenazas, ya que cada dispositivo puede detectar y responder localmente. - Reduce la latencia al procesar los datos de forma local.	- Se agrega complejidad en el desarrollo y mantenimiento de algoritmos de detección en múltiples nodos, y se requiere coordinación y sincronización entre ellos.
Híbrida	Combina elementos de las arquitecturas centralizadas y distribuidas para optimizar la detección de riesgos cibernéticos.	- Permite aprovechar los beneficios del análisis centralizado y distribuido. - Posibilita la implementación de políticas de seguridad tanto a nivel local como central.	- Requiere un diseño cuidadoso para determinar qué tareas se llevan a cabo localmente y cuáles de forma centralizada. - Mayor complejidad en la gestión y configuración.

Después de analizar las ventajas y desafíos de las diferentes categorías de conexiones de redes en sistemas IoT, se ha identificado que los dispositivos IoT para entornos domésticos utilizan una arquitectura centralizada.

3.4 Infraestructura IoT para el hogar

En cuanto a la infraestructura necesaria para la red, se utiliza el modelo de la ITU-T Y.4113, ya que presenta un modelo básico para IoT compuesto por tres partes: la red central, la red de acceso y la red de área de IoT. La infraestructura de la red de área de IoT incluye dispositivos y puertas de enlace que se conectan entre sí para facilitar la comunicación en el entorno del IoT. Esta conectividad se establece mediante enlaces locales, generalmente empleando tecnologías de comunicación de corto alcance [21].

Como se muestra en la Figura 8, el gateway es una unidad con respecto al IoT que interconecta los dispositivos con la red central, realiza la traducción necesaria entre los protocolos utilizados en la red central y los utilizados por los dispositivos. Por otro lado, la red central es una parte del sistema de prestación compuesta por redes, equipos e infraestructuras, y conecta el dominio del proveedor de servicios con la red de acceso.

Finalmente, la red de acceso conecta los dispositivos para IoT y las puertas de enlace a la red central, se puede implementar utilizando diferentes tecnologías como fibra óptica y tecnologías de acceso por radio red de acceso y red de área de IoT [21].

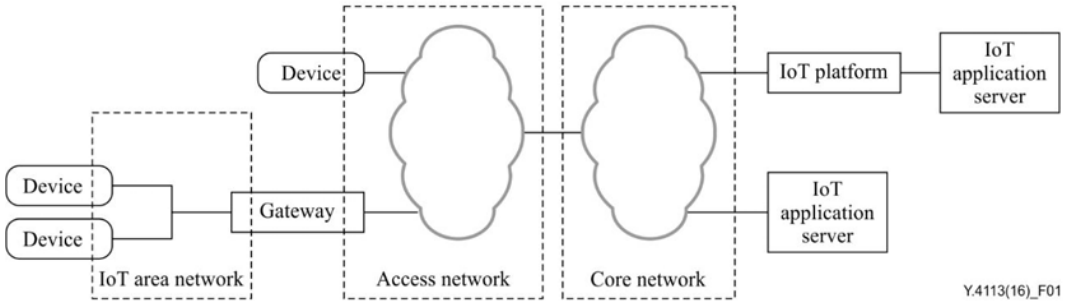


Figura 8. Modelo básico de la red para IoT [21].

3.5 Modelos de arquitectura por capas en IoT para el hogar

Existen varias propuestas de arquitecturas IoT por capas que permiten una tecnología segura y dinámica, se muestra las arquitecturas en base al número de capas 3,4,5 y 6 capas o más [49].

La Tabla 19, muestra el análisis de las arquitecturas de 3 capas: Arquitectura de 3 capas (Survey), Arquitectura de sincronización de reloj de un sistema de acceso IoT, Arquitectura biométrica descentralizada de 3 capas, Arquitectura IoT bajo un esquema pregunta-respuesta.

Tabla 19. Análisis de las arquitecturas de 3 capas en IoT [49].

MODELOS PROPUESTOS	**CAPAS**	**Análisis**
Arquitectura de 3 capas (Survey)	Percepción Transporte Aplicación	Ofrece una separación clara de las funciones principales, lo que facilita la implementación y el mantenimiento.
Arquitectura de sincronización de reloj de un sistema de acceso IoT	Adquisición Mantenimiento Distribución	Garantiza la coherencia temporal en la toma de decisiones y la ejecución de acciones.
Arquitectura biométrica descentralizada de 3 capas	Dispositivo Borde Aplicación	Esta arquitectura se enfoca en la seguridad biométrica, lo que la hace ideal para sistemas de acceso y autenticación
Arquitectura IoT bajo un esquema pregunta-respuesta	Aplicaciones de Front-end Módulo de Aprendizaje Comunicaciones	Es adecuada para aplicaciones donde la interacción intuitiva es importante.

La Tabla 20, muestra el análisis de las arquitecturas de 4 capas: Arquitectura NFV IoT para un ambiente médico, Arquitectura IoT basada en la teoría fractal, Arquitectura WBAN para sistemas IoT.

Tabla 20. Análisis de las arquitecturas de 4 capas en IoT [49].

MODELOS PROPUESTOS	**CAPAS**	**Análisis**
Arquitectura NFV IoT para un ambiente médico	Sensores y actuadores Gateway IoT Red IP Centro de datos	Esta arquitectura está diseñada para entornos médicos donde la seguridad y la confiabilidad son fundamentales.
Arquitectura IoT basada en la teoría fractal	Capa de percepción Capa de red Capa de soporte Capa de aplicación	Es ideal para aplicaciones donde se requiere una alta tolerancia a fallos y adaptabilidad a entornos cambiantes.
Arquitectura WBAN para sistemas IoT	Percepción Red Nube/Middleware Aplicación	Esta arquitectura está optimizada para aplicaciones de monitoreo de salud y bienestar

La Tabla 21, muestra el análisis de las arquitecturas de 6 capas o más: Arquitectura IoT Middleware, Arquitectura de 7 capas, Arquitectura de 7 capas de la ITU-T Y.4000

Tabla 21. Análisis de las arquitecturas de 6 capas o más en IoT [49].

MODELOS PROPUESTOS	**CAPAS**	**Análisis**
Arquitectura IoT Middleware	Módulo de interoperabilidad Módulo de analítica y persistencia Módulo de contexto Módulo de recursos y eventos Interfaz gráfica de usuario Módulo de seguridad	Esta arquitectura ofrece una plataforma completa y flexible para desarrollar y desplegar soluciones IoT
Arquitectura de 7 capas	Capa de aplicación Capa de soporte y gestión de aplicación Capa de servicios Capa de comunicación Capa de red Capa de hardware Capa de entorno	Esta arquitectura proporciona una estructura detallada y completa para implementaciones de IoT en el hogar
Arquitectura de 7 capas de la ITU-T Y.4000	Capa de aplicación Capa de presentación Capa de sesión Capa de transporte Capa de red Capa de enlace de datos Capa fisica	Esta arquitectura está estandarizada por la UIT-T y proporciona una estructura robusta y bien definida para implementaciones de IoT en el hogar, garantizando la interoperabilidad y la seguridad a través de capas bien definidas.

Después de analizar cada una de las arquitecturas, se considera adecuado tomar como referencia la arquitectura de 7 capas de la (ITU-T Y.4000), la cual se basa en el modelo OSI. Este modelo requiere una "capa de adaptación" para conectar la capa de red y la capa de enlace de datos de las interfaces de red de baja potencia. En la Figura 9, se muestran las capas del modelo, la capa de adaptación es responsable de la compresión, fragmentación, reensamblaje de paquetes y configuración de direcciones de red [50].

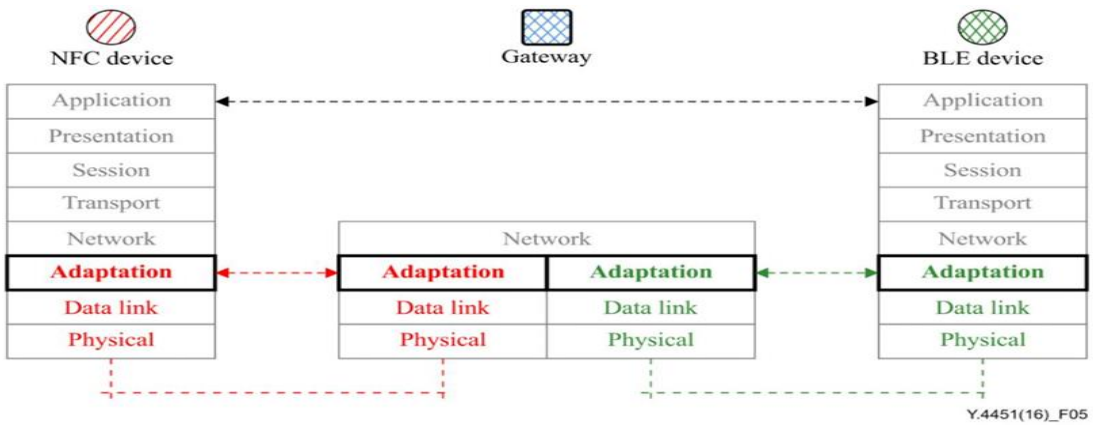


Figura 9. Modelo de arquitectura IoT (ITU-T Y.4000) [50].

Toda esta información recopilada es la base para el diseño del sistema IoT para el hogar. Este sistema está formado por una arquitectura centralizada basada en el modelo de 7 capas de la ITU-T Y.4000, y la infraestructura de red utilizada también es de la ITU Y.4113.

3.6 Diseño del sistema IoT para un hogar

La creación del sistema IoT se desarrolla en un entorno doméstico, este tiene como base una arquitectura centralizada apoyada en el modelo de 7 capas de la ITU-T Y.4000 y una infraestructura para la red basada en la ITU Y.4113. Existen diversos dispositivos inteligentes para el hogar con características y protocolos distintos.

3.6.1 Selección de Sensores y Dispositivos IoT para el hogar inteligente

Para este sistema, se utiliza dispositivos y sensores comerciales IoT más comunes, como asistentes, iluminación inteligente, enchufes inteligentes, cámara de seguridad para el hogar y sensores de contacto. La creación del sistema IoT en un hogar requiere

una planificación cuidadosa y la ejecución de dispositivos adaptados a las necesidades específicas de los habitantes. A continuación, en la Tabla 22, se muestran los dispositivos que se usan para la creación del sistema [51]:

Tabla 22. Dispositivos y sensores IoT del sistema [47-53].

Cantidad	**Tipo**	**Dispositivo**	**Marca**	**Estándares de Comunicación en Redes**	**Ilustración**
1	Parlante de voz	Echo Dot	Amazon	IEEE 802.11n IEEE 802.15	
1	Iluminación	Interruptor de luz inteligente	Teclam	IEEE 802.11b/g/n	
2	Iluminación	Bombilla inteligente	Nexxt Solutions	IEEE 802.11n	
1	Tomacorriente	Enchufe inteligente	Nexxt Solutions	IEEE 802.11b/g	
1	Tomacorriente	Enchufe inteligente	Smart Life	IEEE 802.11n	
1	Vigilancia	Camara inteligente para interiores	Nexxt Solutions	IEEE 802.11b/g	
2	Seguridad	Sensor de contacto para puertas y ventanas	Tuya	IEEE 802.11b/g	

3.6.2 Ubicación de Sensores y Dispositivos IoT en el hogar

Con el objetivo de optimizar la experiencia del usuario y garantizar una mayor eficiencia en la automatización del hogar, a continuación, se presenta un desglose detallado de la ubicación y función de los dispositivos en cada planta del hogar como se puede observar en las Figura 10 y 11, en dónde se detalla la ubicación para la planta baja y alta del hogar.

a. Planta baja

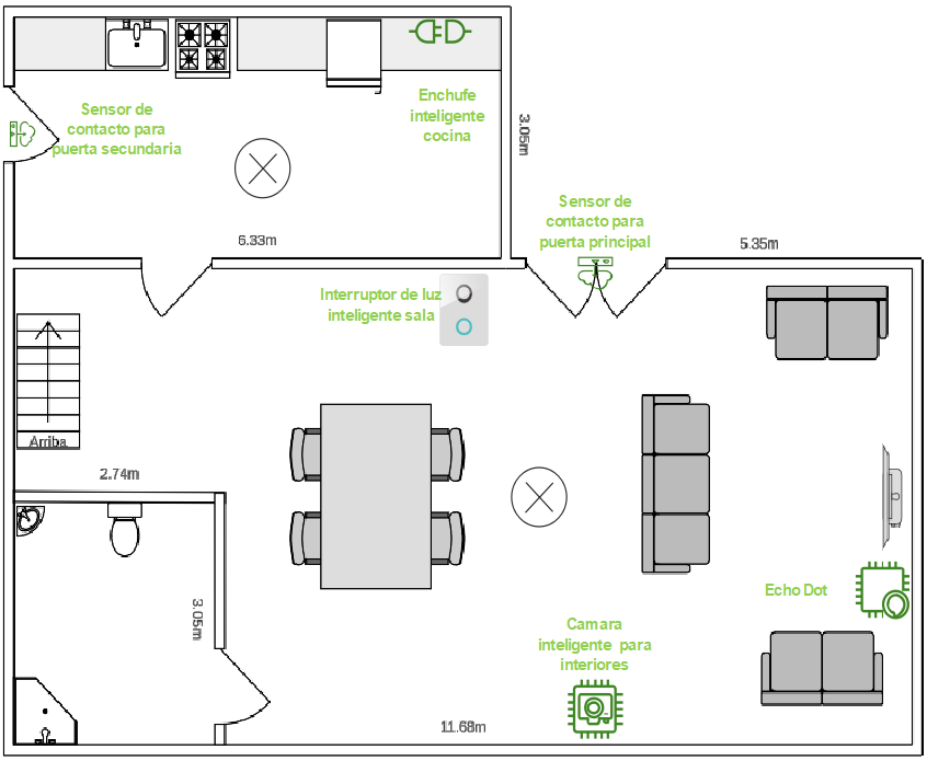


Figura 10. Ubicación de sensores y dispositivos IoT en la planta baja

Sensor de contacto para puertas: La vivienda dispone de dos puertas de acceso, por lo que se ha instala un sensor de contacto tanto en la puerta principal como en la secundaria, con el fin de detectar los accesos al domicilio.

Cámara inteligente para interiores: Se instala a una altura de 2.45 metros sobre el nivel del suelo, con un ángulo de inclinación de 31.48° con respecto al plano horizontal abarcando un campo de visión que cubre las áreas de interés, como la sala, el comedor y la cocina, las cuales conforman la planta baja del domicilio.

Interruptor de luz inteligente: El interruptor controla la iluminación de la sala-comedor y cocina, permitiendo al usuario un manejo más interactivo y sencillo.

Echo dot: Permite el monitoreo de todos los equipos del hogar, facilitando el manejo del sistema a la par puesto que se ha colocado en la sala que es el lugar más concurrido por el usuario ya que en la planta baja se encuentra la sala, comedor, cocina y baño.

Enchufe inteligente: Su ubicación en la cocina se justifica por su capacidad para operar electrodomésticos, porque mejoran la eficiencia en el manejo del dispositivo.

b. Planta alta:



Figura 11. Ubicación de sensores y dispositivos IoT en la planta alta

Enchufe inteligente: Su ubicación en la sala de estar, se justifica porque permite el funcionamiento de un equipo de sonido, optimizando la funcionalidad y contribuyendo a la eficiencia en el manejo del dispositivo.

Bombillas inteligentes: La vivienda se compone de dos estancias, una designada como dormitorio principal y otra destinada para huéspedes. Con el propósito de otorgar al usuario un control óptimo sobre la iluminación, se ha instalado una bombilla inteligente en cada una de estas áreas.

3.6.3 Descripción de la red IoT implementada

La red IoT implementada en el hogar es una infraestructura interconectada de dispositivos inteligentes diseñados para mejorar la comodidad, la eficiencia y la seguridad del hogar. Esta red inteligente permite a los usuarios monitorear y controlar diferentes aspectos de su hogar desde cualquier lugar, optimizando el consumo de energía, aumentando la seguridad y proporcionando una mayor comodidad y conveniencia en la vida diaria. La red se encuentra compuesta por dispositivos IoT, tales como sensores y dispositivos de control, que se conectan a través de una red local inalámbrica (Wi-Fi) a través de un dispositivo intermedio de red, como se observa en la Figura 12.

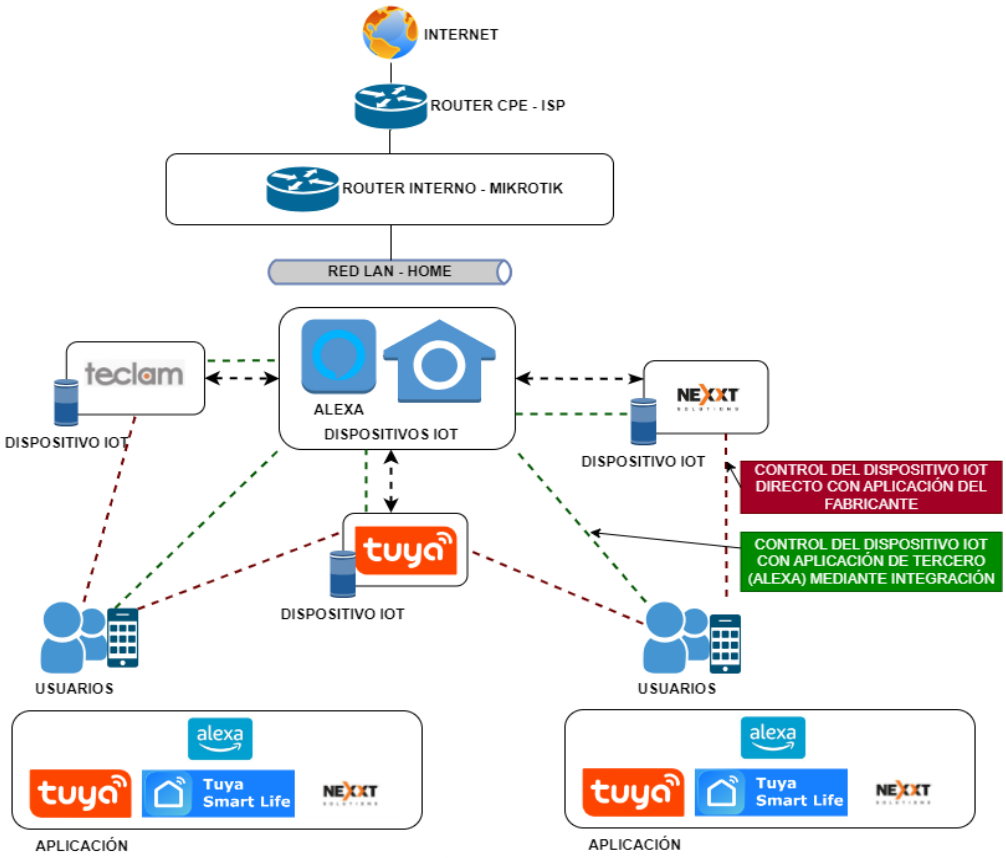


Figura 12. Esquema de red del sistema IoT

Cada dispositivo incorpora una aplicación móvil intuitiva para el usuario, y todas estas son vinculadas a la app de Alexa, lo que le otorga la capacidad de gestionar de manera eficiente cada dispositivo y sensor IoT según las necesidades específicas que se presenten.

3.7 Sistema integral para seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos home

Un sistema integral para seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos domésticos requiere un análisis de varios marcos de referencia, normativas, estándares, buenas prácticas y recomendaciones orientados al área de IoT y Seguridad de la información, como resultado de este análisis se define un modelo parametrizado para cubrir las necesidades de confidencialidad, integridad y disponibilidad en un contexto para entornos domésticos que involucren dispositivos IoT.

3.7.1 Recopilación de Marcos de referencia

Para el desarrollo del modelo de línea base para la seguridad de los datos, la privacidad de las personas y los dispositivos IoT en entornos domésticos, se realiza un exhaustivo análisis de múltiples marcos de referencia reconocidos en el campo de la ciberseguridad y la privacidad de los datos. Entre estos marcos se incluyen importantes normativas, estándares, buenas prácticas y recomendaciones y directrices como el IoT Security Foundation, el National Institute of Standards and Technology (NIST), la Cloud Security Alliance, el Industry IoT Consortium (IIC), el Center for Internet Security (CIS) y el Secure Controls Framework [56-61].

Al integrar las mejores prácticas y recomendaciones de estos marcos de referencia, se ha logrado desarrollar un modelo sólido que aborda de manera integral los aspectos fundamentales de la seguridad de los datos, la protección de la privacidad y la seguridad de los dispositivos IoT en entornos domésticos.

En el Anexo I, en las Tabla I1 a la I3, se encuentra detallada la información de cada uno de los marcos de referencia mencionados anteriormente, con su categoría, dominio, descripción e identificación.

3.7.2 Modelo de línea base para seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos domésticos

A continuación, se detalla el modelo base para seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos del Hogar. Este modelo está subdividido en seis dominios, que son:

1. Gestión - Gobernanza – Dirección.
2. Habilitación e Identificación.
3. Fortaleza Cibernética.
4. Seguimiento – Monitoreo.
5. Educación Digital Avanzada.
6. Continuidad y Anti-Desastre.

a. Gestión - Gobernanza - Dirección.

La gestión de ciberseguridad y privacidad de datos implica procesos, políticas y responsabilidades que contribuyen a la seguridad de la información y los dispositivos. La gobernanza organiza las decisiones de gestión de riesgos cibernéticos y establece estrategias, políticas y vigilancia. Los requerimientos que se deben cumplir son los siguientes [56-61]:

- Establecer objetivos para proteger la seguridad de los datos, de la privacidad de las personas y los dispositivos IoT
- Establecer un modelo o estrategia para la gestión de riesgos
- Establecer políticas y procesos alineados a los objetivos de seguridad y de gestión de riesgos
- Establecer responsabilidades y roles

b. Habilitación e Identificación.

El conjunto de directrices aborda los aspectos físicos, de hardware y software de los dispositivos, asegurando la gestión efectiva de activos, configuraciones seguras y control de acceso. Se enfoca en la protección de activos, la identificación y autenticación de usuarios, así como en la gestión de dispositivos móviles y el desarrollo de tecnología, todo con el objetivo de garantizar un entorno seguro y minimizar los riesgos asociados con los activos tecnológicos. Los requerimientos que se deben cumplir son los siguientes [56-61]:

- Software, Hardware y Objeto físico, se encuentran inventariados o identificados de manera clara
- Se lleva un registro sobre la configuración, la actualización, mantenimientos y cambios realizados en software, hardware y objeto físico
- Gestión de manera segura las contraseñas, autenticación, autorización, control de acceso, gestión de claves

c. Fortaleza Cibernética.

Garantiza la seguridad y protección de los dispositivos por medio de implementación de medidas de seguridad adicionales. Estas prácticas son esenciales para proteger la integridad, confidencialidad y disponibilidad de los dispositivos IoT y los datos que manejan los requerimientos que se deben cumplir, son los siguientes [56-61]:

- Gestión de datos de manera consistente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información. clasificación de datos.
- Comunicaciones seguras y confiables, comunicaciones cifradas, aplicaciones seguras, redes seguras, conexión inalámbrica segura, protecciones criptográficas.
- Gestión de estrategias de riesgo, evaluación de vulnerabilidades y parches para protección de la confidencialidad, integridad y disponibilidad de activos y resiliencia organizacional.

- Dispositivos IoT con configuración segura, plataforma segura, controles de acceso físico, gestión de vulnerabilidades y parches.

- Proteger la confidencialidad, integridad y disponibilidad por medio de la gestión del hardware, software y servicios de plataformas físicas y virtuales.

d. Seguimiento – Monitoreo.

Los activos son monitoreados para encontrar anomalías, indicadores de compromiso para caracterizar los eventos y detectar incidentes de ciberseguridad. Los requerimientos que se deben cumplir son los siguientes [59-60]:

- Monitoreo continuo y análisis de eventos adversos

- Gestión de registros y Defensa de redes

e. Educación Digital Avanzada.

Gestión de hardware, software y servicios de plataformas virtuales y físicas de manera consistente con la estrategia de riesgo de la organización para proteger su confidencialidad, integridad y disponibilidad. Los requerimientos que se deben cumplir son los siguientes [58-60]:

- Concientización de la situación e intercambio de información, a través de actividades de educación continua y ejercicios prácticos.

- Capacitación y concientización para administradores y usuarios

f. Continuidad y Anti-Desastre.

Se gestionan las vulnerabilidades, se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos. Se lleva a cabo respuestas a los incidentes de ciberseguridad detectados. Se realizan pruebas de seguridad y respuestas a eventos e incidentes. Los requerimientos que se deben cumplir son los siguientes [56-60]:

- Evaluación de riesgos y mejoras en los procesos, procedimientos y actividades de gestión de riesgos
- Análisis, administración y mitigación de incidentes
- Ejecución y comunicación de plan de recuperación de incidentes
- Gestión de vulnerabilidades, amenazas, pruebas de seguridad y pruebas de penetración

3.8 Análisis GAP

Para comprender la situación inicial del sistema IoT en el hogar, es fundamental realizar un análisis de necesidades o GAP (Good, Average, Poor), este proceso implica la evaluación entre el estado actual del sistema y el estado deseado o ideal. En el contexto de la seguridad de los dispositivos IoT en el hogar, el análisis GAP ayuda a identificar las brechas o discrepancias entre las prácticas de seguridad actuales y las mejores prácticas recomendadas por los marcos de referencia de seguridad. Al llevar a cabo este análisis, se determina las áreas de mejora y establece un punto de partida claro para implementar las medidas de seguridad permitiendo al usuario comprender dónde se encuentran sus mayores riesgos de seguridad y cómo pueden ser mitigados.

El análisis se lleva a cabo en base al Modelo de línea base para la seguridad de los datos, la privacidad de las personas y los dispositivos IoT en entornos domésticos, con el propósito de mejorar la seguridad cibernética. El Instituto Nacional de Estándares y Tecnología (NIST) proporciona un marco de referencia claro, para la mejora de la seguridad cibernética en infraestructuras críticas, el cual se utiliza como guía para este análisis GAP [63].

En la Tabla 23, se detallan los parámetros utilizados para el análisis de madurez en la que se encuentra el sistema IoT y los mismos que son tomados en cuenta para determinar el nivel de madurez al que se quiere llegar, abarcando desde la valoración "0", hasta la valoración "5", que denota un estado optimizado en el cual se han incorporado herramientas y prácticas avanzadas.

Esto ayuda a llevar a cabo un control para evaluar el estado inicial del sistema IoT doméstico y posteriormente el estado esperado para el mismo para de tal manera mejorar así la eficiencia y efectividad del sistema IoT.

Tabla 23. Niveles de madurez en análisis para la mejora de la seguridad cibernética [63].

Madurez	
0. No existente / No aplicable	Categoría inexistente o Justificación aceptable inherente al contexto
1. Inicial	**No Confiable-** Ambiente impredecible donde las organizaciones no tienen actividades de Categoría y no están diseñadas.
2. Repetible	**Informal-** Las actividades de Categoría existen, pero no se ponen en práctica. Los Categorías dependen básicamente de las personas. No hay un entrenamiento formal ni comunicación de las actividades de Categoría
3. Definido	**Estandarizado-** Las actividades de Categoría existen y están diseñadas, han sido documentadas y comunicadas a los empleados, las desviaciones de las actividades de Categoría probablemente no se detecten
4. Gestionado	**Monitoreado-** Se utilizan herramientas en una forma limitada para soportar las actividades de Categoría
5. Optimizado	**Optimizado-** Es una estructura integrada de Categoría interno con un monitoreo en tiempo real por los responsables, así como mejoras continuas-auto Categoría, se encuentran cambios más rápidos al momento de detectar errores en los manejos de las actividades o en las personas

Mediante la utilización de los criterios detallados en la Tabla 23, se ha llevado a cabo un control para evaluar el estado inicial del sistema IoT doméstico. En la Tabla I4, del Anexo I, se encuentra a detalle el análisis que ofrece una perspectiva de cómo se encuentra el sistema IoT y a donde se quiere llegar.

La Figura 13, detalla un análisis GAP inicial de un sistema IoT doméstico, centrado en la madurez de las categorías (CAT1 a CAT20). Cada categoría se representa en un eje, con niveles de madurez que varían de 0 a 6. La categoría de referencia (REF) presenta un nivel de madurez de 6, mientras que las otras categorías muestran niveles de madurez de 1. Este contraste indica el estado actual del sistema IoT doméstico muestra un desarrollo limitado en las categorías evaluadas, con una significativa brecha.

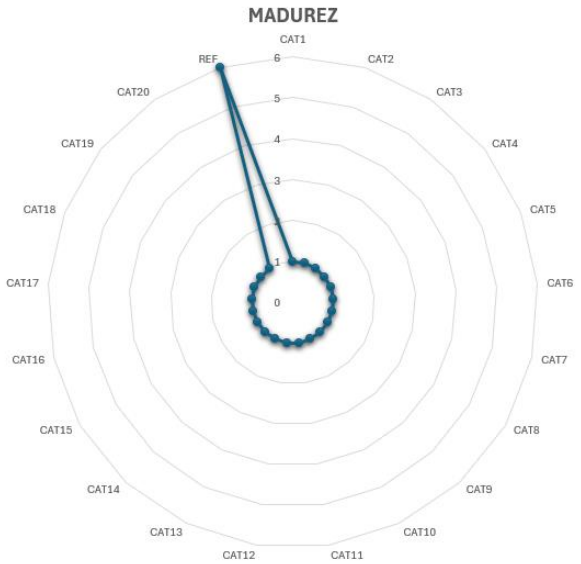


Figura 13. Madurez del análisis GAP inicial

Posteriormente, en la Figura 14, se muestra el nivel de madurez esperado al cual se estima llegar en el contexto de la seguridad de los dispositivos IoT en el hogar, cada categoría se distribuye a lo largo de un eje, con niveles de madurez que varían de 0 a 6. La categoría de referencia (REF) alcanza un nivel de madurez de 6, que representa el objetivo ideal, las demás categorías muestran niveles de madurez variables, con algunas alcanzando hasta 5 y otras cayendo hasta 1 o 2, indicando una brecha significativa, en el Anexo I, Tabla I5, se encuentra a detalle el análisis esperado, mostrando una diferencia con la Figura 13.

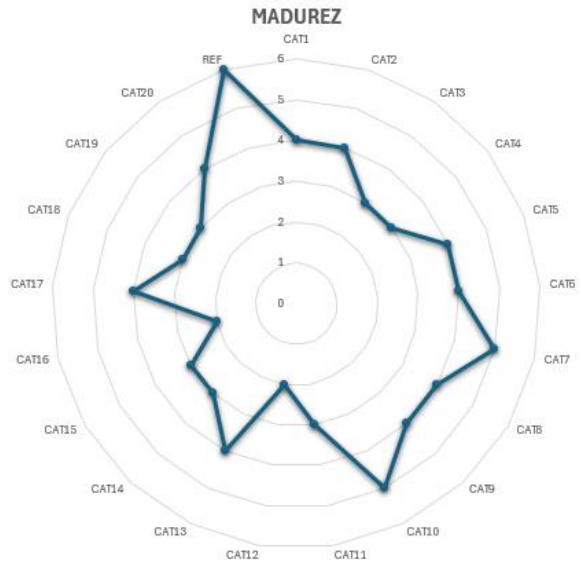


Figura 14. Madurez del análisis GAP esperado

3.9 Implementación del modelo de línea base creado

En este punto, se implementa el modelo de línea base para la seguridad de datos, privacidad de las personas y dispositivos IoT en entornos domésticos iniciando con la identificación y valoración de activos existentes en el hogar, posterior a ello se determina las políticas y controles de seguridad para el hogar, se analiza las vulnerabilidades y se realizan pruebas de penetración, finalmente se elabora el plan de tratamiento de riesgos.

3.9.1 Política general de seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos home.

Esta política tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de los datos, así como proteger la privacidad de los usuarios y la seguridad de los dispositivos IoT en entornos domésticos. Se aplica a todos los miembros del hogar y cualquier persona con acceso a los dispositivos IoT, abarcando todas las actividades relacionadas con la implementación y mejora continua de medidas de seguridad y privacidad.

En esta política general se definen los roles y responsabilidades específicos, tales como el Responsable de Seguridad de la Información (RSI), el Administrador de Dispositivos IoT y el Gestor de Privacidad de Datos, asegurando una gestión eficaz de la seguridad. Además, se establece el alcance completo del modelo a implementar, cubriendo todos los aspectos de protección de datos, privacidad y seguridad de los dispositivos IoT en entornos domésticos.

Se detallan, de manera muy general, las políticas y controles esenciales, como la implementación de cifrado de extremo a extremo, actualizaciones regulares de los dispositivos IoT, configuración segura de la red doméstica y control de acceso a los dispositivos. Para una descripción más detallada de las responsabilidades, roles, objetivos específicos y políticas generales, consulte el Anexo A.

3.9.2 Determinación de herramientas especializadas para la detección de posibles vulnerabilidades existentes en el sistema IoT.

Para determinar las vulnerabilidades existentes en el sistema IoT existen varias herramientas, a continuación, se desarrolla una comparativa de estas en la Tabla 24:

Tabla 24. Comparativa de herramientas para detección de vulnerabilidades [62-64]

Características	**Nessus**	**OpenVAS**	**Rapid7 Nexpose**
Facilidad de Uso	Alta, interfaz gráfica intuitiva y fácil de navegar	Moderada, interfaz gráfica pero más compleja	Moderada, interfaz gráfica pero más compleja
Detección de Vulnerabilidades	Excelente, base de datos de vulnerabilidades amplia y actualizada	Muy buena, base de datos amplia pero menos actualizada	Excelente, base de datos amplia y detallada
Cobertura de Dispositivos IoT	Muy buena, escaneos específicos para dispositivos IoT	Buena, aunque más generalizada	Buena, cubre IoT pero no es su enfoque principal
Reportes y Análisis	Excelente, reportes detallados y personalizables	Buena, reportes detallados, pero menos personalizables	Muy buena, reportes detallados
Costo	Moderado, con opciones de pago según características	Gratuito, aunque con opciones de pago para funcionalidades adicionales	Alto, basado en suscripción

Nessus ofrece un equilibrio entre facilidad de uso, capacidades avanzadas de detección, y cobertura específica para dispositivos IoT, por lo que se elige esta herramienta para la detección de vulnerabilidades en el sistema IoT doméstico.

3.9.3 Identificación y valoración de Activos del sistema IOT doméstico

Para el proceso de identificación de activos, se ha recurrido a varios marcos de referencia. Entre estos destacan el National Institute of Standards and Technology (NIST), el IoT Security Foundation, el Industry IoT Consortium (IIC), el Center for Internet Security (CIS). Estas instituciones ofrecen directrices rigurosas para la clasificación de activos. Conforme a estos marcos de referencia, se ha llevado a cabo una meticulosa clasificación de los tipos de activos existentes, como se observa en la Tabla 25.

Tabla 25. Tipos de activos [57-58], [60-61]

Activo	Definición	Ejemplos
[S] Servicio	Los servicios, se pueden determinar internamente cuando se producen dentro del reparto y se determinan como externos cuando se consume de otras unidades o proveedores.	World Wide Web, Acceso remoto a cuenta local, correo electrónico, almacenamiento y transferencia de ficheros, servicio de directorio, gestión de identidades y privilegios, clave pública.
[D] Datos/información	Los datos son soportes de información que los usuarios los deben valorar. Su clasificación debe determinar los niveles de confidencialidad y el valor que los califica.	Documentación calificada y ordinarios, documentos de gestión interna, voz, multimedia, código fuente, código ejecutable, datos de configuración, logs, datos de pruebas, etc.
[SW] Aplicaciones (software)	Las aplicaciones se refieren a programas, aplicativos, desarrollos, entre otros.	Desarrollo propio, desarrollo a medida, servidor de presentación, de aplicaciones, cliente de correo electrónico, bases de datos, monitor transaccional, antivirus
[HW] Equipos informáticos (hardware)	Se refiere a los bienes materiales o físicos que son de utilidad para la unidad y que pueden ser reemplazados si fuera así la necesidad.	Computadoras (escritorio, laptops), agendas electrónicas, periféricos, equipos de impresión, escáneres, modemes, routers, cortafuegos, punto de acceso Wireless, central telefónica, etc.
[COM] Redes de comunicaciones	Se refiere a la infraestructura de comunicaciones sobre redes.	Red telefónica, red digital, ADSL, Punto a punto, Red inalámbrica, red satelital, red local, Internet
[SI] Soporte de información	Se refiere a los dispositivos de almacenamiento de datos.	Discos duros, almacenamiento en red, CD-ROM, dispositivos USB, DVD, etc.
[AUX] Equipamiento auxiliar	Se refiere al equipamiento que complementa el material informático, apoyando la infraestructura de la unidad.	Fuentes de alimentación, generadores eléctricos, equipos de climatización, cableado, entre otros.
[L] Instalaciones	Las instalaciones, son los lugares donde se encuentra la infraestructura tecnológica.	Edificio, locales, oficinas, plataformas móviles, vehículo terrestre, aéreos, marítimo, contenedores, etc.
[P] Personal	Se refiere a las personas involucradas con los procesos y sistemas de información dentro de la organización.	Operadores, administradores de sistemas, administradores de bases de datos, desarrolladores, etc.

La IoT Security Foundation con el objetivo de asegurar la integridad y confiabilidad de un producto, establece un sistema de clasificación de activos basado en clases de garantía, en la Tabla B1 del Anexo B, se describe cada una de las clases, las cuales permiten valorar el nivel de impacto de cada uno de los dispositivos del hogar.

En la Tabla 26, y basada en la tabla B1 del Anexo B, se examina a detalle todos los activos conectados a la red, acompañado de un análisis de las clases de garantía, evaluando minuciosamente cada activo y asignando el correspondiente valor de impacto a cada dispositivo del sistema IoT, se comprende las áreas críticas dentro del entorno de red para aplicar medidas de protección y mitigación de riesgos.

Tabla 26. Análisis de cada uno de los activos del Hogar

ID	Número de serie	Nombre de activo	Fabricante	Tipo	Usuario	Ubicación fisica	Nivel de Impacto			
							C	I	D	VA
1	2201117TL	Teléfono Inteligente	Xiaomi	Dispositivo	Jefe de Hogar	Casa	Alto	Alto	Alto	Clase 4
2	AHIMPFI4U1	Cámara Inteligente para Interiores	Nexxt Home	Dispositivo	Jefe de Hogar	Sala	Medio	Medio	Alto	Clase 2
3	LR03DC	Sensor de Contacto para Puertas y Ventanas	Tuya	Dispositivo	Jefe de Hogar	Puerta Principal	Medio	Medio	Alto	Clase 2
4	LR03DA	Sensor de Contacto para Puertas y Ventanas	Tuya	Dispositivo	Jefe de Hogar	Puerta Secundaria	Medio	Medio	Alto	Clase 2
5	PT2024	Enchufe Inteligente	Smart Life	Dispositivo	Esposa	Sala de estar	Bajo	Bajo	Bajo	Clase 0
6	AHIWPSO4U1	Enchufe Inteligente	Nexxt Home	Dispositivo	Esposa	Cocina	Bajo	Bajo	Bajo	Clase 0
7	X4YHABUW110	Bombilla Inteligente	Nexxt Home	Dispositivo	Esposa	Habitación Principal	Bajo	Bajo	Bajo	Clase 0
8	X4WHABCY110	Bombilla Inteligente	Nexxt Home	Dispositivo	Jefe de Hogar	Habitación Huéspedes	Bajo	Bajo	Bajo	Clase 0
9	PS0213	Interruptor de Luz Inteligente	Teclam	Dispositivo	Esposa	Sala/Cocina	Bajo	Bajo	Bajo	Clase 0
10	G6G22H0724620VPV	Echo Dot	Amazon	Dispositivo	Jefe de Hogar	Sala	Alto	Alto	Alto	Clase 4

3.10 Análisis de Vulnerabilidades del sistema IoT para el hogar

Para el análisis de vulnerabilidades del sistema IoT en el hogar, se implementa una red honeynet con el objetivo de detectar y registrar los diferentes tipos de ataques. Esta red se configura con puertos y servicios similares a los de los dispositivos IoT, ello se realiza con un análisis de los dispositivos, en la Tabla I6, del Anexo I, se muestra el análisis por capas de cada uno de ellos. Permitiendo una visibilidad completa sobre los posibles ataques, una vez configurada la honeynet, se realiza pruebas de pentesting para identificar y tratar de explotar las vulnerabilidades en base a su criticidad. Este enfoque permite una evaluación detallada y efectiva de las amenazas y debilidades del sistema IoT en el entorno doméstico.

3.10.1 Infraestructura de la red necesaria para la honeynet

En base a la información detallada para la infraestructura de la red del hogar, como se observa en la Figura 15, ésta incluye un enrutador MikroTik y la implementación de una honeynet que proporciona un entorno controlado para la conectividad de

dispositivos, al tiempo que permite la detección y el análisis de posibles riesgos cibernéticos para mejorar la seguridad y conciencia de la ciberseguridad.

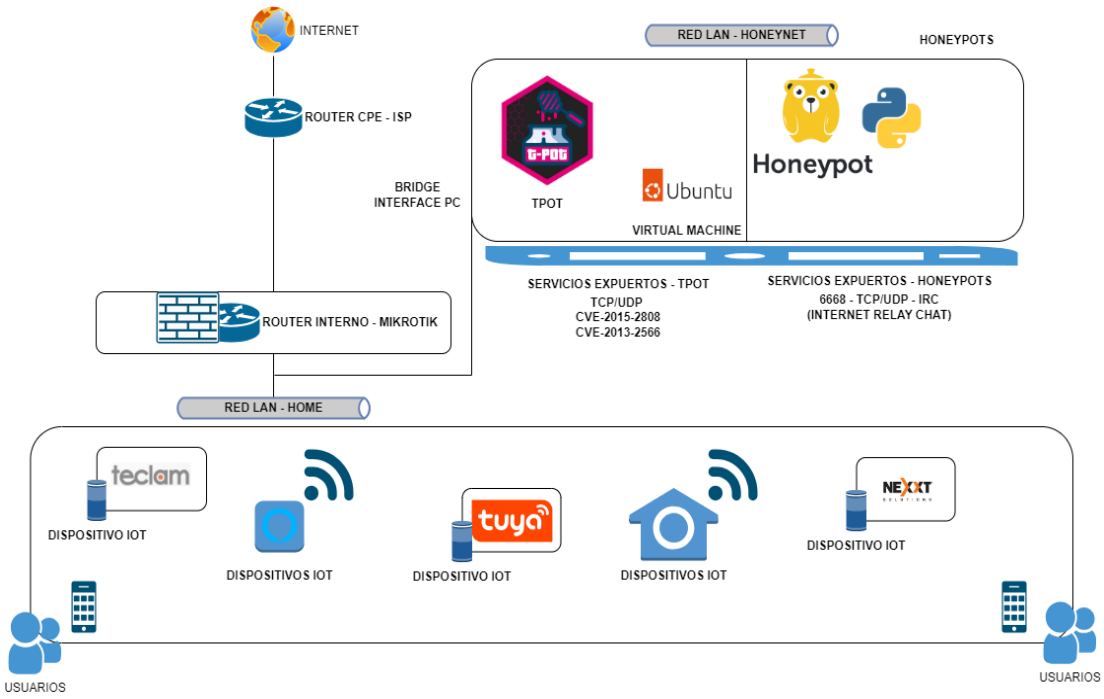


Figura 15. Diagrama de la infraestructura de la red

En el diagrama de la infraestructura de la red, se observa la interconexión detallada entre los dispositivos home, el enrutador interno y el enrutador principal CPE - ISP. Cada dispositivo IoT, como sensores de contacto, luces o enchufes inteligentes, se representa con su propia conexión inalámbrica al enrutador interno, posterior a ello, la honeynet se encuentra entre el enrutador CPE y el enrutador interno en el cual se configura el firewall.

3.10.2 Implementación de HONEYNET

Un honeynet es una red de honeypots conectados entre sí, diseñado específicamente para ser un objetivo fácil para atacantes, existen honeypots de baja, media y alta interacción, la Tabla 27, muestra una comparativa entre estos, para determinar cuál es el más viable para el ámbito de IoT doméstico.

Tabla 27. Comparativa de tipos de honeypots [68].

Tipo	Descripción	Ventajas	Desafíos
Baja Interacción	Simulan servicios y dispositivos con funcionalidad mínima	Facilidad de implementación, seguridad, detección de ataques	Limitada información sobre táctica
Media Interacción	Ofrecen más servicios y respuestas más realistas	Mayor realismo, equilibrio entre complejidad y utilidad	Más complejos que los de baja interacción
Alta Interacción	Simulan sistemas completos, permiten amplia interacción	Información detallada, máximo realismo	Complejidad y riesgo elevados, más recursos necesarios

Los de honeypots de baja y media interacción son los más adecuados, puesto a que ofrecen un equilibrio entre facilidad de implementación, seguridad, y capacidad de captura de información sobre ataques dirigidos a dispositivos IoT domésticos. Para determinar que honeypots son los más adecuados para la implementación de dicha honeynet, en la Tabla 28, se muestra una comparación de los honeypots de media y baja interacción.

Tabla 28. Honeypots de interacción baja y media especializados para IoT [40].

	Dionaea	ConPot	Honeyd	Cowrie	CitrixHoneypot
Interacción	Baja	Media	Baja / Media	Media	Media
Entorno	Profesional	Profesional	Profesional	Profesional	Profesional
Características relevantes	- Fork de Nepenthes. -Soporta IPv6. -Usa libemu	- Emulación de dispositivos industriales - Registro detallado de interacciones	-Permite que un solo host tenga varias direcciones - Usado como base para otros honeypots	-Login muy flexible -Simula sistemas de ficheros completos - Hace log	- Emulación de servicios de Citrix - Detección de ataques específicos a Citrix
Hardware	NO	NO	NO	NO	NO
Protocolo	SMB, Soporta IPv6.	Modbus, SNMP, HTTP, Siemens S7	Telnet	SSH	ICA/HDX
Descargable	SI	SI	SI	SI	NO

Actualmente, existen varias herramientas como TPOT, Modern Honey Network (MHN) y HoneyDrive para la implementación y gestión de honeynets. TPOT es una plataforma multi-honeypot que contiene varios honeypots dockerizados en un mismo sistema operativo, logrando tener servicios de red de detección de intrusos y a la vez un motor de seguimiento, MHN, por su parte, es una plataforma flexible que permite la integración de varios honeypots, pero requiere configuraciones adicionales para alcanzar el mismo nivel de cohesión y funcionalidad que TPOT, y HoneyDrive tiene

una distribución de Linux preconfigurada con diversas herramientas de seguridad y honeypots, que facilita la instalación y uso, pero no ofrece la misma capacidad de análisis en tiempo real y centralización que TPOT [69].

Se encontró ideal usar TPOT, ya que esta herramienta contiene en su entorno honeypots de baja y media interacción, además se toma en cuenta la Tabla I6, del Anexo I, para la selección de honeypots, los honeypot ConPot y CitrixHoneypot son opciones preferibles debido a sus características específicas que abordan las necesidades de seguridad en un sistema IoT doméstico.

a. Diagrama de gestión de la información

En la Figura 16, se muestra el diagrama de gestión de la red, que detalla la administración y supervisión de los dispositivos conectados, se observa que los dispositivos IoT están conectados a la red WIFI y son administrados mediante la app de Alexa, instalada en el teléfono celular del jefe de hogar. La honeynet está conectada a la red mediante un virtualizador tipo uno para la administración de las máquinas virtuales en el cual se levantan las distintas honeypots.

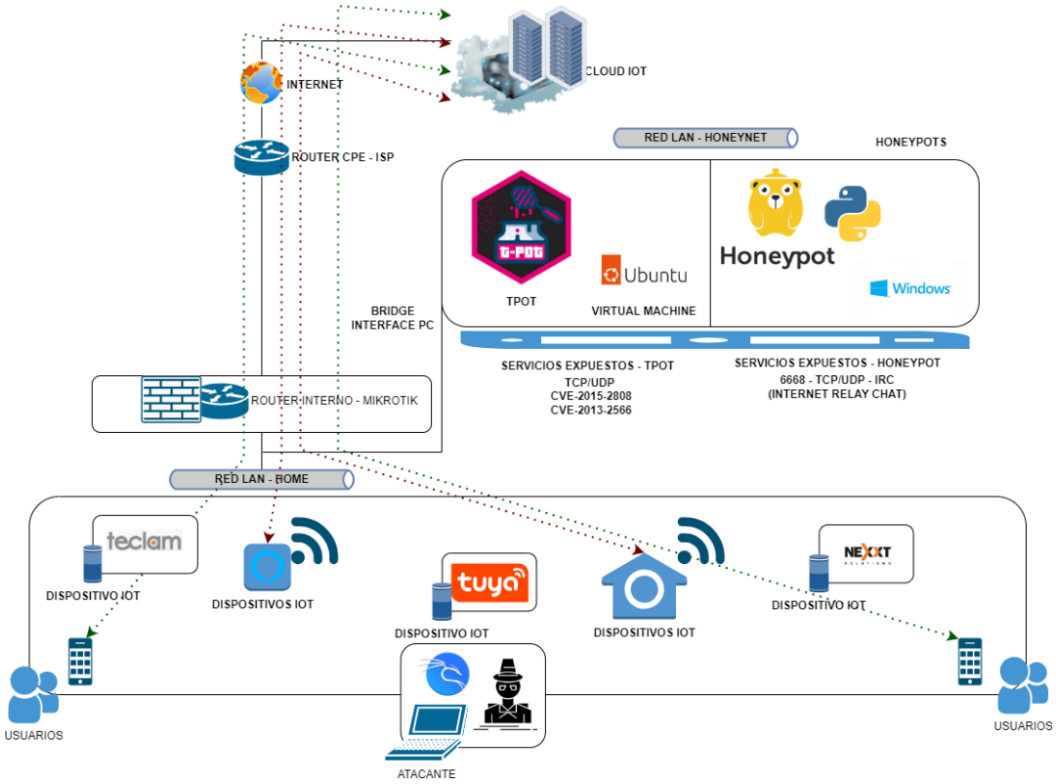


Figura 16. Diagrama de gestión de la red

La honeynet, se coloca dentro de la red LAN junto con los dispositivos IoT legítimos. De esta manera, cuando el atacante realice un primer reconocimiento, podrá ver a los honeypots como objetivos más fáciles de acceder, ya que están diseñados precisamente para atraer a los atacantes. Estos honeypots actúan como "tarros de miel", registrando los ataques y proporcionando valiosa información sobre las tácticas y técnicas utilizadas por los intrusos.

El equipo de red utilizado para esta configuración permite realizar ajustes a nivel de capa 3 (red) y capa 4 (transporte), integrando características de firewall. Esto permite filtrar el tráfico y establecer reglas para bloquear direcciones IP o puertos en función del comportamiento del tráfico de un dispositivo dentro de la red. Estas capacidades no solo mejoran la seguridad al detectar y bloquear actividades maliciosas, sino que también facilitan la recopilación de datos para el análisis de amenazas.

b. Implementación de T-POT

Para el primer escenario de pruebas, se dispone de un servidor T-Pot instalado desde su imagen ISO.

Para la elaboración del escenario de pruebas fueron necesarios los siguientes componentes:

- 1 máquina física
- Programa de virtualización
- Plataforma Multi-Honeypot TPOT

La instalación y configuración de la herramienta se encuentra en https://github.com/telekom-security/tpotce, para la implementación se seleccionó la opción estándar en la que vienen varios honeypot integrados como son: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeysap, honeytrap, mailoney, medpot, rdpy, snare & tanner. Las herramientas de control para la captura de ataques integradas en TPOT para el tipo estándar son: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall,

spiderfoot, p0f & suricata. La Figura 17, muestra que, una vez terminada la instalación, se ingresa por medio del puerto 64297 a la interfaz de inicio de un sistema T-Pot.

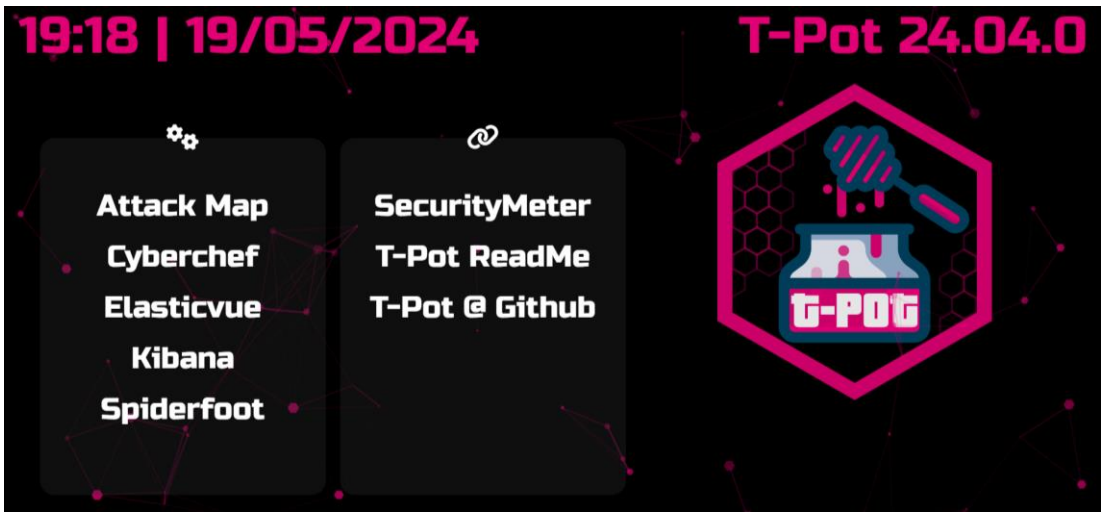


Figura 17. Interfaz de inicio de TPOT

En este caso se usa la herramienta Kibana para la visualización del correcto funcionamiento de TPOT, Kibana es utilizada para la visualización y análisis de datos basada en Elasticsearch. La Figura 18, presenta una barra que muestra la cantidad de ataques recibidos por cada tipo de honeypot. Honeytrap claramente ha recibido la mayor cantidad de ataques. El gráfico circular que muestra la distribución de los sistemas operativos de origen de los ataques. Muestra varios sistemas operativos como Linux, Windows NT Kernel, Windows XP, etc. A más de ello, se muestra un histograma que visualiza los ataques según el puerto de destino, lo cual puede ayudar a identificar qué puertos son más frecuentemente atacados.

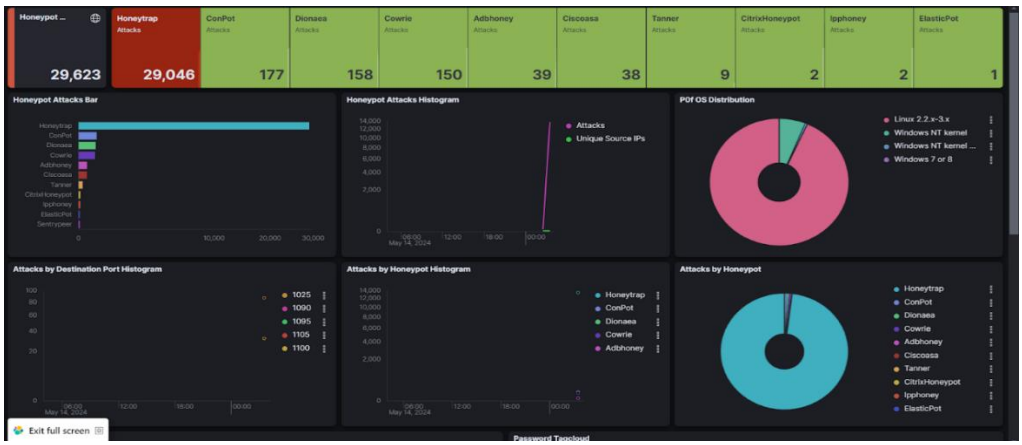


Figura 18. Visualización de funcionamiento de TPOT con Kibana

Los datos visualizados en la interfaz de Kibana, como se ilustra en la Figura 19, revelan una captura exhaustiva del número de ataques a la red, incluyendo las direcciones IP correspondientes. Además, se destacan los CVE (Common Vulnerabilities and Exposures) detectados por Suricata, así como las alertas emitidas por este sistema de detección de intrusiones, proporcionando una visión detallada y precisa de las amenazas y vulnerabilidades identificadas en el entorno monitoreado.

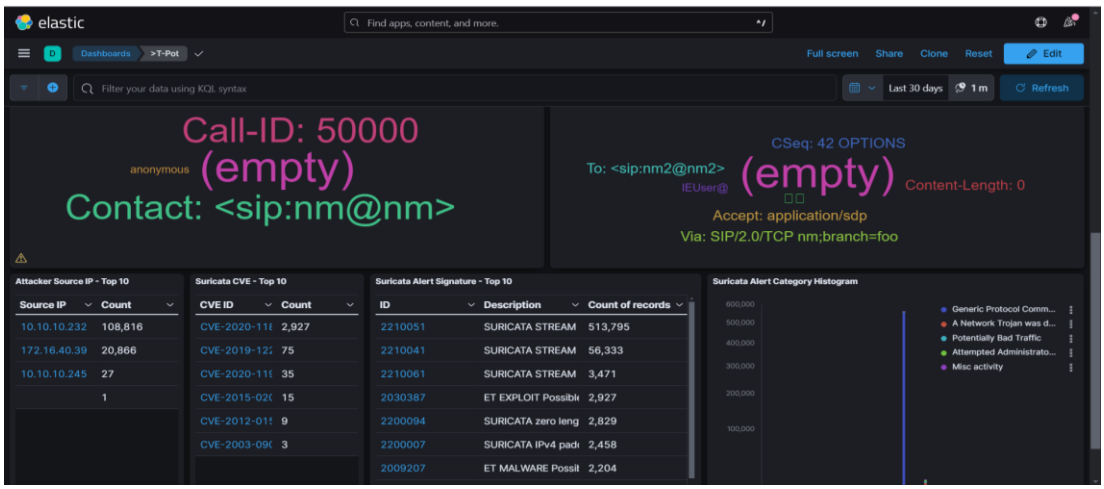


Figura 19. Captura de ataques en TPOT

c. Implementación de Honeypot de baja interacción para detección de ataque de DoS TCP SYN Flooding con Python.

Para la creación de este honeypot de baja interacción, se analiza Python frente a otras herramientas como C y Ruby, y en la Tabla 29, se muestra la comparativa.

Tabla 29. Comparativa para la creación de honeypot [70].

Características	**Python**	**C/C++**	**Ruby**
Facilidad de uso y Lectura del Código	Alta	Baja	Alta
Bibliotecas y Herramientas Específicas	Amplia gama (scapy, twisted, dpkt)	Limitada, requiere más desarrollo manual	Menos especializada que Python
Desarrollo Rápido y Prototipado	Muy rápido	Lento	Rápido
Portabilidad	Muy alta, multiplataforma	Alta, pero puede requerir modificaciones	Alta
Integración con Otras Herramientas	Excelente, fácil integración con SIEM y herramientas de análisis	Buena, pero requiere más esfuerzo	Buena
Rendimiento	Bueno, suficiente para honeypots de baja interacción	Excelente	Bueno

La combinación de Python entre la facilidad de uso, rapidez en el desarrollo, y una amplia disponibilidad de bibliotecas específicamente para la seguridad y redes, lo convierte en una opción adecuada para la implementación de honeypots de baja interacción. Python permitió el diseño de un honeypot cuyo propósito es mantener un puerto abierto y capturar todo el tráfico dirigido a dicho puerto, mediante la utilización de: las librerías *scapy* para capturar y manipular los paquetes de red, *threading* para la ejecución del servicio TCP y la captura de paquetes, *socket* para la creación de servidores TCP y *time* para gestionar y calcular el tiempo. El desarrollo de la programación detallada de este sniffer se encuentra documentado en el Anexo C, proporcionando una descripción exhaustiva de su implementación y funcionamiento. La Figura 20, muestra que, al correr el script de Python, se empieza a capturar los datos.

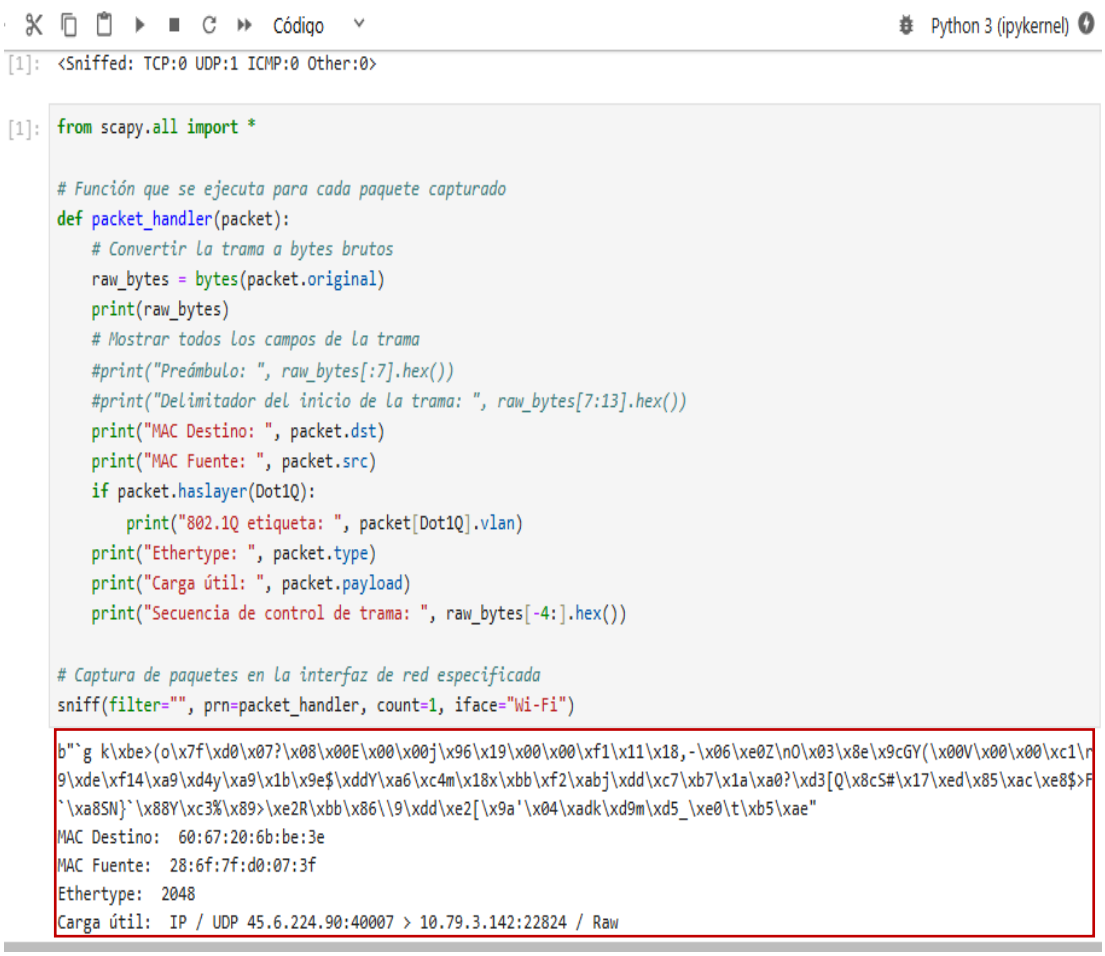


Figura 20. Captura de datos en honeypot

Para una mejor visualización de los datos capturados sobre los ataques DoS TCP SYN Flooding por este honeypot, se crea una base de datos. Para seleccionar la opción más adecuada, se realiza una comparativa detallada, como se muestra en la Tabla 30.

Tabla 30. Comparativa de base de datos

Características	MongoDB	MySQL (Relacional)	Redis (NoSQL - Clave-Valor)
Modelo de Datos	Documental (JSON/BSON)	Relacional (Tablas)	Clave-Valor
Flexibilidad del Esquema	Alta, esquema dinámico	Baja, esquema fijo	Alta, sin esquema
Facilidad de Integración con Python	Excelente, buen soporte de bibliotecas	Buena, pero requiere ORM (e.g., SQLAlchemy)	Excelente, soporte nativo de bibliotecas
Capacidades de Consulta	Potente, con soporte para consultas complejas y agregaciones	Muy potente, pero requiere SQL	Básico, limitado a operaciones clave-valor
Facilidad de Uso y Configuración	Alta, configuración sencilla y uso intuitivo	Moderada, requiere conocimientos de SQL y diseño de esquemas	Muy alta, configuración sencilla
Análisis y Agregación de Datos	Muy buena, soporte para pipeline de agregación	Buena, pero requiere consultas SQL complejas	Limitada, no está diseñada para agregaciones complejas

MongoDB ofrece una combinación de flexibilidad, escalabilidad y facilidad de uso, resultando ideal para este honeypot. Los datos capturados son enviados a la base de datos para su análisis. A partir de estos datos, se generan gráficas que muestran el número de conexiones en función del tiempo y la cantidad de puertos con el número de conexiones correspondientes. Se usan las librerías: *pymongo* para interactuar con MongoDB desde python, *datetime* para el manejo de fechas y horas, *matplotlib* para la generación y visualización de las gráficas, y *pandas* para la manipulación y análisis de datos. Estas visualizaciones permiten una comprensión del comportamiento del ataque. La Figura 21, muestra la base de datos con la que funciona este honeypot.

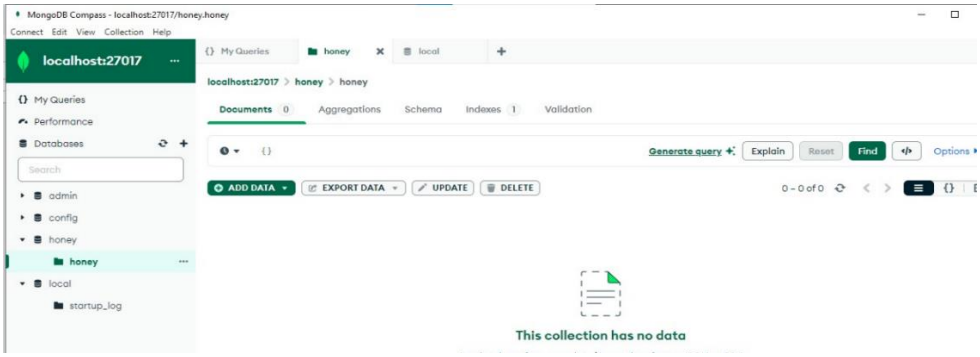


Figura 21. Base de datos en Mongo

Los comandos y funciones clave para el correcto funcionamiento de este honeypot son:

- MongoClient('mongodb://localhost:27017/'): Para conectarse a la base de datos local MongoDB.
- sniff(filter="tcp and dst port 6668", prn=packet_handler, iface="Wi-Fi"): Captura paquetes TCP dirigidos al puerto 6668 en la interfaz de red "Wi-Fi" y ejecuta la función packet_handler por cada paquete capturado.
- packet.haslayer(TCP): Verifica si el paquete capturado contiene una capa TCP.
- packet[TCP].flags == "S": Verifica si el paquete TCP tiene la bandera SYN activa, indicando un intento de inicio de conexión.
- collection.insert_one({...}): Inserta un documento en la colección de MongoDB.
- socket.socket(socket.AF_INET, socket.SOCK_STREAM): Crea un socket TCP para el servidor.
- s.bind((HOST, PORT)): Asocia el socket a una dirección IP y puerto específico.
- s.listen(): Hace que el socket escuche conexiones entrantes.
- threading.Thread(target=tcp_server).start(): Inicia el servidor TCP en un hilo separado.
- matplotlib.pyplot: Utilizada para generar gráficos de las conexiones capturadas y los puertos utilizados.
- pandas.DataFrame(connection_data): Crea un DataFrame con los datos de las conexiones para un análisis más fácil.

3.10.3 Pruebas de penetración “PENTESTING”

En el Anexo D, se presenta el informe técnico a detalle de las pruebas de penetración, desarrollado en base al “Informe de Seguridad de la Información y Ciberseguridad de una entidad financiera”. El alcance de este análisis y escaneo de vulnerabilidades con la plataforma Nessus Tenable se centra en evaluar la seguridad y privacidad de un entorno doméstico típico, abarcando una variedad de dispositivos IoT y sistemas conectados. El objetivo es identificar posibles debilidades en la infraestructura tecnológica del hogar que puedan ser explotadas por amenazas externas o internas, comprometiendo así la integridad de los datos personales y la privacidad de los residentes [71].

3.10.4 Análisis de Vulnerabilidades

a. Situación actual y debilidades encontradas para cada uno de los componentes analizados

La Tabla 31, hace referencia al número de vulnerabilidades detectadas en los activos de la infraestructura del hogar en base al reporte de análisis de Vulnerabilidades generado por Nessus Tenable, el reporte generado por Nessus, se encuentra en el Anexo E.

Tabla 31. Detalle de vulnerabilidades detectadas en IPs

IP	Dispositivo	Crítica	Alta	Media	Baja	Total general
10.10.10.239	Enchufe inteligente	0	0	0	0	0
10.10.10.238	Bombilla inteligente	0	0	0	0	0
10.10.10.236	Interruptor de luz inteligente	0	0	0	0	0
10.10.10.222	Enchufe inteligente	0	0	0	0	0
10.10.10.221	Cámara inteligente para interiores	0	0	0	1	1
10.10.10.220	Echo dot	0	0	8	0	8
10.10.10.218	Bombilla inteligente	0	0	0	0	0
10.10.10.230	Sensor de contacto para puertas	0	0	0	0	0
10.10.10.216	Sensor de contacto para puertas	0	0	0	0	0
Total general		**0**	**0**	**8**	**1**	**9**

Conforme al análisis proporcionado por el informe generado a través de Nessus, en la Tabla 32, se presenta de manera detallada la propuesta de medidas correctivas destinadas a abordar las vulnerabilidades detectadas por esta herramienta.

Tabla 32. Detalle de Remediación Vulnerabilidades – Activos Involucrados

Dispositivo	IP	Código Vulnerabilidad	Vulnerabilidad	Prioridad
Cámara	10.10.10.221	10114	ICMP Timestamp Request Remote Date Disclosure	Baja
Echo dot	10.10.10.220	51192	SSL Certificate Cannot Be Trusted	Medio
Echo dot	10.10.10.220	51192	SSL Certificate Cannot Be Trusted	Medio
Echo dot	10.10.10.220	57582	SSL Self-Signed Certificate	Medio
Echo dot	10.10.10.220	57582	SSL Self-Signed Certificate	Medio
Echo dot	10.10.10.220	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medio
Echo dot	10.10.10.220	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medio
Echo dot	10.10.10.220	104743	TLS Version 1.0 Protocol Detection	Medio
Echo dot	10.10.10.220	157288	TLS Version 1.1 Deprecated Protocol	Medio

b. Evidencias de las principales vulnerabilidades encontradas y mapa de riesgos principales asociadas a las vulnerabilidades identificadas.

La vulnerabilidad ICMP Timestamp Request Remote Date Disclosure se considera de baja severidad, ya que revelar la fecha y hora del sistema remoto por sí sola generalmente no representa un riesgo significativo de seguridad, por lo que a continuación se presenta las evidencias para las vulnerabilidades de gravedad media que son las que si representan un impacto más alto en el sistema IoT. La Tabla 33, muestra a detalle la vulnerabilidad SSL Certificate Cannot Be Trusted encontrada en el dispositivo con la IP 10.10.10.220

Tabla 33. SSL Certificate Cannot Be Trusted

Vulnerabilidad: SSL Certificate Cannot Be Trusted		**CVE:** -
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Baja
CVSS2: 6.4		**CVSS3:** 6.5
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: No se puede confiar en el certificado X.509 del servidor. En esta situación se puede romper la cadena de confianza. La vulnerabilidad se detecta en los puertos TCP: 10001 y 55443		
Impacto de la vulnerabilidad: Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web. facilitando la realización de ataques man-in-the-middle.		
Remediación: Compre o genere un certificado SSL adecuado para este servicio.		

En la Figura 22, se evidencia la explotación de la vulnerabilidad, se identifica que el certificado no es emitido por una entidad autorizada. Por medio de una máquina atacante, con el comando openssl s_client se establece una conexión SSL/TLS con el servidor remoto ubicado en la dirección IP 10.10.10.220 en el puerto 10001

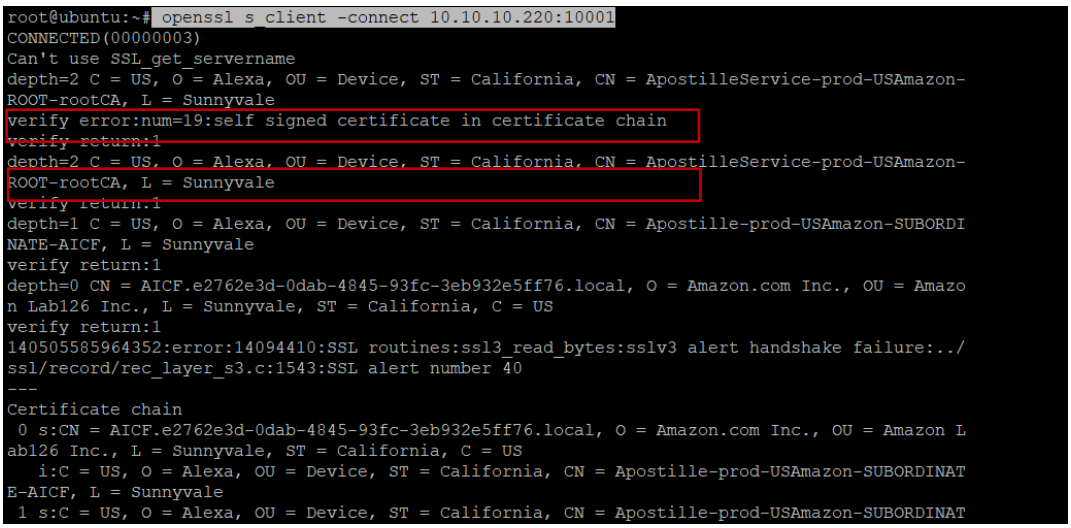


Figura 22. Evidencia de configuración y expedición del certificado SSL.

De igual manera, se explota la misma vulnerabilidad ahora en el TPOT, en la Figura 23, se evidencia la explotación y la respuesta que indica que el certificado no es emitido por una entidad autorizada. Por medio de una máquina atacante, con el comando openssl s_client se establece una conexión SSL/TLS con el servidor remoto ubicado en la dirección IP 10.10.10.217 en el puerto 443

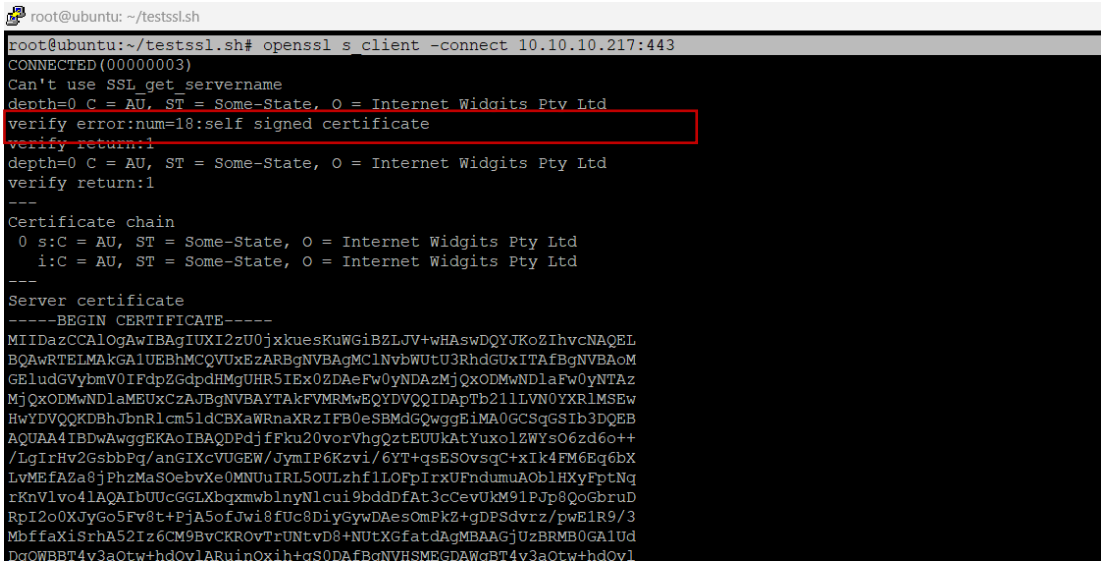


Figura 23. Evidencia de configuración y expedición del certificado SSL en TPOT

La Tabla 34, muestra a detalle la vulnerabilidad SSL Self-Signed Certificate encontrada en el dispositivo con la IP 10.10.10.220

Tabla 34. SSL Self-Signed Certificate

Vulnerabilidad: SSL Self-Signed Certificate		**CVE:** -
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Baja
CVSS2: 6.4		**CVSS3:** -
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido. La vulnerabilidad se detecta en los puertos TCP: 10001 55443		
Impacto de la vulnerabilidad: Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.		
Remediación: Compre o genere un certificado SSL adecuado para este servicio.		

La Figura 24, muestra la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa), se identifica el certificado como autofirmado. Por medio de una máquina atacante, con el comando openssl s_client se establece una conexión SSL/TLS con el servidor remoto ubicado en la dirección IP 10.10.10.220 en el puerto 10001

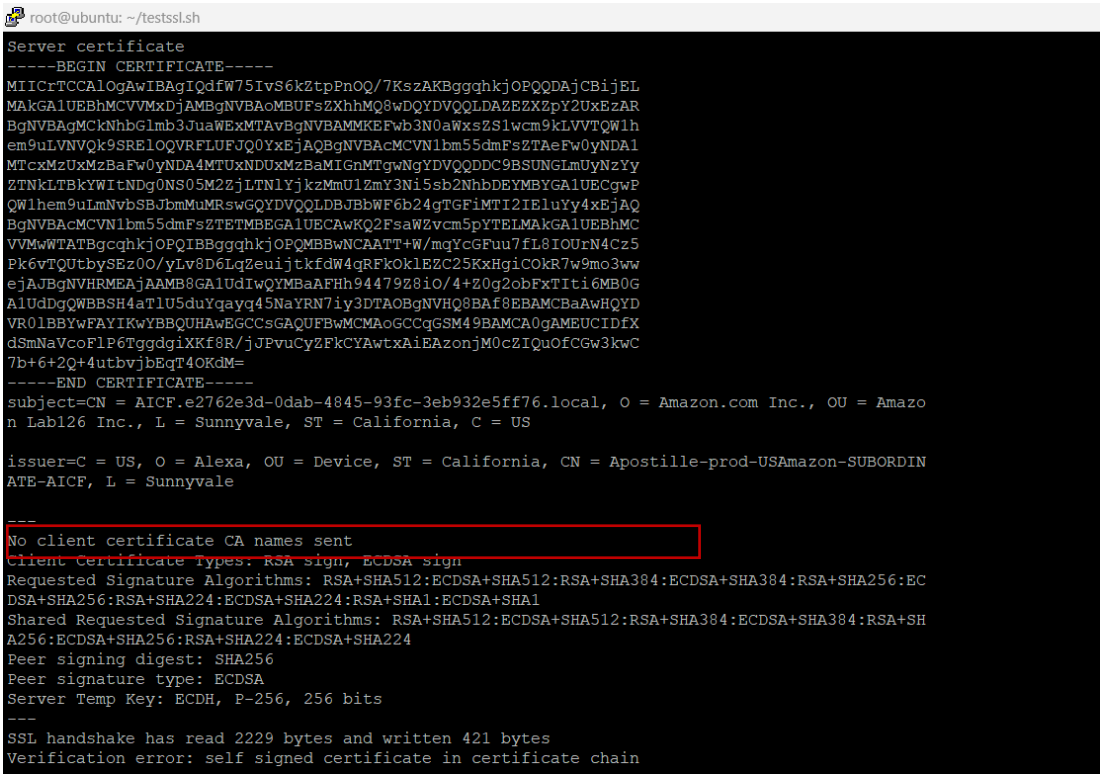


Figura 24. Evidencia de configuración y expedición del certificado SSL

De igual manera, se explota la vulnerabilidad en el TPOT, la Figura 25, detalla la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa), se observa que el certificado aparece como autofirmado. Por medio de una máquina atacante, con el comando openssl s_client se establece una conexión SSL/TLS con el servidor remoto ubicado en la dirección IP 10.10.10.217 en el puerto 443

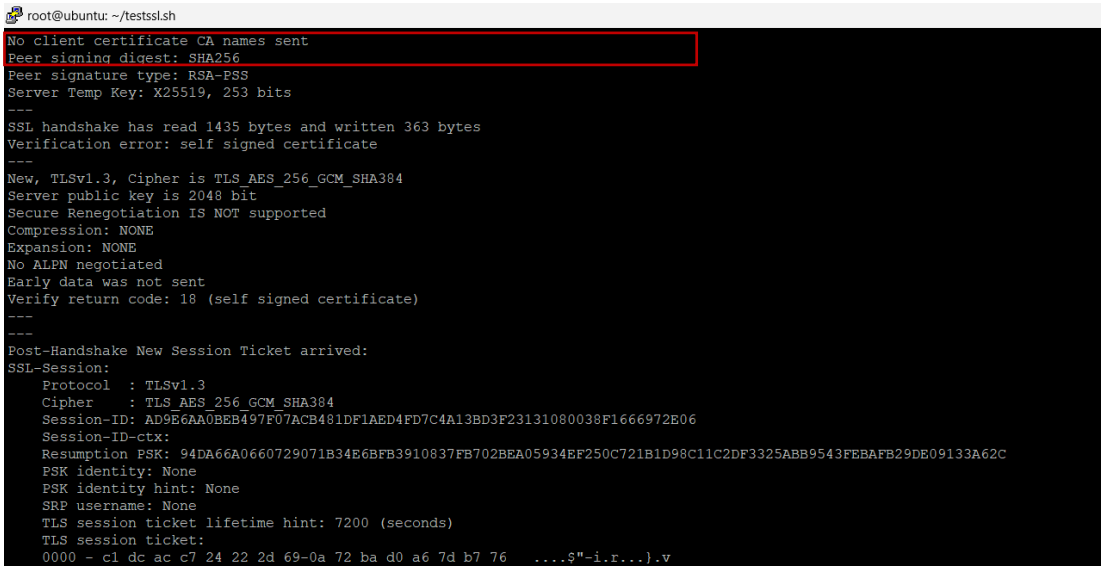


Figura 25. Evidencia de configuración y expedición del certificado SSL en TPOT

La Tabla 35 muestra a detalle la vulnerabilidad TLS Version 1.0 Protocol Detection encontrada en el dispositivo con la IP 10.10.10.220

Tabla 35. TLS Version 1.0 Protocol Detection.

Vulnerabilidad: TLS Version 1.0 Protocol Detection		**CVE:** -
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Bajo
CVSS2: 6.1		**CVSS3:** 6.5
IP Vulnerable: 10.10.10.220		
Descripción de vulnerabilidad: El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico. La vulnerabilidad se detecta en los puertos TCP: 10001		
Impacto de la vulnerabilidad: El servicio remoto acepta conexiones cifradas usando TLS 1.0. TLS 1.0 tiene un número de fallas en el diseño criptográfico. Implementaciones modernas de TLS 1.0 mitigar estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 son diseñado contra estos defectos y debe usarse siempre que sea posible.		
Remediación: Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.		

En la Figura 26, se identifica la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa), se observa que el certificado usa el cifrado TLS 1.0. Por medio de una máquina atacante, se ejecuta el script testssl.sh con el objetivo de realizar una evaluación de seguridad sobre el dispositivo que se encuentra en la dirección IP 10.10.10.220 y en el puerto 10001.

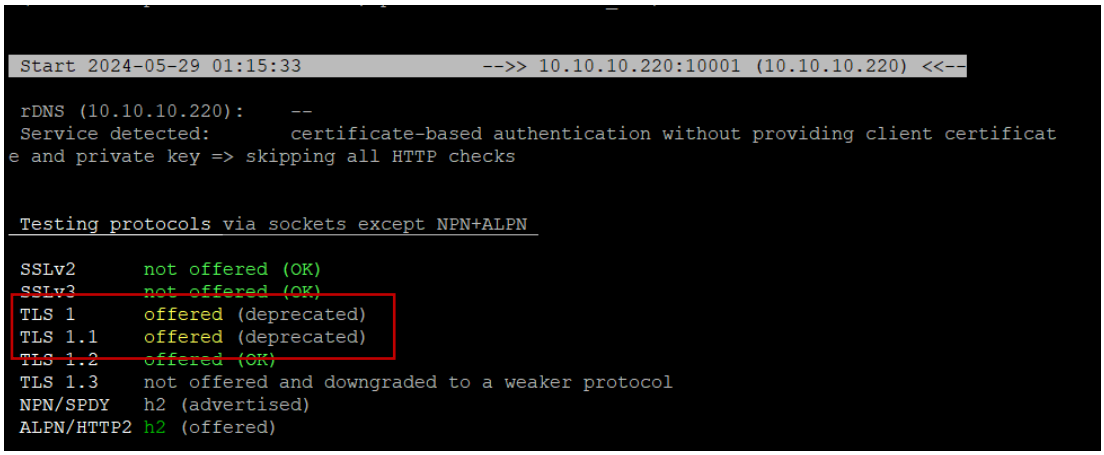


Figura 26. Evidencia de uso de cifrado TLSv1.0.

Así mismo, se explota la vulnerabilidad en el TPOT, como se observa en la Figura 27, en dónde la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa) muestra el certificado que usa cifrado TLS 1.0. Por medio de una máquina atacante, se ejecuta el script testssl.sh con el objetivo de realizar una evaluación de seguridad sobre el dispositivo que se encuentra en la dirección IP 10.10.10.217 y en el puerto 443.

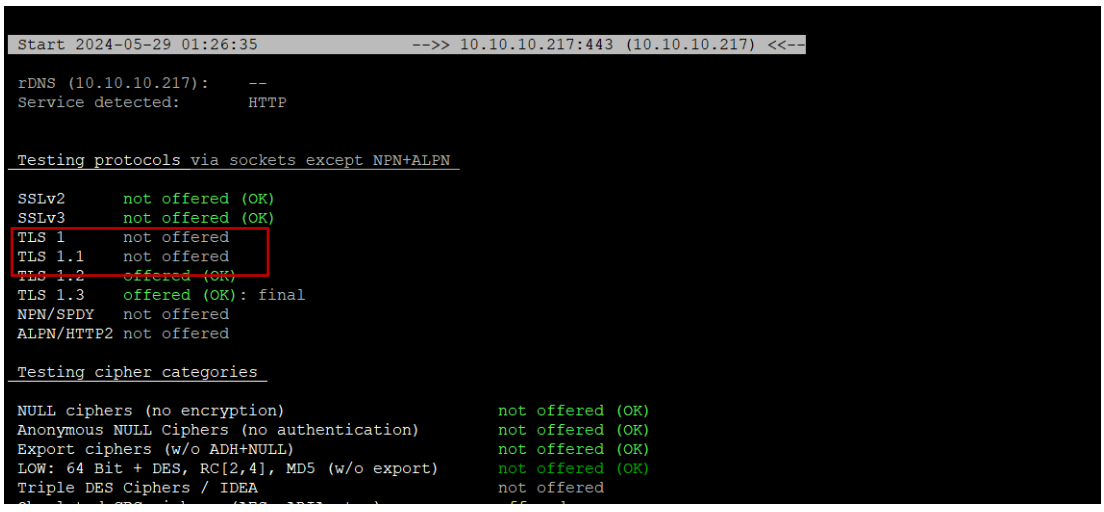


Figura 27. Evidencia de uso de cifrado TLSv1.0 en TPOT

La Tabla 36 muestra la vulnerabilidad SSL RC4 Cipher Suites Supported (Bar Mitzvah) encontrada en el dispositivo con la IP 10.10.10.220

Tabla 36. SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Vulnerabilidad: SSL RC4 Cipher Suites Supported (Bar Mitzvah)		**CVE: CVE-2013-2566 CVE-2015-2808**
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Bajo
CVSS2: 4.3		**CVSS3:** 5.9
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: "El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene errores al generar un flujo pseudoaleatorio de bytes para que se introduzca una amplia variedad de pequeños sesgos en la corriente, disminuyendo su aleatoriedad. Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP), el atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados. La vulnerabilidad se detecta en los puertos TCP: 10001		
Impacto de la vulnerabilidad: La presencia de RC4 en los conjuntos de cifrado de un sistema supone una amenaza considerable para la confidencialidad y la integridad de los datos.		
Remediación: "Reconfigure la aplicación afectada, si es posible, para evitar el uso de RC4 cifrados. Considere usar TLS 1.2 con suites AES-GCM sujetas al navegador y soporte de servidor web."		

En la Figura 28, se evidencia la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa), la evidencia de suites de cifrado identificada incluye detalles del RC4 basado en el protocolo SSL/TLS

```
---
No client certificate CA names sent
Client Certificate Types: RSA sign, ECDSA sign
Requested Signature Algorithms: RSA+SHA512:ECDSA+SHA512:RSA+SHA384:ECDSA+SHA384:RSA+SHA256:EC
DSA+SHA256:RSA+SHA224:ECDSA+SHA224:RSA+SHA1:ECDSA+SHA1
Shared Requested Signature Algorithms: RSA+SHA512:ECDSA+SHA512:RSA+SHA384:ECDSA+SHA384:RSA+SH
A256:ECDSA+SHA256:RSA+SHA224:ECDSA+SHA224
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 2229 bytes and written 421 bytes
Verification error: self signed certificate in certificate chain
---
New, TLSv1.2, Cipher is ECDHE-ECDSA-AES256-GCM-SHA384
Server public key is 256 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-ECDSA-AES256-GCM-SHA384
    Session-ID:
    Session-ID-ctx:
    Master-Key: 468E89B1BA7D60591AC1CF786EB4B715B5C57F991D5A03AA1BF030B67A8F4B3794B6DC2793B0D
1CCC02E660EE5734FEA
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1716967117
    Timeout   : 7200 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
    Extended master secret: yes
---
```

Figura 28. Evidencia de suit de cifrado identificados

De igual manera, se explota la vulnerabilidad en TPOT, en la Figura 29, se evidencia la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa), la evidencia de suites de cifrado identificada incluye detalles del RC4 basado en el protocolo SSL/TLS

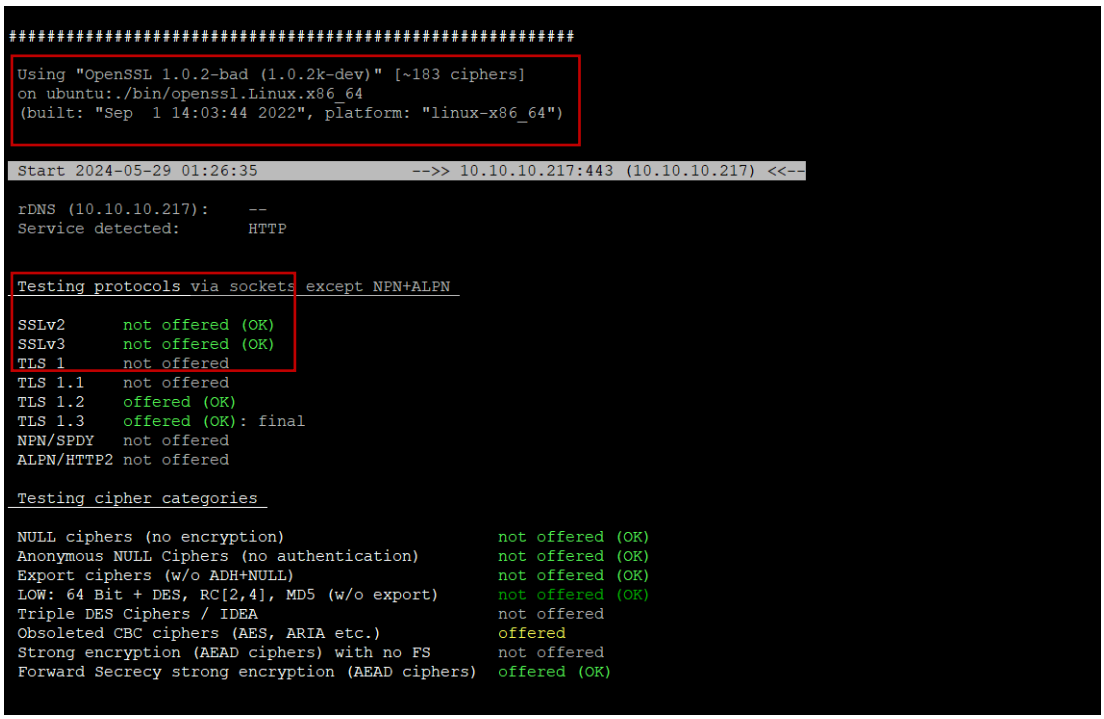


Figura 29. Evidencia de suit de cifrado identificados en TPOT

La Tabla 37, muestra a detalle la vulnerabilidad TLS Version 1.1 Protocol Detection encontrada en el dispositivo con la IP 10.10.10.220

Tabla 37. TLS Version 1.1 Deprecated Protocol

Vulnerabilidad: TLS Version 1.1 Deprecated Protocol		**CVE:** CVE-2020-7061, CVE-2020-7062, CVE-2020-7063
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Bajo
CVSS2: 6.1		**CVSS3: 6**.5
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: El servicio remoto acepta conexiones cifradas usando TLS 1.1. TLS 1.1 carece de soporte para las actualizaciones actuales y recomendadas. Cifrados que admiten cifrado antes del cálculo MAC y modos de cifrado autenticados como GCM no se puede utilizar con TLS 1.1 La vulnerabilidad se detecta en los puertos TCP: 10001		
Impacto de la vulnerabilidad: -El uso de TLS 1.1 en el puerto TCP 10001 representa un riesgo significativo para la seguridad de las comunicaciones, la conformidad regulatoria y la confianza del usuario.		
Remediación: Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.		

En la Figura 30, se evidencia la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa), se observa el certificado con el uso de cifrado TLS 1.1. Por medio de una máquina atacante, se ejecuta el script testssl.sh con el objetivo de realizar una evaluación de seguridad sobre el dispositivo que se encuentra en la dirección IP 10.10.10.220 y en el puerto 10001.

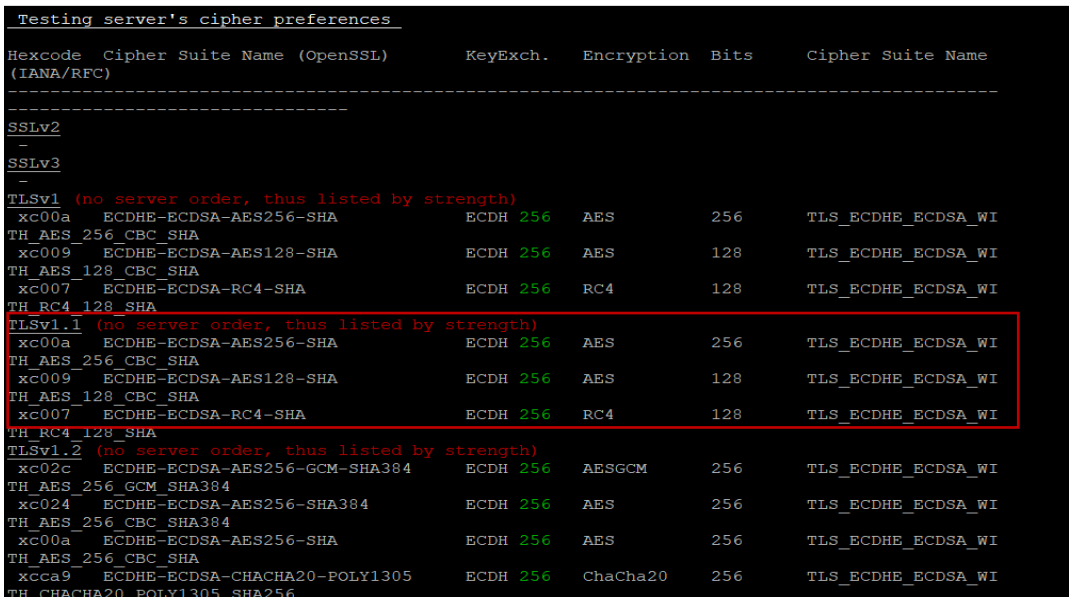


Figura 30. Evidencia de uso de cifrado TLSv1.1.

Se explota la misma vulnerabilidad en el TPOT, en la Figura 31, se evidencia la explotación de la vulnerabilidad detectada en el dispositivo echo dot (Alexa), se identifica el certificado con el uso de cifrado TLS 1.1. Por medio de una máquina atacante, se ejecuta el script testssl.sh con el objetivo de realizar una evaluación de seguridad sobre el dispositivo que se encuentra en la dirección IP 10.10.10.217 y en el puerto 443.

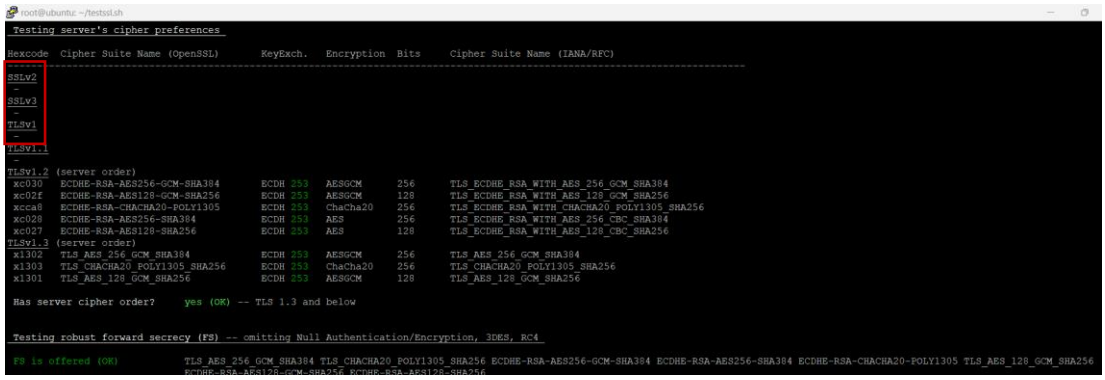


Figura 31. Evidencia de uso de cifrado TLSv1.1 en TPOT.

c. Hacking Network Wireless

- ***FASE 1.*** Identificación

El ataque se ejecuta con una tarjeta WiFi en la máquina atacante con Kali Linux. Primero, se verifica que la tarjeta esté en modo Managed antes de iniciar el ataque, como se muestra en la Figura 32.

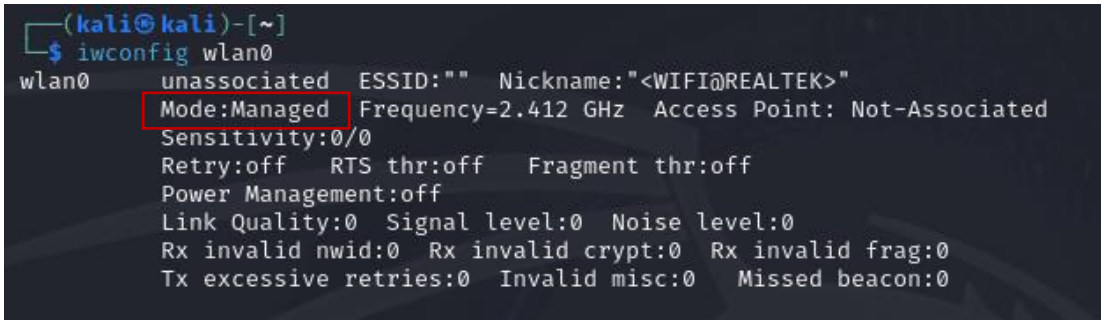


Figura 32. Verificación de la tarjeta WiFi

- ***FASE 2.*** Ejecución

Desde la máquina Kali Linux, se realiza el ataque WPS Pixie-Dust, como se muestra en la Figura 33, a continuación, se detalla el proceso para este ataque:

1. El comando wifite --kill se ejecuta en la terminal de Kali Linux, iniciando la herramienta Wifite versión 2.7.0. Wifite es un auditor inalámbrico diseñado para automatizar la auditoría de redes WiFi.

2. Wifite detecta y finaliza dos procesos conflictivos:

    - NetworkManager se detiene usando el comando systemctl stop NetworkManager.

    - El proceso wpa_supplicant con el PID 2117 también se termina.

3. Configuración de la interfaz inalámbrica:

    - La interfaz inalámbrica wlan0 con el controlador 88XXau (TP-Link AC600 wireless Realtek RTL8811AU [Archer T2U Nano]) se selecciona.

- Wifite habilita el modo monitor en wlan0, lo cual se confirma con el mensaje "enabled!".

4. Wifite escanea y muestra las redes WiFi-disponibles, listadas con los siguientes detalles:

    - NUM: Número de identificación de la red.
    - ESSID: Nombre de la red.
    - CH: Canal de la red.
    - ENCR: Tipo de encriptación (WPA, WPA2, etc.).
    - PWR: Potencia de la señal.
    - WPS: Indica si WPS está habilitado.
    - CLIENT: Número de clientes conectados a la red.

5. La red seleccionada para el ataque es YULISA-HOME (número 7 en la lista), con WPS habilitado.

    - El ataque comienza apuntando a la dirección MAC B8:69:F4:49:B5:45 de YULISA-HOME.
    - Wifite utiliza un ataque conocido como "WPS Pixie-Dust", mostrando tiempos estimados de espera y ejecución:
    - Espera de 5 minutos para que el objetivo aparezca.
    - Después de 4 minutos y 56 segundos, Wifite comienza a enviar mensajes Pixiewps y a ejecutar el ataque Pixie-Dust.



Figura 33. Escaneo de redes cercanas para realizar ataque

- ***FASE 3.*** Verificación

La Figura 34, muestra la verificación del ataque a la red, descubriendo la contraseña de la red, a continuación, se detalla el proceso para descubrir la misma.

1. Análisis del archivo de handshake capturado:

    - La herramienta tshark se utiliza para analizar el archivo .cap y confirmar que contiene un handshake válido para la dirección MAC 00:0b:82:e9:57:f5.

- Posteriormente, aircrack también confirma que el archivo .cap contiene un handshake válido para la misma dirección MAC.

2. Crackeo del handshake WPA:

   - Se ejecuta aircrack-ng con un archivo de lista de palabras (wordlist-probable.txt) para intentar descifrar el handshake WPA.

   - El proceso de crackeo comienza mostrando un avance del 0.01% y una ETA de 4 minutos y 30 segundos a una velocidad de 753.4 kps.

   - El handshake WPA se crackea exitosamente, revelando la clave PSK: admin1234.

3. Información del punto de acceso:

   - BSSID del punto de acceso: 00:08:82:E9:57

   - Encriptación: WPA.

   - Archivo de handshake: hs/handshake_Piso2_00-0B-82-E9-57-F5_2024-06-19T15-49-08.cap.

   - Clave PSK (contraseña): admin1234.

4. Finalización del proceso:

   - El ataque a 1 objetivo se completa y el proceso termina, indicando que la interfaz permanece en modo monitor.

   - Para deshabilitar el modo monitor, se sugiere usar el comando airmon-ng stop wlan0.

   - Se menciona que se puede reiniciar NetworkManager cuando se termine, utilizando el servicio NetworkManager.

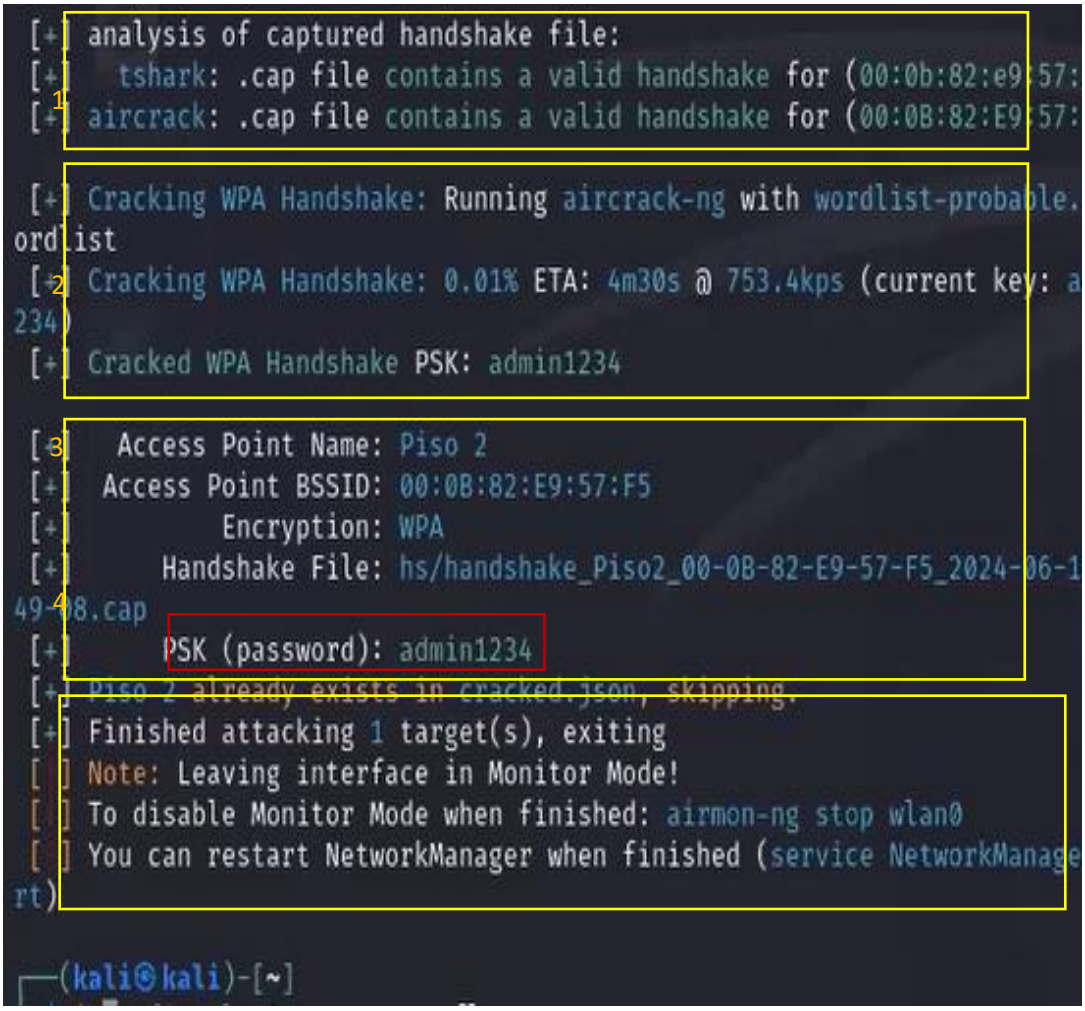


Figura 34. verificación del ataque a la red

Como resultado, se obtuvo la contraseña de la red del hogar, "admin1234", confirmando que el ataque para descubrir la contraseña de la red WiFi fue exitoso, permitiendo así el acceso no autorizado a la red del hogar.

d. Pruebas de denegación de servicio

La ejecución de una prueba de DoS a los dispositivos IoT, se realiza siguiendo las siguientes fases: identificación, ejecución y verificación.

Para identificar la información como los servicios y puertos de un dispositivo, existen varias herramientas disponibles, a continuación, en la Tabla 38, se muestra una comparativa entre Zenmap, Nmap, Hercules y Wireshark, para elegir aquellas que más se adapten a las necesidades en las pruebas pentesting.

Tabla 38. Comparativa de herramientas para identificación y análisis.

Características	Zenmap	Nmap	Hercules	Wireshark
Facilidad de Uso	Alta, interfaz gráfica intuitiva	Moderada, basado en línea de comandos	Moderada, interfaz gráfica básica	Moderada, requiere conocimientos sobre análisis de paquetes
Capacidades de Detección de Puertos	Excelente, interfaz gráfica para Nmap	Excelente, herramienta base de Zenmap	Limitada, centrado en pruebas de red	Limitada, no está diseñado específicamente para escaneo de puertos
Identificación de Servicios	Excelente, basado en Nmap	Excelente, detallada identificación de servicios	Básica, enfocado en pruebas de conectividad	Limitada, centrado en análisis de tráfico
Escaneo de Red	Excelente, soporta múltiples tipos de escaneo	Excelente, muy configurable	Básica, pruebas de conectividad y red	Limitada, análisis pasivo
Reportes y Análisis	Buena, exportación de resultados en diferentes formatos	Moderada, requiere scripts adicionales	Básica, centrado en resultados de prueba	Excelente, análisis profundo de paquetes
Interfaz de Usuario	Gráfica, fácil de usar	Línea de comandos, poderosa pero menos intuitiva	Gráfica, básica y funcional	Gráfica, compleja y detallada
Costo	Gratuito	Gratuito	Gratuito	Gratuito

En base a la comparativa, el uso combinado de Zenmap, Hercules y Wireshark proporciona un enfoque para aprovechar las fortalezas de cada herramienta. Zenmap, con su interfaz gráfica intuitiva, facilita el escaneo de puertos y la identificación de servicios. Hercules, aunque más limitado en escaneo de puertos, complementa las pruebas de conectividad y red con una interfaz gráfica. Wireshark, se usa para el análisis del tráfico de red.

- ***FASE 1.*** Identificación

1. Se procede con un mapeo a fin de identificar el dispositivo utilizando la herramienta Zenmap. Este proceso se inicia mediante la especificación de la dirección IP del dispositivo IoT, situada en el segmento de red 10.10.10.236.

Una vez iniciado el escaneo, se observa en la Figura 35, que el mapeo muestra el servicio IRC con el puerto 6668/TCP abierto

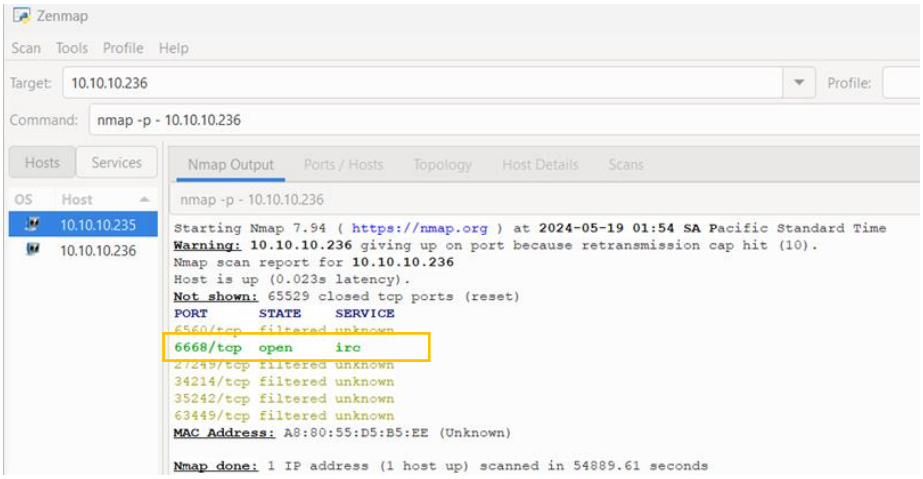


Figura 35. Mapeo de identificación

2. Con la herramienta Hércules se conecta el dispositivo identificado para verificar que este tenga conexión mediante TCP.

Con el fin de corroborar la disponibilidad de acceso al dispositivo en cuestión, por medio de TCP por el puerto 6668, como se muestra en la Figura 36. Mediante la evaluación de la conectividad se establece la capacidad de interactuar de manera efectiva con el dispositivo objetivo que en este caso es el interruptor de luz inteligente.

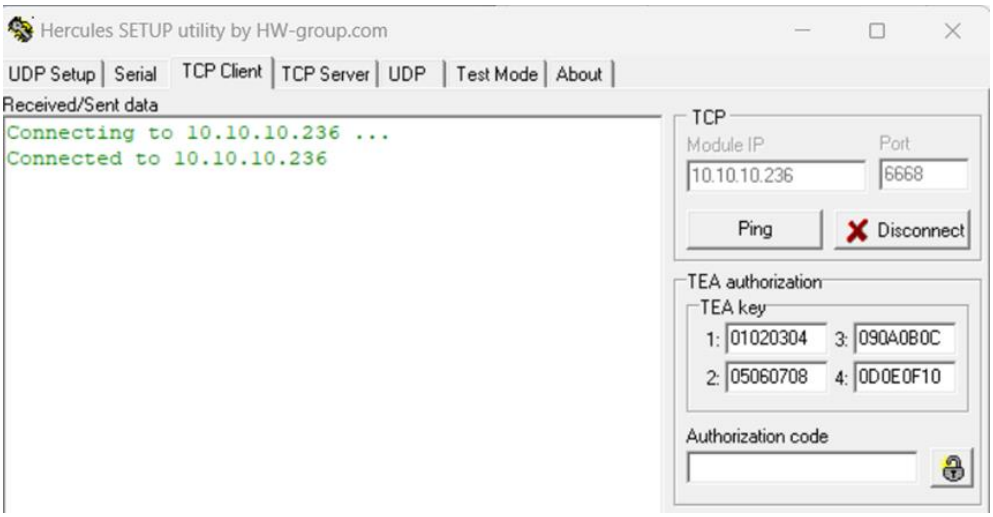


Figura 36. Acceso al dispositivo IoT con Hércules

- ***FASE 2.*** Ejecución

1. Se ejecuta el comando hping3 –syn –rand-source –flood -p 6668 10.10.10.236 desde la máquina atacante como se muestra en la Figura 37.

Este comando envía un flujo continuo de paquetes SYN con direcciones de origen aleatorias hacia el puerto 6668 del dispositivo con la dirección IP 10.10.10.236, simulando un ataque de denegación de servicio (DoS) con el objetivo de evaluar la resiliencia del dispositivo frente a tales amenazas.

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 --syn --rand-source --flood -p 6668 10.10.10.236
HPING 10.10.10.236 (eth0 10.10.10.236): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figura 37. Ataque dirigido

2. Se corrobora el tráfico generado por el ataque mediante Wireshark, con ipaddr == 10.10.10.236 && TCP.

La herramienta de análisis de red documenta cada paquete SYN enviado al puerto 6668 del dispositivo con la dirección IP 10.10.10.236 como se muestra en la Figura 38, proporcionando una representación detallada del ataque y permitiendo una evaluación exhaustiva del impacto y la respuesta del dispositivo ante la simulación de una amenaza de denegación de servicio (DoS).

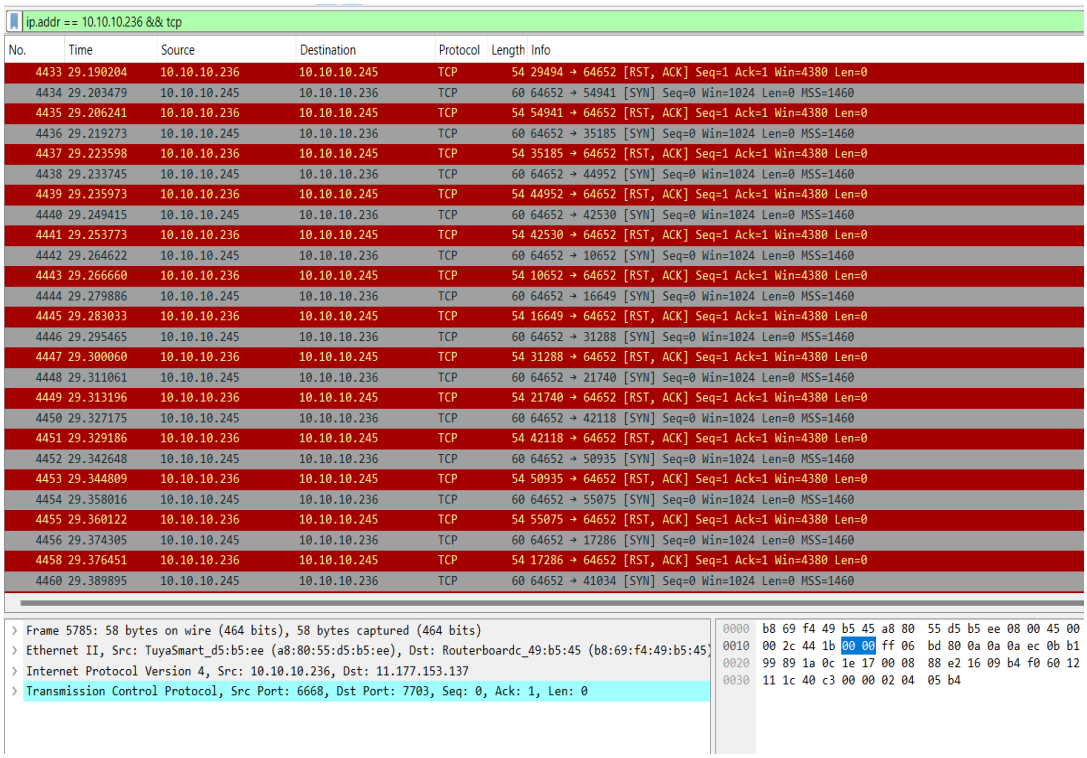


Figura 38. Captura del tráfico generado por el ataque

- ***FASE 3.*** Verificación

1. Mediante Wireshark se verifica el tráfico en el puerto tcp port == 6668.

Se observa que la dirección IP 10.10.10.236 emplea el protocolo TCP a través del puerto 6668 como se muestra en la Figura 39. Esta captura proporciona una visión detallada del tráfico de red asociado al dispositivo, permitiendo observar el comportamiento del ataque.

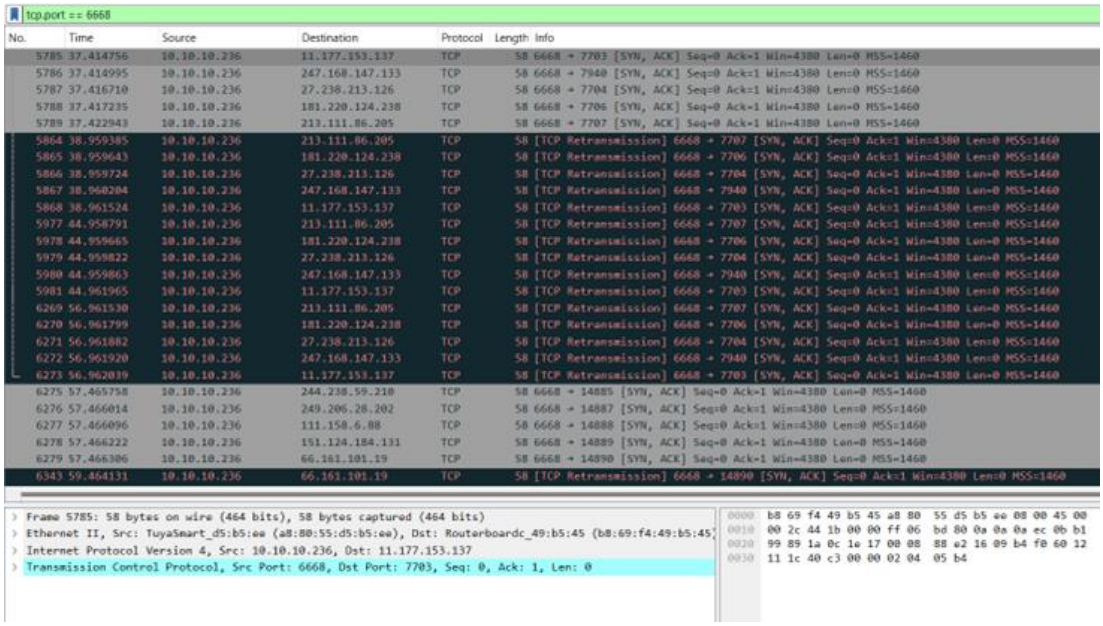


Figura 39. Captura de trama en IP 10.10.10.236

2. Con la herramienta Hércules se conecta el dispositivo identificado para verificar que este tenga conexión mediante TCP, como se muestra en la Figura 40.

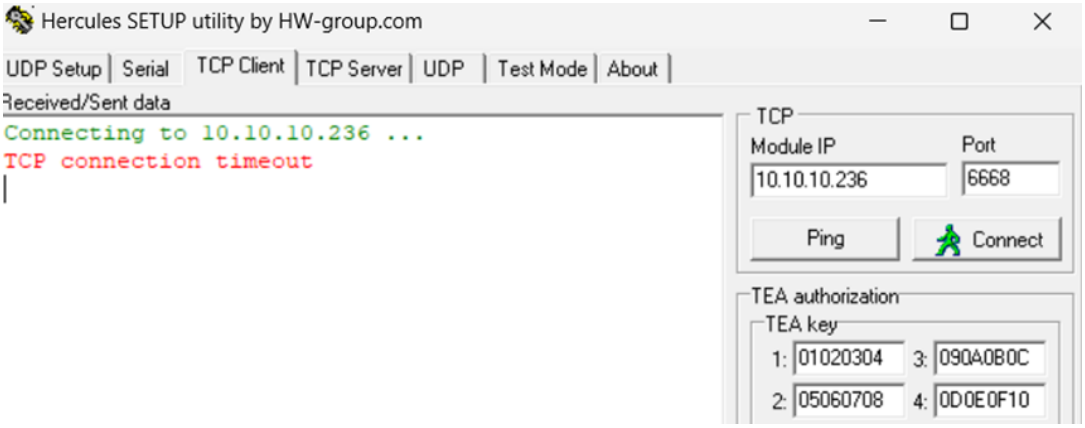


Figura 40. Resultado del ataque

Como resultado, se observa que, al intentar establecer una nueva conexión mediante el protocolo TCP utilizando la herramienta Hércules y la dirección IP del dispositivo, la conexión no se establece. Cabe destacar que, durante la ejecución de este ataque, el dispositivo no muestra ninguna información ni emite alertas de intrusión, lo que indica una ausencia de mecanismos de detección o respuesta ante el ataque DoS por inundación de paquetes SYN.

e. Control del dispositivo IoT desde LAN

Teniendo en cuenta el funcionamiento de los dispositivos IoT, se procede a controlar el dispositivo desde la LAN.

- ***FASE 1.*** Identificación

1. A través de la utilización de Wireshark, se identifica y captura el tráfico de datos correspondiente al dispositivo IoT

Esta captura permite un análisis detallado de las comunicaciones del dispositivo, proporcionando información sobre su comportamiento y los protocolos utilizados, lo que es fundamental para evaluar la seguridad y el funcionamiento del dispositivo en el entorno de red. Se identifica que se trata del sensor de contacto para puertas y ventanas con la IP 10.10.10.230 que se muestra en la Figura 41.

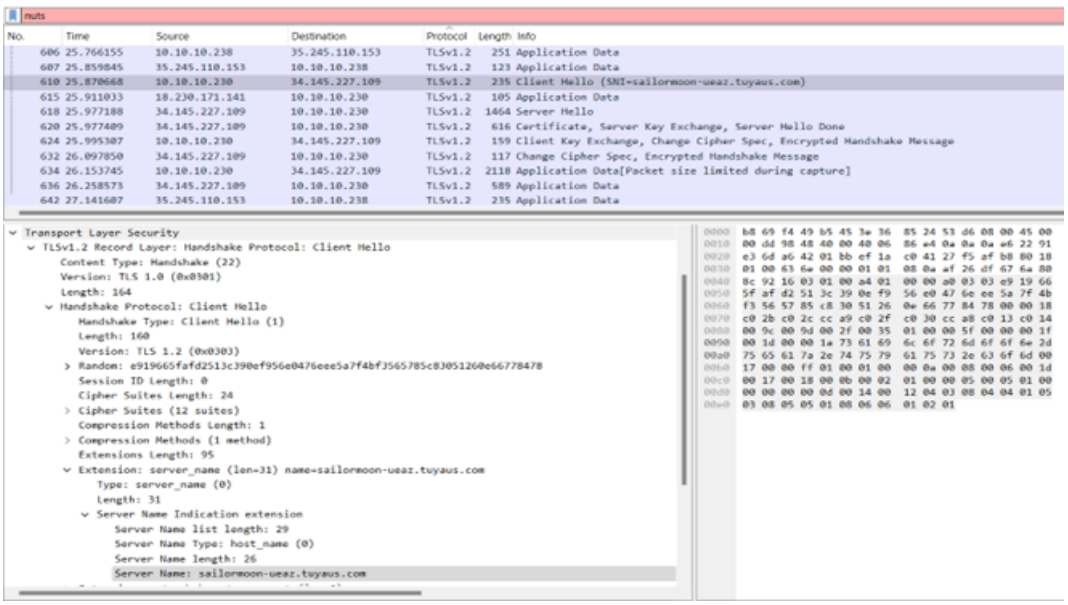


Figura 41. Captura para análisis detallado de las comunicaciones del dispositivo

- ***FASE 2.*** Ejecución

Para controlar los dispositivos IoT desde la red es necesario incluir la siguiente información:

- Dirección: Dirección de red (IPv4) del dispositivo, por ejemplo, 10.0.1.100.
- ID del Dispositivo: Identificador único del dispositivo Tuya.
- Versión: Versión del protocolo Tuya utilizada (3.1, 3.2, 3.3, 3.4 o 3.5).
- Clave Local: Clave de seguridad necesaria para acceder al dispositivo Tuya. Consulte el Asistente de Configuración para obtener estas claves.

1. A través de un script desarrollado en Python, se puede obtener los parámetros requeridos para el control, como se observa en la Figura 42, es importante mencionar, que la clave local no se puede obtener por la versión gratuita de Tuya.



Figura 42. Script para tener el control del dispositivo

- ***FASE 3.*** Verificación

La Figura 43 muestra la ejecución del script diseñado para el control y monitoreo del dispositivo.

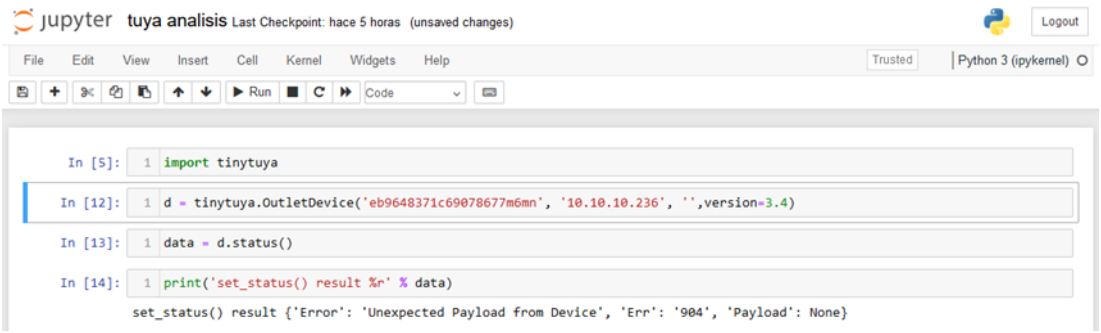


Figura 43. Verificación del control y monitoreo del dispositivo

Como resultado de este ataque, se observa que existe un error, ya que no se dispone de la clave de seguridad necesaria para acceder al dispositivo Tuya. Esta falta de acceso subraya la importancia de contar con medidas de autenticación robustas para proteger dispositivos IoT contra accesos no autorizados y ataques potenciales.

3.11 Resultados de la Honeynet

3.11.1 TPOT

Se ha desarrollado e implementado una Honeynet por medio de TPOT, que es una plataforma multi-honey configurado en modo estándar e incluye a ConPot y CitrixHoneypot, que son honeypots específicos para IoT. Esta Honeynet ha sido configurada para capturar tráfico de red, registros de actividad y cualquier intento de ataque o intrusión. TPOT ha permitido la identificación de múltiples riesgos, vulnerabilidades y amenazas en el sistema IoT, los más importantes que se halla posterior al análisis de vulnerabilidades es los CVE, estos tratan de un proyecto de MITRE que asigna indicadores únicos a las debilidades y errores de seguridad de software y firmware.

Por medio de una máquina atacante, se utiliza el comando openssl s_client -connect 10.10.10.217:443 para establecer una conexión SSL/TLS con el servidor en la

dirección IP 10.10.10.217.38 en el puerto 443, permitiendo inspeccionar el certificado del servidor y verificar su validez como se muestra en la Figura 44. Este proceso es útil para detectar configuraciones incorrectas o vulnerabilidades en la seguridad SSL/TLS del servidor. Aunque, generalmente no causa una carga significativa en el dispositivo, su uso repetido debe manejarse con cuidado para evitar posibles impactos en el rendimiento.

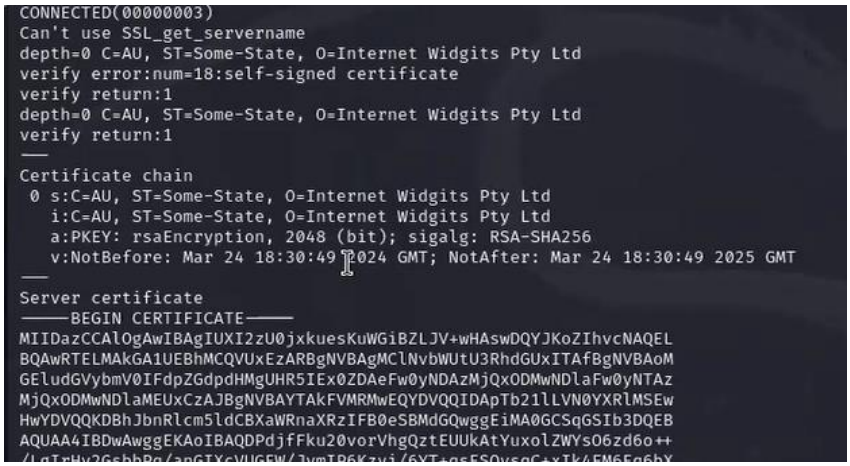


Figura 44. Conexión SSL/TLS con el servidor en el puerto 443

A través de una máquina atacante, se utiliza el comando ./testssl.sh 10.10.10.217:443 para iniciar una evaluación de seguridad SSL/TLS en el servidor ubicado en la dirección IP 10.10.10.217 y el puerto 443. Este comando permite realizar un análisis exhaustivo del estado de la configuración SSL/TLS del servidor, incluyendo la inspección del certificado SSL y la verificación de su validez, tal como se muestra en la Figura 45.

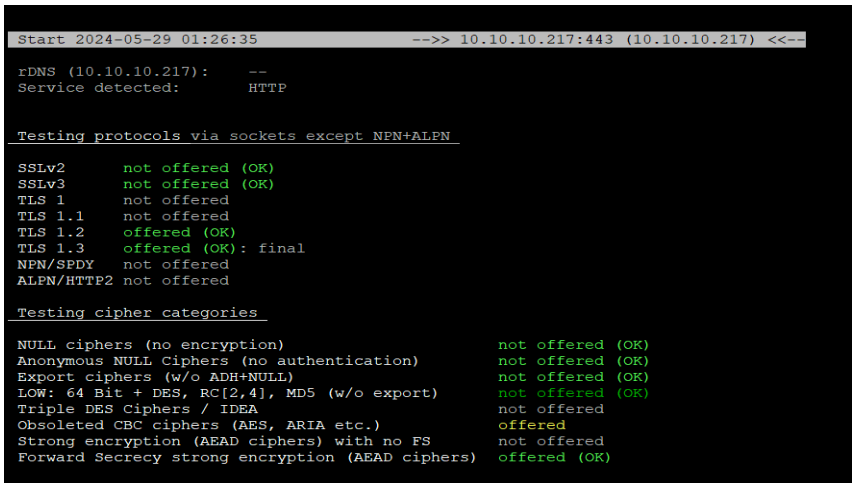


Figura 45. Conexión SSL/TLS para inspección del certificado SSL

Se configura TPOT para que muestre los ataques capturados por ConPot y CitrixHoneypot. La Figura 46, muestra que Kibana detecta el CVE-2015-0204 CVE-2015-1637 desde la IP 10.10.10.242.

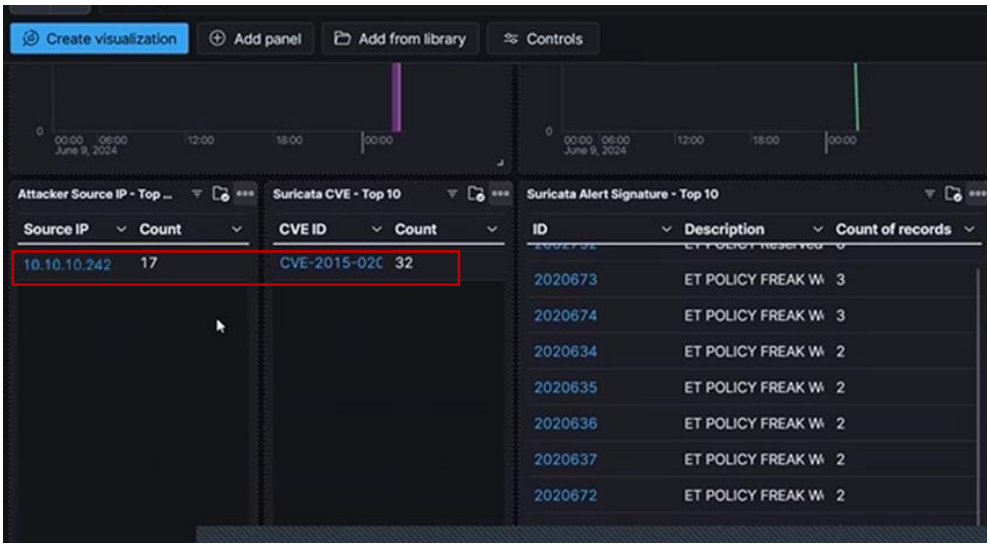


Figura 46. Captura de CVE en TPOT

La Figura 47, muestra que por medio de kibana, el TPOT registra 4354 eventos, entre estos se registra ataques al puerto 10001, que se encontró vulnerable con el análisis realizado a los dispositivos IoT por medio de Nessus.

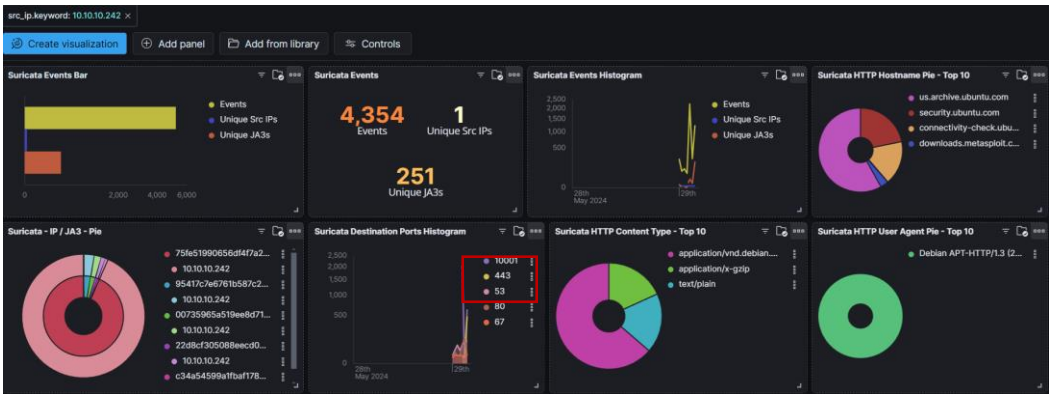


Figura 47. Registro de ataques a TPOT

3.11.2 Implementación de Honeypot de baja interacción para detección de ataque de DoS TCP SYN Flooding con Python

Se ha implementado un honeypot de baja interacción específicamente diseñado para la detección de ataques de Denegación de Servicio (DoS) TCP SYN Flooding

utilizando Python. Este honeypot es capaz de identificar patrones de tráfico característicos de un ataque SYN Flood, donde un atacante envía una serie de solicitudes SYN sin completar el proceso de enlace de tres vías, saturando el puerto objetivo y provocando que el sistema se vuelva inoperante.

La Figura 48, muestra la ejecución de un ataque de inundación TCP SYN (SYN Flood) utilizando la herramienta hping3 en un entorno Kali Linux. El comando sudo hping3 --syn --rand-source --flood -p 6668 10.10.10.210 inicia un ataque en el que se envían múltiples paquetes SYN al puerto 6668 de la dirección IP 10.10.10.210. La opción --syn especifica que se enviarán paquetes SYN, --rand-source indica que se usarán direcciones IP de origen aleatorias, y --flood activa el modo de inundación para enviar los paquetes lo más rápido posible.

El resultado es un flujo constante de solicitudes SYN al destino, abrumando su capacidad de respuesta y potencialmente llevando al sistema a un estado de denegación de servicio (DoS), donde el servidor se vuelve inoperante debido al alto volumen de solicitudes incompletas.

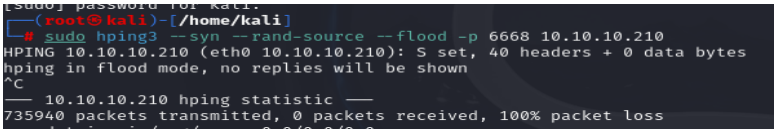


Figura 48. Ataque DoS TCP SYN Flooding desde Kali Linux

En la Figura 49, se muestra el resultado de la captura y registro de solicitudes maliciosas a través del puerto 6668/TCP. Se observa que tanto el puerto como la dirección IP de origen varían, indicando la utilización de direcciones IP aleatorias en el ataque.

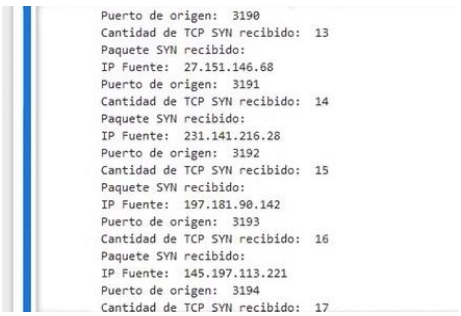


Figura 49. Captura y Registro de solicitudes maliciosas por medio del puerto 6668/TCP

La Figura 50, muestra la captura de inundación de paquetes utilizando la herramienta Wireshark, los cuales se envían a través del puerto 6668/TCP hacia la dirección IP 10.10.10.210, que corresponde al honeypot.

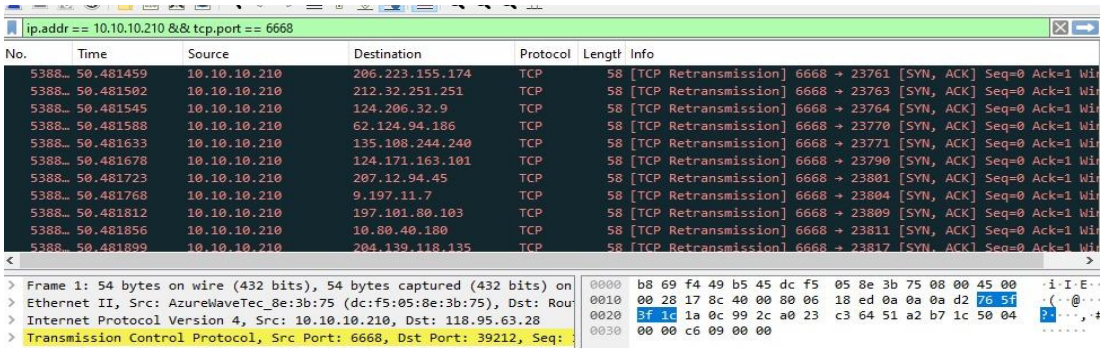
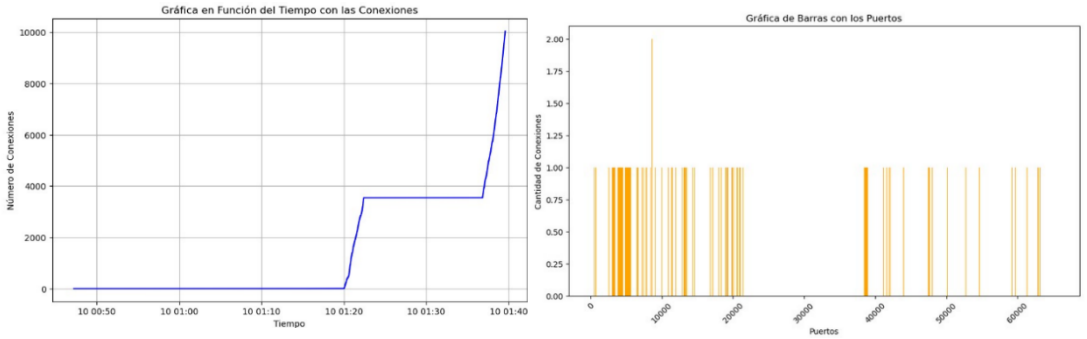


Figura 50. Inundación TCP SYN en honeypot

La Figura 51, muestra de manera gráfica el resultado del ataque DoS TCP SYN Flooding, en la subfigura (a) se encuentra la gráfica de conexiones con las diferentes IP en función del tiempo y en la subfigura (b), la gráfica de barras que indica los diferentes puertos utilizados para enviar la inundación de paquetes.



(a) Gráfica de conexiones en función del tiempo

(b) Gráfica de barras de los puertos

Figura 51. Registro de solicitudes maliciosas por medio del puerto 6668/TCP

Se observa como resultado, los datos capturados, por medio de las respectivas gráficas, se facilita una comprensión más profunda del impacto y comportamiento del ataque. En (a) se muestra que en un período de aproximadamente 10 segundos se producen más de 3,000 conexiones, lo que evidencia la magnitud del ataque. Además, en (b) se identifican los distintos puertos utilizados en cada conexión que van desde el puerto 0 hasta el 60000, proporcionando una visión detallada de los vectores de ataque empleados.

3.12 Gestión de riegos

Este plan establece las estrategias y acciones específicas que se implementarán para mitigar, transferir, aceptar o evitar los riesgos identificados en el proceso de evaluación de riesgos en el sistema IoT para el hogar. El resultado del análisis y la gestión de riesgos tiene como objetivo general garantizar la integridad, confidencialidad y disponibilidad de los datos, así como la protección de la privacidad de los usuarios y la seguridad de los dispositivos IoT en entornos domésticos, mediante la implementación de medidas de seguridad robustas, actualizaciones periódicas, controles de acceso adecuados, educación y concienciación de los usuarios, y una evaluación continua de riesgos y vulnerabilidades.

3.12.1 Matriz de riesgos

Para el desarrollo de una gestión de riesgos efectiva, se elabora una matriz de riesgos que considera meticulosamente las vulnerabilidades identificadas. Esta matriz permite no solo la identificación y evaluación de las amenazas que pueden comprometer los activos del hogar, sino también la priorización de las áreas que requieren una atención inmediata.

a. Catálogo de amenazas

Se elabora un catálogo de amenazas, como se muestra en la Este catálogo de amenazas sirve como base para analizar y determinar cuáles de estas amenazas se tienen en el sistema IoT doméstico.

Tabla 39, con el fin de identificar y categorizar las posibles fuentes de riesgos. Este catálogo se basa en marcos de referencia como la NIST, en la ISO/IEC27001, en la CIS, en la GDPR, ITIL y OWASP IoT [62-65].

Proporcionando una base estructurada para el análisis de riesgos, permitiendo de esa manera una evaluación de las amenazas que podrían afectar al sistema IoT del hogar, facilitando la implementación de estrategias de mitigación adecuadas. Este catálogo de amenazas sirve como base para analizar y determinar cuáles de estas amenazas se tienen en el sistema IoT doméstico.

Tabla 39. Catálogo de amenazas [62-65].

Categoría	Amenaza	Descripción	Impacto	Medidas de Mitigación
Seguridad de los Datos	Acceso no autorizado	Personas no autorizadas acceden a datos sensibles.	Alto	Implementar controles de acceso robustos y autenticación multifactor.
Seguridad de los Datos	Pérdida de datos	Pérdida de datos críticos debido a fallos en el sistema o borrado accidental.	Medio	Realizar copias de seguridad periódicas y mantener sistemas de recuperación de datos.
Seguridad de los Datos	Ransomware	Malware que cifra los datos y exige un rescate para su liberación.	Alto	Mantener actualizado el software antivirus y educar a los usuarios sobre la identificación de correos electrónicos sospechosos.
Privacidad de las Personas	Robo de identidad	Uso indebido de la información personal para realizar fraudes.	Alto	Utilizar servicios de monitoreo de identidad y prácticas seguras de manejo de datos personales.
Privacidad de las Personas	Filtración de datos personales	Exposición de información personal debido a brechas de seguridad.	Alto	Implementar políticas de privacidad estrictas y encriptar datos sensibles.
Dispositivos IoT	Protocolos y comunicaciones no encriptadas	Fuga y acceso a la información que viaja en texto plano o sin encriptar	Medio	Verificar que los dispositivos IoT utilicen protocolos y comunicaciones encriptadas
Dispositivos IoT	Compromiso de dispositivo	Dispositivos IoT son controlados por atacantes para actividades maliciosas.	Alto	Actualizar regularmente el firmware y utilizar redes seguras.
Dispositivos IoT	Ataques DDoS	Saturación de dispositivos IoT mediante tráfico malicioso para dejarlos inoperativos.	Medio	Implementar soluciones de protección contra DDoS y segmentar la red.
Dispositivos IoT	Software y Firmware desactualizado	Explotación de vulnerabilidades debido a software y firmware obsoleto en los dispositivos IoT.	Alto	Actualizar firmware y software regularmente y realizar auditorías de seguridad.

b. Criterios de valoración

En el Anexo B, desde la Tabla B2 a la B5, se encuentran detallados los criterios de valoración que ayudan al desarrollo de la matriz de riesgos. Todos estos criterios de valoración son tomados del Instituto Nacional de Estándares y Tecnología (NIST) [63].

c. Mapa de calor

Para el mapa de calor, es necesario ponderar cuidadosamente la probabilidad como el potencial impacto o consecuencia. En el sistema IoT, se emplea una escala de valoración tomada del Instituto Nacional de Estándares y Tecnología (NIST), los criterios de valoración se muestran en el Anexo B, Tabla B5 [74].

Se incrementa el nivel de riesgo mediante la fórmula de Probabilidad multiplicada por Impacto/Consecuencia, facilitando una evaluación más robusta y precisa. A continuación, en la Tabla 40, se observa una descripción de la estrategia a tomar entorno al nivel de riesgo.

Tabla 40. Probabilidad x Impacto/Consecuencia [76].

Nivel de riesgo (Probabilidad x Impacto/Consecuencia)		Estrategia (Asumir, Mitigar, Transferir, Eliminar)
B	Zona de riesgo baja (1 - 2)	Asumir el riesgo
M	Zona de riesgo moderada (3 - 4 - 5 - 6 - 8 - 9 - 10)	Asumir el riesgo, mitigar
A	Zona de riesgo alta (12 -15 -16)	Asumir el riesgo, mitigar, transferir
E	Zona de riesgo extrema (20 - 25)	Mitigar el riesgo, mitigar, transferir, eliminar

La Tabla 41, muestra la Matriz de Calificación, Evaluación y Respuesta de los Riesgos, también conocida como Mapa de Calor, que permite una visualización clara y estructurada de las diferentes categorías de riesgo, proporcionando una base sólida para la toma de decisiones estratégicas para asumir, mitigar, transferir o eliminar el riesgo.

Tabla 41. Matriz de Calificación, Evaluación y Respuesta de los Riesgos [76].

		Impacto / Consecuencia				
		Insignificante (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Critico (5)**
Probabilidad	**Raro (1)**	**B(1)**	**B(2)**	**M(3)**	**M(4)**	**M(5)**
	Improbable (2)	**B(2)**	**M(4)**	**M(6)**	**M(8)**	**M(10)**
	Ocasional (3)	**M(3)**	**M(6)**	**M(9)**	**A(12)**	**A(15)**
	Frecuente (4)	**M(4)**	**M(8)**	**A(12)**	**A(16)**	**E(20)**
	Casi Seguro (5)	**M(5)**	**M(10)**	**A(15)**	**E(20)**	**E(25)**

d. Matriz de riesgos

En la Tabla 42, se identifican los riesgos considerando cuatro categorías principales: red, software, protocolo y credenciales. Posteriormente, se determinan los posibles riesgos del sistema IoT para el hogar en cada categoría, considerando las amenazas de la Tabla 39, catálogo de amenazas, los vectores de ataque y consecuencia se toman en cuenta en base a las consideraciones del sistema IoT doméstico y los criterios recomendados para la ciberseguridad de la NIST [76].

Este enfoque integral permite identificar y evaluar de manera detallada los diferentes puntos vulnerables del sistema, facilitando la implementación de medidas de mitigación adecuadas para garantizar la seguridad y privacidad en el entorno doméstico.

Tabla 42. Identificación de riesgos

ID	Riesgo	Amenaza	Vector de ataque	Consecuencia	Categoría
1	Acceso a la red	Acceso no autorizado	Puertos abiertos	Acceso a datos sensibles	Red
2	Versión de software/firmware desactualizado	Software y Firmware desactualizado	Software obsoleto	Explotación de vulnerabilidades	Software
3	Protocolos de comunicación no encriptados	Protocolos y comunicaciones no encriptadas	Protocolos no seguros	Acceso a información confidencial	Protocolo
4	Gestión inadecuada de credenciales	Acceso no autorizado Robo de identidad Filtración de datos personales	Gestión inadecuada de los datos	Acceso no autorizado a datos	Credenciales

Para la matriz de riesgos, se toma en cuenta los criterios de valoración, una vez identificados los riesgos, se valora el impacto en el sistema en base al Anexo B, Tabla B1, para cada una de las categorías, considerando la confidencialidad, integridad y disponibilidad. Para la valoración de la probabilidad de ocurrencia de los riesgos, se toma en cuenta la Tabla B4, del Anexo B, determinando si es frecuente, ocasional o raro.

Con los criterios de valoración de la Matriz de Calificación, Evaluación y Respuesta de los Riesgos Tabla 41, se calcula el riesgo inherente mediante la fórmula:

$$\textbf{Riesgo Inherente} = \textbf{impacto} * \textbf{probabilidad} \quad (1)$$

Para determinar si el riesgo inherente cualitativo es crítico, moderado o significativo, se toma en cuenta la Tabla 40, Probabilidad x Impacto/Consecuencia. La Tabla B2, del Anexo B, muestra las estrategias que se utiliza para valorar si los riesgos pueden ser mitigados, asumidos, evitados o transferidos. En resumen, se tiene la matriz de riesgos, como muestra la Tabla 43.

Tabla 43. Matriz de riesgos

ID	Riesgo	Valoración Impacto	Valoración Probabilidad	Riesgo Inherente Cuantitativo	Riesgo Inherente Cualitativo	Opciones de Tratamiento
1	Acceso a la red	Alto	Frecuente	16	Crítico	Mitigar
2	Versión de software/ firmware desactualizado	Medio	Ocasional	9	Significativo	Mitigar
3	Protocolos de comunicación no encriptados	Bajo	Raro	2	Moderado	Asumir
4	Gestión inadecuada de credenciales	Critico	Frecuente	20	Crítico	Transferir

3.12.2 Políticas y controles

a. Políticas

Las políticas de seguridad para el sistema IoT en el hogar, son fundamentales para garantizar la protección integral de los dispositivos y los datos personales, en el Anexo F, se encuentra cada una de las políticas. A continuación, se da una descripción breve de cada una de las políticas establecidas:

- ***Política de Contraseñas Seguras.*** establece la necesidad de utilizar contraseñas robustas y únicas para cada dispositivo

- ***Política de Actualización de Software.*** asegura que los dispositivos estén siempre protegidos contra vulnerabilidades conocidas.

- ***Política de Acceso y Autorización.*** garantiza que solo los usuarios autorizados puedan interactuar con los dispositivos IoT y acceder a la información sensible.

- ***Política de Privacidad de Datos.*** Asegura que los datos personales recopilados por los dispositivos sean tratados de manera transparente y conforme a las leyes de privacidad aplicables.

- ***Política de Monitoreo y Detección de Amenazas.*** establece la necesidad de implementar sistemas de monitoreo continuo para identificar posibles intrusiones o comportamientos anómalos.

- ***Política de Respuesta a Incidentes.*** define los procedimientos a seguir en caso de que se produzca una brecha de seguridad

- ***Política de Educación y Concientización.*** promueve la formación de los usuarios sobre prácticas seguras.

- ***Política de Evaluación de Riesgos y Cumplimiento.*** garantiza que se realicen evaluaciones periódicas de seguridad y se cumplan los requisitos legales y regulatorios pertinentes.

b. Controles

Resulta esencial implementar controles efectivos que aborden las áreas críticas, siguiendo tanto marcos normativos como prácticas recomendadas. En el Anexo G, se encuentra a detalle cada uno de los controles que van de la mano de los riesgos del sistema IoT doméstico. Los controles que aplican para el sistema IoT doméstico son:

- Firewall
- Actualización regular
- Encriptación
- Políticas de gestión

Para la seguridad de la red se toma en cuenta la normativa ISO/IEC 27001:2022 Anexo A.8.20-A.8.23 que controla los firewalls, además, se considera la directriz y política de firewall de la NIST SP 800-41 que es una guía específica para firewall [75-77].

Para el mantenimiento de sistemas, las actividades de detección y las actualizaciones regulares, se incluyen las normativas ISO/IEC 27001:2022 Anexo A.8.8-A.8.9 y A.8.19-A.8.20. Estas se centran en la gestión de vulnerabilidades técnicas, la gestión de la configuración, la instalación de software en sistemas operativos y la seguridad de redes. Además, se aplica la directriz NIST SP 800-40, que proporciona una guía específica para la gestión de parches y actualizaciones de software [76-77], [79].

La protección de datos utiliza la normativa ISO/IEC 27001:2022, Anexo A.8.3, A.8.10-A.8.13, A.8.24 y A.8.28-A.8.29, que abarcan la restricción de acceso a la información, eliminación segura de datos, enmascaramiento de datos, prevención de fuga de datos, copias de seguridad, y el uso de criptografía y codificación segura. Se aplican medidas preventivas para garantizar que la información se maneje de manera segura en todas las etapas de su ciclo de vida. La directriz NIST SP 800-57 proporciona una guía específica para la gestión de criptografía, asegurando que los algoritmos y métodos de encriptación utilizados sean robustos y actualizados [76-77], [80].

Para la gestión de seguridad, se toman en cuenta las normativas ISO/IEC 27001:2022 Anexo A.8.14, A.8.18, A.8.20 y A.8.22, que contemplan a la redundancia de las instalaciones de procesamiento de información, el uso de programas de utilidad privilegiados, la seguridad de redes y la segregación de redes. Se consideran las mejores prácticas y directrices de ITIL y COBIT, que proporcionan información para la gestión de servicios y el control de tecnología de la información [76-77].

3.13 Plan de tratamiento de riesgos

El desarrollo de un plan de tratamiento de riesgos específico para sistemas IoT en el hogar es indispensable, para garantizar un entorno seguro y confiable, donde la integridad y confidencialidad de la información personal se mantengan intactas, y los dispositivos conectados operen sin vulnerabilidades que puedan ser explotadas.

3.13.1 Proyectos del Plan de Tratamiento de Riesgos

La Tabla 44, presenta un resumen del plan de tratamiento de riesgos para el sistema IoT para el hogar:

Tabla 44. Resumen del Plan de Tratamiento de Riesgos

Riesgo	Medida	Descripción	Responsable	Fecha de Implementación	Estado
Acceso no autorizado a la red	Implementar firewall	Configurar firewall	Propietario del hogar/Administrador de red	Inmediato	Abierto
Versiones desactualizadas de software/firmware	Actualización regular	Implementar actualizaciones automáticas	Propietario del hogar/Proveedor de servicios	Mensual	Abierto
Protocolos de comunicación no encriptados	Implementar encriptación de extremo a extremo	Usar WPA3 y TLS	Propietario del hogar/Administrador de red	Inmediato	Abierto
Gestión inadecuada de credenciales	Gestión segura de credenciales	Usar gestor de contraseñas y MFA	Propietario del hogar/Proveedor de servicios	Inmediato	Abierto

Este plan se encuentra a detalle en el Anexo H, en dónde se tratan los cuatro riesgos: Acceso no autorizado a la red, Versiones desactualizadas de software/firmware, Protocolos de comunicación no encriptados, y Gestión inadecuada de credenciales encontrados en el sistema IoT doméstico.

a. Acceso no autorizado a la red

En la Tabla 45, se muestra el plan de tratamiento para el acceso no autorizado a la red.

Tabla 45. Acceso no autorizado a la red

Categoría	Descripción
Riesgo	Acceso no autorizado a la red doméstica.
Amenaza	Actores maliciosos obtienen acceso no autorizado a la red.
Vulnerabilidad	Puertos abiertos, contraseñas débiles y configuraciones de seguridad deficientes.
Consecuencia	Acceso a datos sensibles, instalación de malware, interrupción de servicios.
Tratamiento	Revisión de los controles definidos en el documento controles de Firewall para su implementación y socialización de las políticas de Monitoreo y Detección de Amenazas, Acceso y Autorización, que respalda el control indicado.

Categoría	Descripción
Medida	Implementar un firewall robusto y una VPN.
Beneficios	Mejora la seguridad de la red al controlar y monitorear todo el tráfico entrante y saliente, y protege las comunicaciones de red contra la interceptación y el acceso no autorizado.
Responsable	Propietario del hogar/Administrador de red.
Fecha de implementación	Inmediato.
Estado	Abierto.

- ***Descripción:***

Firewall: Configurar un firewall de última generación (Next-Generation Firewall, NGFW) que filtre el tráfico basado en reglas predefinidas y analice el contenido del tráfico en tiempo real, detectando y bloqueando amenazas avanzadas.

b. Versiones desactualizadas de software/firmware

En la Tabla 46, se desarrolla el plan de tratamiento para versiones desactualizadas de software/firmware

Tabla 46. Versiones desactualizadas de software/firmware

Categoría	Descripción
Riesgo	Vulnerabilidades en software/firmware debido a versiones desactualizadas.
Amenaza	Explotación de vulnerabilidades conocidas en software/firmware desactualizado.
Vulnerabilidad	Software y firmware obsoletos que no reciben parches de seguridad.
Consecuencia	Compromiso de dispositivos IoT, pérdida de control sobre dispositivos, acceso a datos personales.
Tratamiento	Revisión de los controles definidos en el documento controles de Actualización Regular para su implementación y socialización de las políticas de Monitoreo y Detección de Amenazas, Actualización de software, que respalda el control indicado.
Medida	Implementar un programa de actualización regular de software y firmware.
Beneficios	Reduce significativamente el riesgo de explotación de vulnerabilidades conocidas y mejora la resiliencia general de la red doméstica.
Responsable	Propietario del hogar/Proveedor de servicios.
Fecha de implementación	Mensual.
Estado	Abierto.

- ***Descripción:***

Sistema de Actualización Automática: Configurar todos los dispositivos IoT para que realicen actualizaciones automáticas del software y firmware. Asegurarse de que los dispositivos se actualicen automáticamente a las versiones más recientes disponibles tan pronto como se publiquen.

Gestión Centralizada de Actualizaciones: Utilizar una solución de gestión de dispositivos que permita centralizar y automatizar la distribución de actualizaciones a todos los dispositivos conectados.

c. Protocolos de comunicación no encriptados

En la Tabla 47, se desarrolla el plan de tratamiento para protocolos de comunicación no encriptados

Tabla 47. Protocolos de comunicación no encriptados

Categoría	Descripción
Riesgo	Intercepción de datos transmitidos sin encriptación.
Amenaza	Eavesdropping, Man-in-the-Middle (MitM) attacks.
Vulnerabilidad	Uso de protocolos de comunicación no seguros (por ejemplo, HTTP en lugar de HTTPS).
Consecuencia	Robo de información sensible, como credenciales y datos personales.
Tratamiento	Revisión de los controles definidos en el documento controles de Encriptación para su implementación y socialización de las políticas de Monitoreo y Detección de Amenazas, Evaluación de Riesgos y Respuesta a incidentes, que respalda el control indicado.
Medida	Implementar encriptación de extremo a extremo.
Beneficios	Protege la integridad y confidencialidad de los datos en tránsito, asegurando que los datos no puedan ser interceptados ni alterados por actores maliciosos.
Responsable	Propietario del hogar/Administrador de red.
Fecha de implementación	Inmediato.
Estado	Abierto.

- ***Descripción:***

Wi-Fi Security: Configurar la red Wi-Fi para utilizar el protocolo WPA3, que ofrece mejoras significativas en seguridad con respecto a WPA2, incluyendo una encriptación más fuerte y protección contra ataques de fuerza bruta.

TLS/SSL: Asegurar que todas las comunicaciones web utilicen HTTPS con TLS 1.2 o superior.

Implementar certificados SSL/TLS para todos los dispositivos y servicios web que se utilicen en el entorno doméstico.

d. Gestión inadecuada de credenciales

En la Tabla 48, se desarrolla el plan de tratamiento para protocolos de comunicación no encriptados

Tabla 48. Protocolos de comunicación no encriptados

Categoría	Descripción
Riesgo	Fuga de información debido a la gestión inadecuada de credenciales.
Amenaza	Robo de credenciales, ataques de phishing, ataques de fuerza bruta.
Vulnerabilidad	Uso de contraseñas débiles, reutilización de contraseñas, falta de rotación de contraseñas.
Consecuencia	Acceso no autorizado a cuentas y dispositivos, pérdida de datos sensibles, compromisos de privacidad.
Tratamiento	Revisión de los controles definidos en el documento controles de Políticas de gestión para su implementación y socialización de las políticas de Acceso y Autorización, Contraseñas seguras, y Privacidad de datos que respalda el control indicado.
Medida	Implementar una gestión segura de credenciales.
Beneficios	Reduce significativamente el riesgo de acceso no autorizado debido a credenciales comprometidas, asegurando que incluso si una contraseña se ve comprometida, los atacantes no puedan acceder fácilmente a las cuentas o dispositivos.
Responsable	Propietario del hogar/Proveedor de servicios.
Fecha de implementación	Inmediato.
Estado	Abierto.

- ***Descripción:***

- Gestor de Contraseñas: Usar un gestor de contraseñas que genere y almacene contraseñas fuertes y únicas para cada cuenta y dispositivo.

- Autenticación Multifactor (MFA): Implementar MFA en todas las cuentas críticas y dispositivos. MFA añade una capa adicional de seguridad al requerir múltiples formas de verificación (algo que sabes, algo que tienes, y algo que eres).

- Políticas de Contraseñas: Establecer políticas de contraseñas estrictas que incluyan requisitos de longitud mínima, complejidad, y periodicidad de cambios.

3.13.2 Validez y Gestión de Documentos

Este plan será revisado y actualizado periódicamente. Se recomienda a los usuarios mantener registros de auditoría y documentación de seguridad para garantizar la validez y la efectividad continua de las medidas implementadas.

3.14 Plan de acción de tratamiento de riesgos

El Plan de Acción de Tratamiento de Riesgos de la Tabla 49, tiene como objetivo principal establecer un conjunto de medidas estratégicas destinadas a identificar, evaluar y mitigar los riesgos cibernéticos asociados a los sistemas IoT en entornos domésticos. Este plan está fundamentado en un análisis de las vulnerabilidades detectadas, así como en las mejores prácticas y marcos de referencia internacionales en materia de seguridad de la información. Mediante la implementación de controles preventivos, detectivos y correctivos, se busca garantizar la integridad, confidencialidad y disponibilidad de los datos.

Tabla 49. Plan de acción de tratamiento de riesgos

Actividad	**Objetivo**	**Tiempo**	**Responsable**	**Riesgos**	**Indicadores de Éxito**
Implementar Medidas de Seguridad	Mejorar la seguridad de la infraestructura de TI mediante la implementación de medidas de seguridad adicionales.	3 meses	Equipo de Seguridad de la Información	Falta de recursos adecuados, resistencia al cambio por parte de los usuarios y posibles interrupciones en el servicio durante la implementación.	Reducción de incidentes de seguridad, mejora en la detección y respuesta a amenazas, y cumplimiento con estándares de seguridad reconocidos.
Actualizar Software	Mejorar la seguridad de los sistemas mediante la actualización regular del software.	Continuo	Equipo de IT	Interrupciones en el servicio debido a actualizaciones fallidas, incompatibilidad con sistemas existentes y posibles vulnerabilidades no parcheadas.	Aumento en la seguridad de los sistemas, reducción de vulnerabilidades conocidas y cumplimiento con los requisitos de seguridad y regulaciones.
Utilizar Comunicaciones Encriptadas	Proteger la confidencialidad de la información durante la transmisión mediante el uso de comunicaciones encriptadas.	6 meses	Equipo de Seguridad de la Información	La complejidad de implementación, la falta de compatibilidad con sistemas heredados y la degradación del rendimiento debido al cifrado.	Reducción en el número de datos interceptados, cumplimiento con requisitos de seguridad de la información y mejora en la confianza del cliente
Implementar Gestión Segura de Credenciales	Fortalecer la seguridad de la autenticación y prevenir el acceso no autorizado mediante la gestión segura de credenciales.	4 meses	Equipo de Seguridad de la Información	La resistencia al cambio por parte de los usuarios, la pérdida de productividad durante la implementación	Reducción en el número de violaciones de credenciales, mejora en la seguridad de la autenticación y cumplimiento con regulaciones de privacidad de datos.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- La integración de honeynet y la selección de arquitecturas adecuadas para sistemas IoT son esenciales para la detección y mitigación de riesgos cibernéticos en entornos domésticos, que en conjunto con los honeypots de baja interacción como ConPot y CitrixHoneypot, permiten recolectar datos de los ataques frecuentes a los dispositivos IoT para el hogar. Estos dispositivos IoT usan una categoría de arquitectura centralizada de 7 capas de la ITU-T Y.4000 basada en el modelo OSI, que es específica para entornos IoT.

- El análisis de los dispositivos permitió descubrir la existencia de nueve vulnerabilidades, ocho de ellas de categoría media y una baja, de las ocho, dos son vulnerabilidades conocidas como CVE-2013-2566 y CVE-2015-2808. La RC4bias o CVE-2013-2566 permite al atacante obtener información parcial de la sesión, y CVE-2015-2808 concede al atacante forzar una conexión SSL/TLS por el uso claves RSA débiles. Además, se encontró que el puerto 6668/TCP habilitado con el servicio IRC estaba abierto, este puerto es el que admite que los dispositivos IoT tengan conectividad continua a través de un control remoto, cuando no se usa el puerto, éste resulta un riesgo para el sistema IoT al ser una puerta de ingreso.

- Se creó un honeypot específico programa en Python que registra, captura y analiza ataques DoS TCP SYN Flooding. Se utilizaron librerías de python, como: ***scapy, threading, socket y matplotlib*** que permitieron capturar los paquetes de red, ejecutar el servicio TCP, crear servidores TCP, generar y visualizar las gráficas. La función principal es capturar paquetes TCP dirigidos al puerto 6668 en la interfaz de red "Wi-Fi" y ejecutar la función packet_handler por cada paquete capturado, esta función comprueba si el paquete capturado contiene una capa TCP para posteriormente verificar si el paquete TCP tiene la bandera SYN activa, indicando un intento de inicio de conexión, a continuación, se conecta por medio de socket a MongoDB para

generar gráficos de las conexiones capturadas y los puertos utilizados, creando finalmente un DataFrame con los datos de las conexiones para un análisis más fácil.

- Las pruebas de penetración se realizaron con una máquina atacante con Kali Linux, se ejecutaron cuatro tipos de pruebas, la primera es Hacking Network Wireless, con un tiempo estimado de 10 minutos para la obtención de la contraseña de la red inalámbrica. La segunda prueba, fue la explotación de las vulnerabilidades y exposiciones comunes (CVE), para ello se utilizaron los comandos ***openssl s_client -connect 10.10.10.217:443 y ./testssl.sh 10.10.10.217:443***, simultáneamente para establecer una conexión SSL/TLS, e instantáneamente se registraron 17 ataques en el TPOT, registrados con el nombre CVE-2015-0204 CVE-2015-1637 desde la IP 10.10.10.242, con 4354 eventos, entre los que denota el puerto vulnerable 10001, que coincide con el Echo-Dot Alexa.

- Con el Honeypot, se realizó la tercera prueba, que consistió en la Denegación de servicio, en esta se enviaron ataques DoS TCP SYN Flooding, con el comando ***sudo hping3 --syn --rand-source --flood -p 6668 10.10.10.210***, de esta manera, el honeypot registró alrededor de 4.000 solicitudes en un periodo de 10 segundos de paquetes de diferentes IP y puertos. Al mismo tiempo se realizó la misma prueba con un dispositivo IoT, identificando por medio de Zenmap que el dispositivo tenía abierto el puerto 6668/TCP con el servicio IRC, después se verificó que el dispositivo tenía conexión TCP al puerto 6668 con la herramienta Hercules, para posteriormente ejecutar el comando ***hping3 –syn –rand-source –flood -p 6668 10.10.10.236*** desde la máquina Kali, pero el dispositivo no muestra ninguna información ni emite alertas de intrusión.

- El control de los dispositivos desde la LAN, fue la cuarta prueba de penetración, se tomó como base el proyecto ***tinytuya*** de python, que requiere la dirección IP, el ID del dispositivo, la versión del protocolo y la clave local. Por medio del comando ***python -m tinytuya scan***, se escanean los dispositivos IoT generando un archivo JSON con la información, sin embargo, la clave local

no se pudo obtener con la versión gratuita de Tuya, y se generó un error al realizar esta prueba de penetración.

- En base al modelo de línea base para seguridad de los datos, privacidad de las personas y dispositivos IoT para entornos domésticos creado, se lleva a cabo un análisis exhaustivo para las categorías: red, software, protocolo y credenciales, tomando en cuenta el catálogo de amenazas, los riesgos del sistema IoT, los vectores de ataque y las consecuencias. Se generó una matriz de riesgo con los criterios de valoración para el impacto del riesgo en el sistema con respecto a la triada de la CIA, después se valoró la probabilidad de ocurrencia de estos riesgos determinando si son frecuentes, ocasionales o raros. Se calculó el riesgo inherente cuantitativo con el producto del ***impacto * probabilidad***, en base a ello se determinó si el riesgo inherente cuantitativo es crítico, moderado o significativo.

- Sobre los riesgos, se pudo determinar si se van a mitigar, asumir o transferir considerando las políticas para gestionarlos. Las políticas más importantes fueron el uso de Contraseñas Seguras, la Actualización de Software, Respuesta a Incidentes, entre otras, que van de la mano con los controles para firewall, de actualización regular, de encriptación y políticas de gestión en general.

4.2 Recomendaciones

- A más de las pruebas de penetración realizadas en este proyecto, se sugiere incluir pruebas para ataques de fuerza bruta, para inyección de comandos, para reproducción de ataques de Man-in-the-Middle, para manipulación de firmware y actualizaciones de manera frecuente, de al menos cada 3 meses, para asegurar la protección de datos transmitidos, para garantizar la integridad y seguridad del firmware y sus actualizaciones. Estas pruebas permiten identificar y corregir vulnerabilidades, garantizando así una mayor efectividad en la protección contra posibles ataques que puedan comprometer el sistema.

- Para asegurar el control de los dispositivos IoT desde la LAN, es fundamental obtener la clave local, para ello, se recomienda crear una cuenta de

desarrollador en iot.tuya.com y crear un nuevo proyecto en la nube de Tuya, para obtener las claves locales de los dispositivos, ya que esto va más allá de la versión gratuita, además, hay que verificar y considerar las versiones del protocolo Tuya utilizadas, pues ésta prueba de penetración solo funciona para versiones inferiores a la 3.1, pues estas presentan vulnerabilidades conocidas que pueden facilitar la recuperación de la clave local del dispositivo.

- Para asegurar que el TPOT funcione sin interrupciones, y capture los incidentes en tiempo real, se sugiere asignar al menos 16GB de RAM, de esta manera, se garantizará una plataforma robusta que permita detectar y analizar amenazas en el entorno IoT doméstico.

- Para asegurar la efectividad del plan de tratamiento de riesgos en sistemas IoT domésticos, se recomienda realizar análisis de vulnerabilidades de manera periódica que ayuden a determinar el estado del sistema utilizando herramientas especializadas como Nessus, Rapid7, Shodan, IoT inspector, OpenVAS, entre otras, pues la combinación de herramientas permite obtener una cobertura integral y una mayor seguridad para los dispositivos IoT.

- Es importante la implementación del plan de tratamiento de riesgos de manera inmediata ante los riesgos de acceso no autorizado a la red, protocolos de comunicación no encriptados y gestión inadecuada de credenciales, asignando responsables, identificando objetivos e implementando medidas para garantizar la protección de datos y de dispositivos, y poder cumplir con la triada de la ciberseguridad CIA.

REFERENCIAS BIBLIOGRÁFICAS

[1] V. Ratcheva, S. Zahidi, K. Pal, K. Piaget, S. Baller, and World Economic Forum, *Global gender gap report 2022: insight report.*, 18th Edition. Accessed: Nov. 19, 2023. [Online]. Available: https://www.weforum.org/reports/global- risks-report-2023/.

[2] D. Demeter, "El número de ataques a dispositivos IoT se duplica en un año," Oct. 2021. Accessed: Nov. 19, 2023. [Online]. Available: https://www.kaspersky.es/about/press-releases/2021_el-numero-de-ataques-a-dispositivos-iot-se-duplica-en-un-ano

[3] S. Vesselina, S. Zahidi, K. K. Pal, K. Piaget, S. Baller, and World Economic Forum., "Informe de Riesgos Globales 2023," 2023. Accessed: Jan. 10, 2024. [Online]. Available: https://es.weforum.org/publications/global-risks-report-2023/

[4] Checkpoint, "Mapa de Amenazas Cibernéticas," Checkpoint. Accessed: Dec. 11, 2023. [Online]. Available: https://threatmap.checkpoint.com/

[5] M. Vargas, "Informe de gestión de la dirección general de inteligencia," Quito, Jul. 2023. Accessed: Dec. 11, 2023. [Online]. Available: https://www.policia.gob.ec/wp-content/uploads/downloads/2022/02/INFORME-RENDICION-DE-CUENTAS-PRELIMINAR-DGI-2021_10-FEB-2022-1.pdf

[6] Agencia de regulación y control de las Telecomunicaciones, "Estadísticas de Seguridad de Redes de Telecomunicaciones-agosto-2023," Aug. 2023, Accessed: Nov. 19, 2023. [Online]. Available: www.ecucert.gob.ec

[7] D. Salazar, M. Mauricio, T. Maldonado, M. Beatriz, and R. Tapia, "Revista Científica de Ciencias Jurídicas, Criminología y Seguridad," Quito.

[8] A. Sánchez, T. Vayas, F. Mayorga, and C. Freire, "Delincuencia e Inseguridad ciudadana en Ambato," Ambato, 2023.

[9] S. Manzano and R. Terán, “Despliegue de un honeynet basado en redes definidas por software para un ISP,” 2021.

[10] D. Ordóñez, “Reducing the IoT security breach with a microservice architecture based on TLS and OAuth2,” *Ingenius*, vol. 2021, no. 25, pp. 94–103, Jan. 2021, doi: 10.17163/ings.n25.2021.09.

[11] I. Castañón, “Análisis, diseño e implementación de una honeynet para el estudio de malware en entornos industriales IoT,” 2021.

[12] R. Andrade, I. Ortiz, M. Cazares, G. Navas, and M. I. Sánchez, “Defining Cyber Risk Scenarios to Evaluate IoT Systems,” *Games (Basel)*, vol. 14, no. 1, Feb. 2022, doi: 10.3390/g14010001.

[13] M. Rabzelj, L. Južnič, M. Volk, A. Kos, M. Kren, and U. Sedlar, “Designing and Evaluating a Flexible and Scalable HTTP Honeypot Platform: Architecture, Implementation, and Applications,” *Electronics (Switzerland)*, vol. 12, no. 16, Aug. 2023, doi: 10.3390/electronics12163480.

[14] V. Roblek, M. Meško, and A. Krapež, “A Complex View of Industry 4.0,” *Sage Open*, vol. 6, no. 2, p. 215824401665398, Apr. 2016, doi: 10.1177/2158244016653987.

[15] P. Kowalikova, P. Polak, and R. Rakowski, “The Challenges of Defining the Term ‘Industry 4.0,’” *Society*, vol. 57, no. 6, pp. 631–636, Dec. 2020, doi: 10.1007/s12115-020-00555-7.

[16] L. G. Antoni Garrell, *La Industria 4.0 en la sociedad digital*, Marge books., vol. 1. Barcelona, 2019.

[17] J. A. Saucedo-Martínez, M. Pérez-Lara, J. A. Marmolejo-Saucedo, T. E. Salais-Fierro, and P. Vasant, “Industry 4.0 framework for management and operations: a review,” *J Ambient Intell Humaniz Comput*, vol. 9, no. 3, pp. 789–801, Jun. 2018, doi: 10.1007/s12652-017-0533-1.

[18] F. Rozo-García, “Revisión de las tecnologías presentes en la industria 4.0,” *Revista UIS Ingenierías*, vol. 19, no. 2, pp. 177–191, May 2020, doi: 10.18273/revuin.v19n2-2020019.

[19] K. Rose, S. Eldridge, and L. Chapin, “La Internet de las Cosas-Una breve reseña para entender mejor los problemas y desafíos de un mundo más conectado,” Oct. 2015.

[20] Orbit Consulting, “Infraestructura necesaria para IOT,” https://www.orbit.es/cual-es-la-infraestructura-necesaria-para-iot/.

[21] International Teleommunication Union, “ITU-T Framework of constrained device networking in the IoT environments,” 2016. [Online]. Available: http://handle.itu.int/11.1002/1000/1

[22] L. Hernández, *Arquitectura IoT prototipando los dispositivos del futuro*. 2019. Accessed: Jan. 10, 2024. [Online]. Available: https://programarfacil.com/podcast/arduino-wifi-proyectos-iot/

[23] S. N. Swamy and S. R. Kota, “An empirical study on system level aspects of Internet of Things (IoT),” *IEEE Access*, vol. 8, pp. 188082–188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[24] Shulong Wang, Yibin Hou, Fang Gao, and Songsong Ma, “A novel clock synchronization architecture for IoT access system,” in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, IEEE, Oct. 2016, pp. 1456–1459. doi: 10.1109/CompComm.2016.7924944.

[25] M. Kolhar, F. Al-Turjman, A. Alameen, and M. Abualhaj, “A three layered decentralized lot biometric architecture for city lockdown during covid-19 outbreak,” *IEEE* , vol. 10.1109, pp. 163608–163617, 2020.

[26] S. Y. Shapsough and I. A. Zualkernan, “A Generic IoT Architecture for Ubiquitous Context-Aware Learning,” *IEEE Transactions on Learning Technologies*, vol. 13, no. 3, pp. 449–464, Jul. 2020, doi: 10.1109/TLT.2020.3007708.

[27] I. Miladinovic and S. Schefer-Wenzl, “NFV enabled IoT architecture for an operating room environment,” in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, IEEE, Feb. 2018, pp. 98–102. doi: 10.1109/WF-IoT.2018.8355128.

[28] J. Sun, S. Li, Q. Zhou, Y. Su, and Y. Fu, “Exploration and Research of Internet of Things Architecture Based on Fractal Theory,” in *2018 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS)*, IEEE, Nov. 2018, pp. 187–192. doi: 10.1109/CCIS.2018.8691200.

[29] M. Boujrad, S. Lazaar, and M. Hassine, “Performance Assessment of Open Source IDS for improving loT Architecture Security implemented on WBANs,” *PervasiveHealth Pervasive Comput*, 2020.

[30] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, “A Survey of IoT Applications in Blockchain Systems,” *ACM Comput Surv*, vol. 53, no. 1, pp. 1–32, Jan. 2021, doi: 10.1145/3372136.

[31] M. A. A. da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. de Albuquerque, “A Reference Model for Internet of Things Middleware,” *IEEE Internet Things J*, vol. 5, no. 2, pp. 871–883, Apr. 2018, doi: 10.1109/JIOT.2018.2796561.

[32] N. M. Kumar and P. K. Mallick, “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers,” *Procedia Comput Sci*, vol. 132, pp. 109–117, 2018, doi: 10.1016/j.procs.2018.05.170.

[33] C. Tonato and S. Sinche, “Análisis comparativo entre arquitecturas de sistemas IoT,” *Revista de Investigación en Tecnologías de la Información*, vol. 10, no. 21, pp. 55–70, Sep. 2022, doi: 10.36825/riti.10.21.006.

[34] Tinytuya, “Tuya WiFi smart devices,” tinytuya 1.14.0. Accessed: Jun. 23, 2024. [Online]. Available: https://pypi.org/project/tinytuya/

[35] J. Minguet, “Riesgos Cibernéticos,” 2003. Accessed: Jan. 10, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=917276

[36] Kaspersky, “Los riesgos de seguridad y las buenas prácticas de la Internet de las cosas,” https://latam.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security.

[37] L Spitzner, “Honeypots,” in *Honeypots: catching the insider threat*, : : 19th., vol. 19th, Annual Computer Security Applications Conference, 2003.

[38] E. Gallego and J. E. López De Vergara, “Honeynets: Aprendiendo del Atacante.” [Online]. Available: http://www.honeynet.org

[39] A. G. Javier, *Seguridad en Internet de las Cosas Honeypot to capture Iot-Attack methods*. 2018.

[40] Elhacker, “Los mejores HoneyPots,” https://blog.elhacker.net/2021/01/los-mejores-honeypots-ejemplos-y-tipos-trampas-rdp-ssh-cowrie-docker-rdpy.html. Accessed: Jun. 21, 2024. [Online]. Available: https://blog.elhacker.net/2021/01/los-mejores-honeypots-ejemplos-y-tipos-trampas-rdp-ssh-cowrie-docker-rdpy.html

[41] D. Fraunholz, M. Zimmermann, and H. Schotten, *An adaptive honeypot configuration, deployment and maintenance strategy*. issn: 17389445, 2017.

[42] S. Chadha, “Honeything: The IoT Trap System,” Medium. Accessed: Mar. 24, 2024. [Online]. Available: https://medium.com/@shreya16aug/honeything-the-iot-trap-system-12e7bf9b6a8a

[43] T. Britton, “Wificam, repositorio de código.” Accessed: Mar. 24, 2024. [Online]. Available: https://github.com/h-m-s/wificam

[44] A. Bredo, “Honeypot-Camera, repositorio de código.” Accessed: Mar. 24, 2024. [Online]. Available: https://github.com/alexbredo/honeypot-camera

[45] I. Goldberg, “MTPot, repositorio de código.” Accessed: Mar. 24, 2024. [Online]. Available: https://github.com/Cymmetria/MTPot

[46] D. Demeter, “IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019,” Demeter, Dan. Accessed: Mar. 29, 2024.

[Online]. Available: https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019

[47] D. Demeter, "¿Qué es un honeypot?," Kaspersky. Accessed: Mar. 29, 2024. [Online]. Available: https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

[48] C. Bannon, E. Momeni, and S. Lekkala, "Arquitecturas de red centralizadas y descentralizadas," Diseño de redes. Accessed: May 16, 2024. [Online]. Available: https://es.linkedin.com/advice/0/how-do-you-evaluate-trade-offs-between-centralized?lang=es

[49] D. Buitrón, "Arquitecturas y Modelos de Referencia para sistemas IoT," Escuela Politécnica Nacional, Quito, 2022.

[50] International Teleommunication Union, "ITU-T Requirements of the network for the Internet of things," Sep. 2016. [Online]. Available: http://handle.itu.int/11.1002/1000/11

[51] DOMONOVA, "Dispositivos para lograr una vivienda domótica," DOMONOVA. Accessed: Apr. 04, 2024. [Online]. Available: https://domonova.com/blog/12-dispositivos-para-lograr-una-vivienda-domotica/

[52] Amazon, "ECHO DOT 5ta Gen," Amazon. Accessed: May 21, 2024. [Online]. Available: https://www.amazon.com/-/es/generaci%C3%B3n-modelo-Parlante-inteligente-Carb%C3%B3n/dp/B09B8V1LZ3

[53] Nexxt Solutions, "Bombilla Inteligente," 2023. Accessed: May 21, 2024. [Online]. Available: https://www.nexxtsolutions.com/es/conectividad/interna-productos/AHIBUSO4U1-es/

[54] Nexxt Solutions, "Cámara inteligente Wi-Fi de 2K para interior." Accessed: May 21, 2024. [Online]. Available:

https://www.nexxtsolutions.com/es/conectividad/interna-productos/camara-de-2k-para-interior-NHC-I710-es/

[55] Teclam, “Interruptor de luz inteligente,” 2023, Accessed: May 21, 2024. [Online]. Available: https://digitalserver.com.ec/producto/interruptor-inteligente-de-2-tomas-wifi-5228/

[56] Smart Life, “Enchufe inteligente Versión: 1.0.” Accessed: May 21, 2024. [Online]. Available: https://www.novicompu.com/enchufe-inteligente/p

[57] Tuya, “Sensor de Puerta y Ventana.” Accessed: May 21, 2024. [Online]. Available: https://mirosplayer.com/producto/sensor-puerta-ventana-wifi-app-tuya-smart-life-alarma-casa/

[58] Nexxt Solutions, “Enchufe inteligente,” 2022. Accessed: May 21, 2024. [Online]. Available: https://www.nexxtsolutions.com/es/conectividad/interna-productos/AHIWPSO4U1-es/

[59] Secure Controls Framework, “SCF Overview & Instructions,” 2024. [Online]. Available: https://securecontrolsframework.com/capability-maturity-model/

[60] CIS, “Controls Internet of Things Companion Guide.”

[61] K. Caindec *et al.*, “Industry Internet of Things Security Framework (IISF),” 2023.

[62] Cloud Security Alliance, “Guide to the IoT Security Controls Framework Version 2,” 2021. [Online]. Available: https://cloudsecurityalliance.org

[63] NIST, “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products,” Feb. 2022. doi: 10.6028/NIST.CSWP.02042022-2.

[64] IoT Security Foundation, “IoTSF IoT Security Assurance Framework,” 2021. [Online]. Available: https://iotsecurityfoundation.org.

[65] Tenable Nessus, “Nessus,” Tenable. Accessed: Apr. 23, 2024. [Online]. Available: https://es-la.tenable.com/products/nessus

[66] OpenVAS, “Greenbone OpenVAS.” Accessed: Jun. 21, 2024. [Online]. Available: https://openvas.org/

[67] Rapid7, “Rapid7 Nexpose.” Accessed: Jun. 21, 2024. [Online]. Available: https://www.rapid7.com/

[68] “Honeypots,” Ciberseguridad. Accessed: Jun. 21, 2024. [Online]. Available: https://ciberseguridad.com/servicios/honeypots/

[69] C. De, I. De Sistemas, I. E. Jairo, and S. Cabrera, “‘DESPLIEGUE DE HONEYPOT EN LA NUBE PRIVADA COMO PRIMER PERÍMETRO DE SEGURIDAD,’” 2021.

[70] Rootstack, “¿Qué lenguaje es más fácil, Perl, Python o Ruby? ,” RootStack. Accessed: Jun. 21, 2024. [Online]. Available: https://rootstack.com/es/blog/que-lenguaje-es-mas-facil-perl-python-o-ruby

[71] M. Rogers, “Exposing One of China’s Cyber Espionage Units,” 2012. [Online]. Available: www.mandiant.com

[72] M. Meucci and A. Muller, “Testing Guide,” 2013. [Online]. Available: http://www.owasp.org

[73] ITIL, “BRIEFING OUTLINE,” 2005.

[74] NIST, “MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad,” 2019.

[75] ISO27001, “ISO27001.” Accessed: Jun. 18, 2024. [Online]. Available: https://normaiso27001.es/

[76] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology,” 2002.

[77] Iso, “ISO/IEC 27001:2022,” 2022.

[78] Iso, “ISO/27002,” 2022.

[79] K. A. Scarfone and P. Hoffman, “Guidelines on firewalls and firewall policy,” Gaithersburg, MD, 2009. doi: 10.6028/NIST.SP.800-41r1.

[80] M. Souppaya and K. Scarfone, “Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology,” Gaithersburg, MD, Nov. 2021. doi: 10.6028/NIST.SP.800-40r4-draft.

[81] E. Barker, “Recommendation for key management:,” Gaithersburg, MD, May 2020. doi: 10.6028/NIST.SP.800-57pt1r5.

[82] IoT Security Foundation, “IoTSF IoT Security Assurance Framework Release 3.0,” 2021. [Online]. Available: https://iotsecurityfoundation.org.

ANEXOS

Anexo A. Política General de Seguridad de la Información

Macroproceso: Administración de riesgos	**Versión:** 1.0
Proceso: Gestión de seguridad de información y prevención de riesgos	**Custodio:** Políticas y controles
Autor: Yulisa Acosta	

Política General de Seguridad de la Información

1. Objetivo

Garantizar la integridad, confidencialidad y disponibilidad de los datos, así como la protección de la privacidad de los usuarios y la seguridad de los dispositivos IoT en entornos domésticos, mediante la implementación de medidas de seguridad robustas, actualizaciones periódicas, controles de acceso adecuados, educación y concienciación de los usuarios, y una evaluación continua de riesgos y vulnerabilidades.

2. Alcance

El alcance de la presente política abarca todos los aspectos relacionados con la protección de la seguridad de los datos, la privacidad de las personas y la seguridad de los dispositivos IoT en entornos domésticos.

Esta política se aplica a todos los miembros del hogar, incluidos residentes, familiares, invitados y cualquier personal externo que tenga acceso a las instalaciones y/o a los dispositivos IoT del hogar.

Además, esta política es aplicable a todos los dispositivos IoT y activos de información en cualquier forma o medio de almacenamiento utilizados en el entorno doméstico, ya sea físico o digital.

El alcance incluye, pero no se limita a, la implementación de medidas de seguridad, la gestión de la privacidad de los datos personales, la protección de los dispositivos IoT contra amenazas y vulnerabilidades, y la promoción de una cultura de seguridad cibernética en el hogar.

Esta política se extiende a todas las actividades relacionadas con el diseño, implementación, operación y mejora continua de medidas de seguridad y privacidad en el entorno doméstico, con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de los datos, así como la protección de la privacidad de las personas y la seguridad de los dispositivos IoT.

3. Responsabilidades y Roles

a. Responsable de Seguridad de la Información (RSI):
    i. Este rol es responsable de diseñar, implementar y mantener las políticas y procedimientos de seguridad de la información en el hogar.
    ii. Supervisa la gestión de riesgos, la protección de datos y la seguridad de los dispositivos IoT.
    iii. Coordina la respuesta a incidentes de seguridad y proporciona capacitación en seguridad cibernética a los miembros del hogar.

b. Administrador de Dispositivos IoT:
    i. Se encarga de la configuración y gestión de los dispositivos IoT en el hogar, incluyendo la instalación de actualizaciones de firmware y la aplicación de medidas de seguridad.
    ii. Monitoriza el estado de los dispositivos y responde a posibles problemas de seguridad o funcionamiento.

c. Usuario Responsable:
    i. Cada miembro del hogar es responsable de seguir las políticas de seguridad establecidas, incluyendo la protección de contraseñas, la actualización de software y la adopción de prácticas seguras de navegación y uso de dispositivos IoT.
    ii. Debe informar cualquier actividad sospechosa o incidente de seguridad al RSI o al administrador de dispositivos IoT.

d. Gestor de Privacidad de Datos:
    i. Se encarga de garantizar el cumplimiento de las leyes y regulaciones de privacidad de datos en el hogar, incluyendo la gestión de consentimientos y el tratamiento adecuado de la información personal.
    ii. Supervisa la recopilación, almacenamiento y compartición de datos personales en el hogar, asegurando la confidencialidad y privacidad de la información.

e. Auditor de Seguridad:
    i. Realiza evaluaciones periódicas de la seguridad de la red doméstica y los dispositivos IoT, identificando posibles vulnerabilidades y áreas de mejora.
    ii. Proporciona recomendaciones para fortalecer la seguridad y la privacidad en el hogar.

f. Usuario Final:
    i. Todos los miembros del hogar que utilizan dispositivos IoT y acceden a la red doméstica tienen la responsabilidad de seguir las prácticas de seguridad recomendadas y proteger la privacidad de su propia información.

Estos roles y responsabilidades garantizan una distribución clara de tareas y responsabilidades para proteger la seguridad de los datos, la privacidad de las personas y los dispositivos IoT en entornos domésticos.

4. Objetivos

Objetivos para Proteger la Seguridad de los Datos, la Privacidad de las Personas y los Dispositivos IoT en Entornos Domésticos

a. Implementación del Cifrado de Extremo a Extremo:
    i. Garantizar que todos los datos transmitidos entre dispositivos IoT y servidores estén protegidos mediante cifrado de extremo a extremo, minimizando así el riesgo de interceptación por parte de terceros.

b. Actualización Regular de Dispositivos IoT:
    i. Establecer un protocolo para la actualización periódica de todos los dispositivos IoT en el hogar con los últimos parches de seguridad y firmware disponibles, con el fin de mitigar vulnerabilidades conocidas y garantizar su integridad y seguridad.

c. Configuración Segura de la Red Doméstica:
    i. Implementar medidas de seguridad, como firewalls y contraseñas robustas, para proteger la red doméstica contra intrusiones externas y garantizar que solo los dispositivos autorizados puedan acceder a ella.

d. Control de Acceso a Dispositivos IoT:
    i. Establecer controles de acceso para limitar quién puede interactuar con los dispositivos IoT en el hogar, con especial atención a aquellos que recopilan datos personales, asegurando así la confidencialidad y privacidad de la información.

e. Minimización de la Recopilación de Datos:
    i. Configurar los dispositivos IoT para que recojan únicamente la información necesaria y relevante, reduciendo así el riesgo de

exposición de datos personales y respetando la privacidad de los usuarios del hogar.

f. Transparencia y Consentimiento del Usuario:
    i. Garantizar que los usuarios estén plenamente informados sobre qué datos se recopilan, cómo se utilizan y con quién se comparten, obteniendo su consentimiento explícito antes de recopilar cualquier información personal.

g. Respaldo y Recuperación de Datos:
    i. Establecer un plan de respaldo regular para proteger los datos críticos almacenados en dispositivos IoT y facilitar su recuperación en caso de pérdida, fallo del dispositivo o incidente de seguridad.

h. Monitoreo Activo de Seguridad:
    i. Implementar herramientas de monitoreo de seguridad para detectar y responder de manera proactiva a actividades sospechosas o intentos de intrusión en la red doméstica y los dispositivos IoT.

i. Educación y Concienciación:
    i. Proporcionar educación y recursos sobre seguridad cibernética a los miembros del hogar para aumentar su conciencia sobre las amenazas potenciales y capacitarlos para protegerse adecuadamente.

j. Evaluación y Actualización Continua:
    i. Realizar evaluaciones periódicas de la seguridad de la red doméstica y los dispositivos IoT, y ajustar las medidas de seguridad según sea necesario para hacer frente a nuevas amenazas y vulnerabilidades, garantizando así una protección continua y efectiva.

5. Políticas Generales

a. Política de Contraseñas Seguras:
b. Política de Actualización de Software:
c. Política de Acceso y Autorización:
d. Política de Privacidad de Datos:
e. Política de Monitoreo y Detección de Amenazas:
f. Política de Respuesta a Incidentes:
g. Política de Educación y Concientización:
h. Política de Evaluación de Riesgos y Cumplimiento:

Estas políticas proporcionan un marco sólido para proteger la seguridad de los datos, la privacidad de las personas y los dispositivos IoT en entornos domésticos.

Anexo B. Criterios de valoración para los activos y Matriz de riesgos

Para la valoración de activos, IoT Security Foundation con el objetivo de asegurar la integridad y confiabilidad de un producto, establece un sistema de clasificación de activos basado en clases de garantía

- Clase 0: cuando es probable que el compromiso de los datos generados o la pérdida de control tenga como resultado un impacto poco discernible en un individuo u organización [82].

- Clase 1: cuando es probable que el compromiso de los datos generados o la pérdida de control no tenga más que un impacto limitado en un individuo u organización [82].

- Clase 2: además de la clase 1, el dispositivo está diseñado para resistir ataques a la disponibilidad que tendrían importantes impactos en un individuo u organización o impactar a muchos individuos. Por ejemplo, limitando las operaciones de una infraestructura a la que está conectada [82].

- Clase 3: además de la clase 2, el dispositivo está diseñado para proteger datos confidenciales, incluida la información de identificación personal (PII) [82].

- Clase 4: además de la clase 3, donde el compromiso de los datos generados o la pérdida de control tienen el potencial de afectar la infraestructura crítica o causar lesiones personales [82].

La Tabla B1, presenta los niveles indicativos de confidencialidad, integridad y disponibilidad para cada clase de garantía.

Tabla B1. Clases de garantías para confidencialidad, integridad y disponibilidad [64].

Clase	**Confidencialidad (C)**	**Integridad (I)**	**Disponibilidad (D)**
Clase 0	Básico	Básico	Básico
Clase 1	Básico	Medio	Medio
Clase 2	Medio	Medio	Alto
Clase 3	Alto	Medio	Alto
Clase 4	Alto	Alto	Alto

En la Tabla B2, se muestra las estrategias que se utiliza para los riesgos, estos pueden ser mitigados, asumidos, evitados o transferidos.

Tabla B2. Estrategias para los riesgos

Estrategias	
Mitigar	Implemento controles para reducir el nivel de riesgo.
Asumir	Se asume o retiene el riesgo en su nivel actual.
Evitar	Cancelo la actividad que genera el riesgo.
Trasnferir	Comparto el riesgo con partes externas (compra de un seguro o tercerización de servicios)

En la Tabla B3, se muestra el tipo de control que se aplica para cada riesgo.

Tabla B3. Tipo de control para los riesgos

Tipo de Control	
Preventivo	Anticipan eventos no deseados antes de que sucedan.
Detectivo	Identifican los eventos en el momento en que se presentan.
Correctivo	Aseguran que las acciones correctivas sean tomadas para revertir un evento no deseado.

En la Tabla B4, se muestra la valoración de la probabilidad de ocurrencia de los riesgos

Tabla B4. probabilidad de ocurrencia de los riesgos

Probabilidad	
1 – Raro	El evento puede ocurrir solo en circunstancias excepcionales. **No se ha presentado en los últimos 3 años**
2 - Improbable	El evento puede ocurrir solo en algún momento. **Al menos una vez en los últimos 3 años**
3 - Posible	El evento podría ocurrir en algún momento. **Al menos una vez en los últimos 2 años.**
4 - Probable	El evento probablemente ocurriría en la mayoría de las circunstancias. **Al menos una vez en el último año**
5 - Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias. **Mas de una vez al año.**

En la Tabla B5, se muestra la valoración del impacto/consecuencia de los riesgos

Tabla B5. Impacto/Consecuencia de los riesgos

Impacto / Consecuencia	
1 - Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2 - Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3 - Dañino	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4 - Severo	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5 - Critico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Anexo C. Sniffer

En la Tabla C1 , se muestra el script de Python de la captura de datos del ataque DoS por inundación de paquetes SYN

Tabla C1. Script para captura de datos en honeypot

```
from scapy.all import *
import threading
import socket
import time
from pymongo import MongoClient
from datetime import datetime
# Inicializar el cliente de MongoDB
client = MongoClient('mongodb://localhost:27017/')
db = client['honey']
collection = db['honey']
# Variables globales para el seguimiento de SYN
syn_count = 0
start_time = time.time()
# Función que se ejecuta para cada paquete capturado
def packet_handler(packet):
    global syn_count, start_time
    if packet.haslayer(TCP):
        if packet[TCP].flags == "S":
            syn_count += 1
            print("Paquete SYN recibido:")
            print("IP Fuente: ", packet[IP].src)
            print("Puerto de origen: ", packet[TCP].sport)
            print("Cantidad de TCP SYN recibido: ", syn_count)
            # Obtener la hora actual
            current_time = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
            # Insertar los datos en la base de datos MongoDB
            collection.insert_one({
                "timestamp": current_time,
                "source_ip": packet[IP].src,
                "source_port": packet[TCP].sport,
                "syn_count": syn_count
            })

    # Calcular y mostrar la tasa de SYN por segundo
    elapsed_time = time.time() - start_time
    if elapsed_time >= 1:
        syn_rate = syn_count / elapsed_time
        # Reiniciar el contador y el tiempo
        syn_count = 0
        start_time = time.time()

# Función para manejar las conexiones entrantes al servidor TCP
def tcp_server():
    HOST = '0.0.0.0'  # La dirección IP en la que el servidor va a escuchar
    PORT = 6668  # El puerto en el que el servidor va a escuchar
    with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
        s.bind((HOST, PORT))
        s.listen()
        print(f"Servidor TCP escuchando en {HOST}:{PORT}")
```

```
        conn, addr = s.accept()
        with conn:
            print('Conexión entrante de:', addr)
            while True:
                data = conn.recv(1024)
                if not data:
                    break
                print('Datos recibidos:', data.decode())

# Iniciar el servidor TCP en un hilo aparte
tcp_server_thread = threading.Thread(target=tcp_server)
tcp_server_thread.start()
# Captura de paquetes en la interfaz de red especificada
sniff(filter="tcp and dst port 6668", prn=packet_handler,iface="Wi-Fi")
```

En la Figura C1, se muestra la base de datos para honeypot de ataque DoS

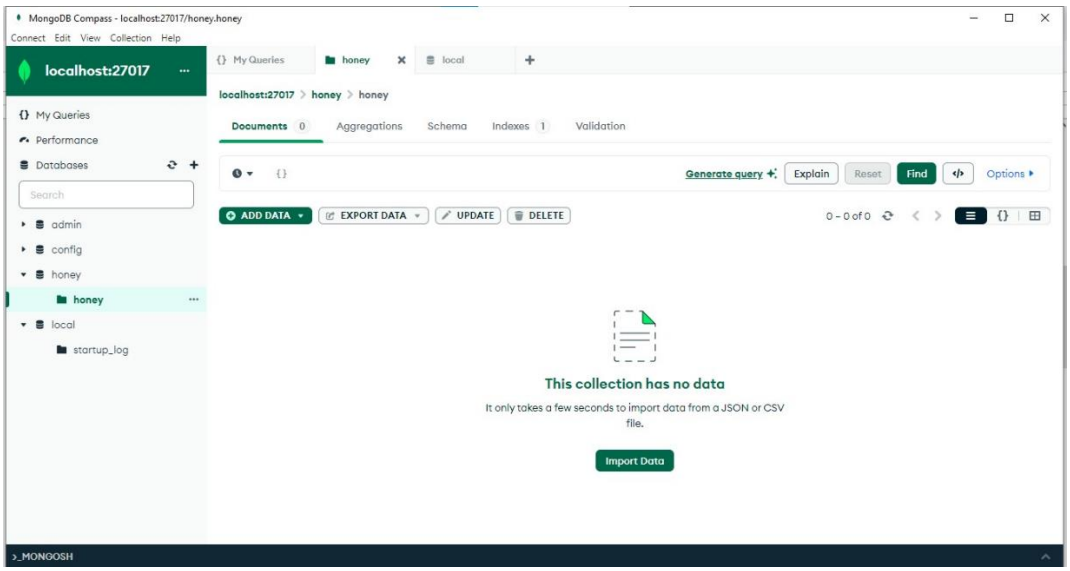


Figura C1. Base de datos para honeypot de ataque DoS

En la Tabla C2, se muestra el código para las gráficas del honeypot

Tabla C2. Script para gráficas de honeypot

```
import pymongo
from pymongo import MongoClient
import matplotlib.pyplot as plt
from datetime import datetime
import pandas as pd
# Conectar a MongoDB
client = MongoClient('mongodb://localhost:27017/')
db = client['honey']
collection = db['honey']
# Recuperar datos de la base de datos
data = collection.find()
# Procesamiento de datos
connections = {}
ip_counts = {}
port_counts = {}
timestamps = []
connection_data = []
for item in data:
    connection_data.append({
        'Fecha': item['timestamp'],
        'IP': item['source_ip'],
        'Puerto': item['source_port']
    })
    # Grafica en función del tiempo con las conexiones
    timestamps.append(datetime.strptime(item['timestamp'], "%Y-%m-%d %H:%M:%S"))
    # Grafica de barras con los puertos
    port = item['source_port']
    if port not in port_counts:
        port_counts[port] = 1
    else:
        port_counts[port] += 1

# Grafica en función del tiempo con las conexiones
plt.figure(figsize=(10, 6))
plt.plot(timestamps, range(len(timestamps)), color='blue')
plt.xlabel('Tiempo')
plt.ylabel('Número de Conexiones')
plt.title('Gráfica en Función del Tiempo con las Conexiones')
plt.grid(True)
plt.show()
# Grafica de barras con los puertos
plt.figure(figsize=(10, 6))
plt.bar(port_counts.keys(), port_counts.values(), color='orange')
plt.xlabel('Puertos')
plt.ylabel('Cantidad de Conexiones')
plt.title('Gráfica de Barras con los Puertos')
plt.xticks(rotation=45)
plt.tight_layout()
plt.show()
# Crear un DataFrame con los datos
df = pd.DataFrame(connection_data)
df
```

INFORME TÉCNICO DE RESULTADOS

CONTROL DOCUMENTAL

PROYECTO:	Honeynet para análisis y tratamiento de riesgos cibernéticos en un sistema IoT para el hogar
ENTIDAD:	FAMILIA XYZ
TITULO:	Análisis y explotación de vulnerabilidades interno
VERSIÓN:	1.0
FECHA EDICIÓN:	25/05/24
HERRAMIENTAS DE EDICIÓN:	Microsoft Office Word
AUTORES:	Acosta Proaño Yulisa Francisca
RESUMEN:	

VALIDACIONES Y APROBACIONES

Elaborado Por:	Acosta Proaño Yulisa Francisca Ing. Andrea Patricia Sánchez Zumba, Mg.

Vigencia

Este documento entrará en vigor en el momento en que la versión de la documentación haya alcanzado la versión 1.0. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación. Esta versión seguirá vigente mientras no se aprueben y publiquen modificaciones.

Introducción

En la era digital actual, la proliferación de dispositivos conectados y la creciente dependencia de la tecnología en los entornos domésticos han traído consigo una serie de desafíos en términos de seguridad y privacidad. Los dispositivos IoT (Internet de las Cosas), que van desde asistentes inteligentes hasta cámaras de seguridad y electrodomésticos conectados, introducen nuevas vulnerabilidades que pueden ser explotadas por actores malintencionados. Estos riesgos no solo comprometen la seguridad de la infraestructura tecnológica del hogar, sino que también ponen en peligro la privacidad de los individuos que habitan en estos entornos.

El presente informe tiene como objetivo proporcionar un análisis exhaustivo de las vulnerabilidades presentes en un entorno doméstico típico mediante el uso de la plataforma de escaneo de vulnerabilidades Nessus Tenable. Esta herramienta avanzada permite identificar y evaluar las debilidades en la seguridad de los dispositivos conectados, proporcionando una visión detallada de los riesgos potenciales y ofreciendo recomendaciones específicas para mitigarlos.

Alcance

El alcance de este análisis y escaneo de vulnerabilidades con la plataforma Nessus Tenable se centra en evaluar la seguridad y privacidad de un entorno doméstico típico, abarcando una variedad de dispositivos IoT y sistemas conectados. El objetivo es identificar posibles debilidades en la infraestructura tecnológica del hogar que puedan ser explotadas por amenazas externas o internas, comprometiendo así la integridad de los datos personales y la privacidad de los residentes.

1. Análisis y explotación de vulnerabilidades

1.1. Análisis IP

Tabla D1. Análisis – IP's

Dispositivo	IP
Camara inteligente para interiores	10.10.10.221
Sensor de contacto para puertas	10.10.10.230
Sensor de contacto para puertas	10.10.10.216
Enchufe inteligente	10.10.10.239
Enchufe inteligente	10.10.10.222
Interruptor de luz inteligente	10.10.10.236
Echo dot	10.10.10. 220
Bombilla inteligente	10.10.10.238
Bombilla inteligente	10.10.10.218

2. Objetivos

2.1. Objetivo General

Evaluar y mejorar la seguridad de los datos, la privacidad de las personas y la integridad de los dispositivos IoT en entornos domésticos mediante la identificación y mitigación de vulnerabilidades a través del análisis y escaneo con la plataforma Nessus Tenable.

2.2. Objetivos Específicos

- Analizar exhaustivamente los resultados del escaneo de vulnerabilidades para identificar y clasificar las debilidades críticas, altas y medias que puedan comprometer la seguridad informática y la privacidad en el entorno doméstico.

- Realizar pruebas de explotación con las vulnerabilidades identificadas para evaluar la capacidad de comprometer la integridad, confidencialidad y disponibilidad de la información en los dispositivos IoT y sistemas conectados del hogar.

- Establecer recomendaciones específicas para abordar y mitigar las vulnerabilidades descubiertas, priorizando aquellas que representen un mayor

riesgo para la seguridad de los datos y la privacidad de las personas en entornos domésticos.

3. Metodología

3.1. Metodología de clasificación de vulnerabilidades

La metodología de clasificación de vulnerabilidades se centra en evaluar el impacto, la probabilidad y el riesgo asociados con cada vulnerabilidad identificada en el entorno doméstico. Estos tres aspectos son fundamentales para priorizar las acciones de mitigación y reducir eficazmente el riesgo de posibles incidentes de seguridad. A continuación, se detallan los criterios utilizados para cada uno de estos aspectos:

3.1.1.- Impacto de vulnerabilidad

- ***Impacto en la Seguridad:*** Se evalúa el potencial impacto en la seguridad de los datos y la integridad de los sistemas en el entorno doméstico. Esto incluye consideraciones sobre la posibilidad de acceso no autorizado, la divulgación de información confidencial y la capacidad de comprometer la disponibilidad de los sistemas.

- ***Impacto en la Privacidad:*** Se analiza cómo la vulnerabilidad podría afectar la privacidad de las personas en el entorno doméstico, incluyendo la exposición de información personal y la invasión de la privacidad a través de dispositivos IoT comprometidos.

3.1.2.- Probabilidad de explotación

- ***Facilidad de Explotación:*** Se evalúa la facilidad con la que un atacante podría aprovechar la vulnerabilidad para llevar a cabo un ataque exitoso. Esto incluye consideraciones sobre la disponibilidad de exploits públicos, la complejidad técnica requerida y la accesibilidad de los vectores de ataque.

- ***Exposición a Amenazas Externas:*** Se analiza la exposición del sistema vulnerable a amenazas externas, como ataques remotos a través de Internet o acceso físico no autorizado a dispositivos IoT.

3.1.3.- Riesgo de Vulnerabilidad

- ***Riesgo General:*** Se calcula un nivel de riesgo general para cada vulnerabilidad, teniendo en cuenta tanto su impacto como su probabilidad de explotación. Esto permite priorizar las vulnerabilidades que representan el mayor riesgo para la seguridad y privacidad en el entorno doméstico.

- ***Priorización de Acciones:*** Se utiliza el nivel de riesgo asignado para priorizar las acciones de mitigación, enfocándose en abordar primero las vulnerabilidades con un riesgo más alto y un impacto más significativo en la seguridad y privacidad.

Al aplicar esta metodología de clasificación de vulnerabilidades, se obtiene una visión holística del panorama de seguridad y privacidad en el entorno doméstico, lo que permite tomar decisiones informadas sobre las medidas de mitigación necesarias para proteger eficazmente los datos personales y los dispositivos IoT.

3.2. Metodología de pruebas de intrusión

La metodología de prueba de intrusión diseñada para entornos domésticos se basa en principios reconocidos de seguridad y se adapta específicamente a la evaluación de la seguridad de datos, la privacidad de las personas y los dispositivos IoT en hogares. La siguiente metodología se ha elaborado tomando en consideración el enfoque requerido:

3.2.1. Identificación y Recopilación de Información:

- Obtención y análisis de la documentación disponible sobre los dispositivos IoT, redes domésticas y sistemas informáticos presentes en el entorno.

- Identificación de los dispositivos IoT, sistemas operativos, versiones de software y servicios activos en la red doméstica.

3.2.2. Verificación y Enumeración:

- Prueba de los dispositivos IoT y sistemas operativos para validar su existencia y funcionalidad.

- Verificación de la configuración de red y servicios comparándola con la documentación disponible y los estándares de seguridad recomendados.

3.2.3. Investigación y Análisis de Vulnerabilidades:

- Identificación y evaluación de posibles vulnerabilidades en los dispositivos IoT y sistemas conectados.

- Prueba de penetración para verificar la explotabilidad de las vulnerabilidades descubiertas, teniendo en cuenta su impacto en la seguridad de datos y la privacidad de las personas.

Elaboración de Reportes y Recomendaciones:

- Creación de informes detallados que incluyan un resumen de los hallazgos, evaluación de riesgos y recomendaciones para mitigar las vulnerabilidades identificadas.

- Entrega de informes al propietario del hogar, proporcionando orientación sobre cómo mejorar la seguridad y privacidad en su entorno doméstico.

4. Análisis

4.1. Análisis de vulnerabilidades

4.1.1. Situación actual y debilidades encontradas para cada uno de los componentes analizados

El siguiente resumen hace referencia al número de vulnerabilidades detectadas en los activos de la infraestructura del hogar. En este escenario de evaluación se realiza las evaluaciones desde la red LAN del hogar. El resumen de Resultados se detalla en la Tabla D2 y D3:

Tabla D2. Detalle de vulnerabilidades detectadas en IP.

IP	Dispositivo	Crítica	Alta	Media	Baja	Total general
10.10.10.239	Enchufe inteligente	0	0	0	0	0
10.10.10.238	Bombilla inteligente	0	0	0	0	0

10.10.10.236	Interruptor de luz inteligente	0	0	0	0	0
10.10.10.222	Enchufe inteligente	0	0	0	0	0
10.10.10.221	Cámara inteligente para interiores	0	0	0	1	1
10.10.10.220	Echo dot	0	0	8	0	8
10.10.10.218	Bombilla inteligente	0	0	0	0	0
10.10.10.230	Sensor de contacto para puertas	0	0	0	0	0
10.10.10.216	Sensor de contacto para puertas	0	0	0	0	0
Total general		0	0	8	1	9

Tabla D3. Resumen de vulnerabilidades detectadas en IP.

Severidad	Total
Crítica	0
Alta	0
Media	8
Baja	1
1 general	**9**

Conforme al análisis proporcionado por el informe generado a través de Nessus, en la Tabla D4, se presenta de manera detallada la propuesta de medidas correctivas destinadas a abordar las vulnerabilidades detectadas por esta herramienta.

Tabla D4. Detalle de Remediación Vulnerabilidades – Activos Involucrados

Dispositivo	IP	Código Vulnerabilidad	Vulnerabilidad	Prioridad
Cámara inteligente para interiores	10.10.10.221	10114	ICMP Timestamp Request Remote Date Disclosure	Baja
Echo dot	10.10.10.220	51192	SSL Certificate Cannot Be Trusted	Medio
Echo dot	10.10.10.220	51192	SSL Certificate Cannot Be Trusted	Medio
Echo dot	10.10.10.220	57582	SSL Self-Signed Certificate	Medio
Echo dot	10.10.10.220	57582	SSL Self-Signed Certificate	Medio
Echo dot	10.10.10.220	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medio
Echo dot	10.10.10.220	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medio
Echo dot	10.10.10.220	104743	TLS Version 1.0 Protocol Detection	Medio
Echo dot	10.10.10.220	157288	TLS Version 1.1 Deprecated Protocol	Medio

4.1.2. Evidencias de las principales vulnerabilidades encontradas y mapa de riesgos principales asociadas a las vulnerabilidades identificadas

El resumen de vulnerabilidades hace referencia a los resultados de nueve Vulnerabilidades, sin embargo, se analiza solamente las 8 vulnerabilidades de prioridad media puesto a que la vulnerabilidad de prioridad baja no cuenta con un puerto expuestos, por lo que se lo toma solo como información.

Tabla D5. SSL Certificate Cannot Be Trusted.

Vulnerabilidad: SSL Certificate Cannot Be Trusted	**CVE:** -	
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Baja
CVSS2: 6.4	**CVSS3:** 6.5	
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: No se puede confiar en el certificado X.509 del servidor. En esta situación se puede romper la cadena de confianza. La vulnerabilidad se detecta en los puertos TCP: 10001 55443		
Impacto de la vulnerabilidad: Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.		
Evidencias de la vulnerabilidad: Se identifica la respuesta de que el certificado no es emitido por una entidad autorizada. Por medio de una máquina virtual Ubuntu, con el comando openssl s_client se establece una conexión SSL/TLS con el servidor remoto ubicado en la dirección IP 10.10.10.220 en el puerto 10001 En la Figura D1, se observa la evidencia de configuración y expedición del certificado SSL, con el comando openssl s_client -connect 10.10.10.220:10001		

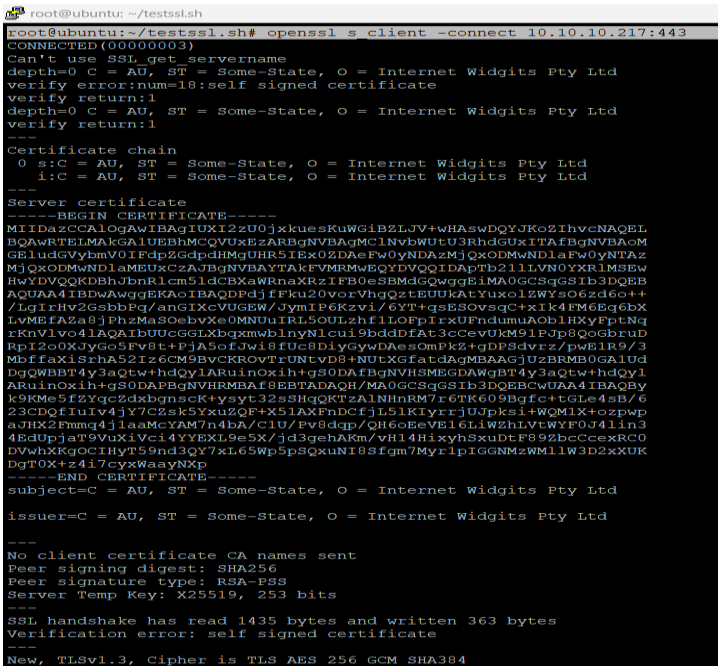


Figura D1. Evidencia de configuración y expedición del certificado SSL en TPOT

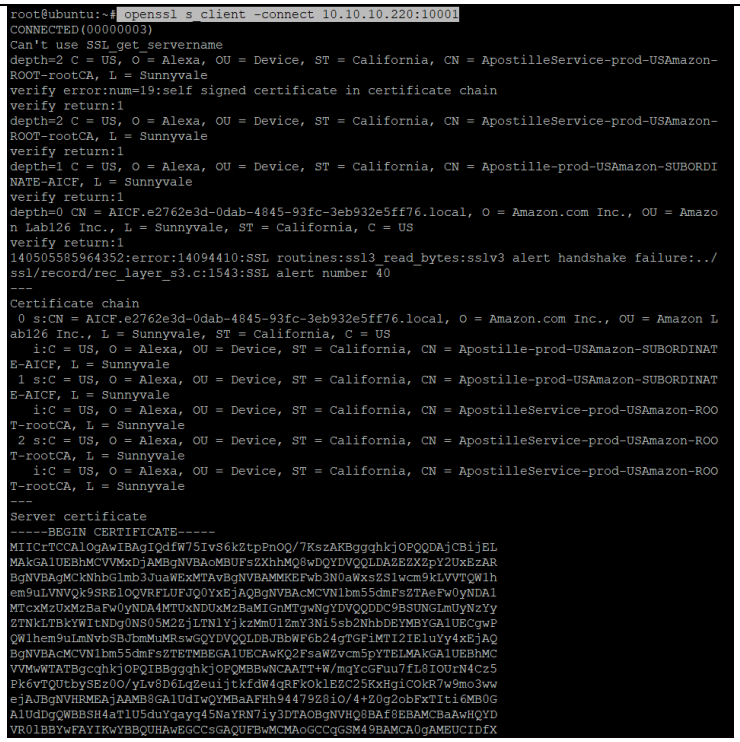


Figura D2. Evidencia de configuración y expedición del certificado SSL en ALEXA – TARGET

Remediación: Compre o genere un certificado SSL adecuado para este servicio.

Tabla D6. SSL Self-Signed Certificate.

Vulnerabilidad: SSL Self-Signed Certificate		**CVE:** -
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Baja
CVSS2: 6.4		**CVSS3:** -
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido. La vulnerabilidad se detecta en los puertos TCP: 10001 55443		
Impacto de la vulnerabilidad: Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.		
Evidencias de la vulnerabilidad: Se identifica el certificado como autofirmado. Por medio de una máquina virtual Ubuntu, con el comando openssl s_client se establece una conexión SSL/TLS con el servidor remoto ubicado en la dirección IP 10.10.10.220 en el puerto 10001		

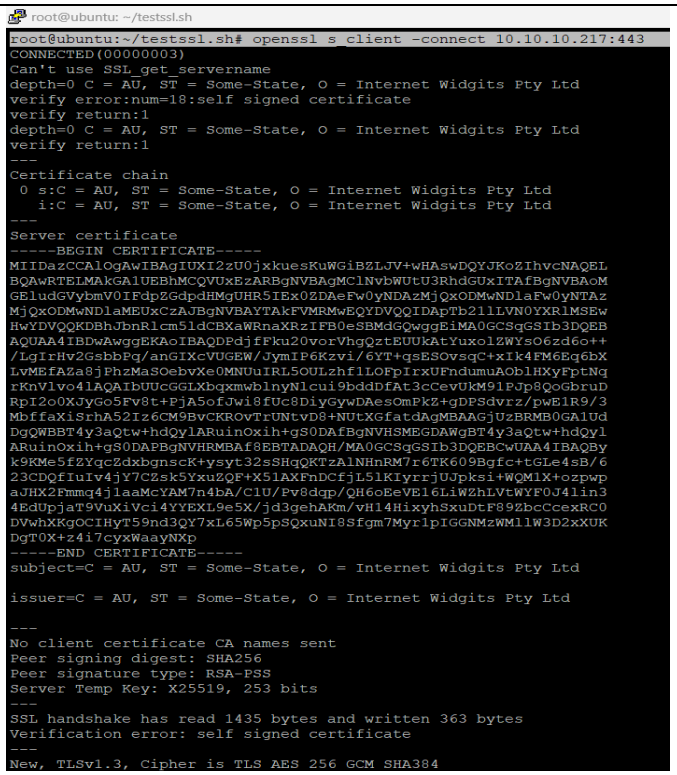


Figura D3. Evidencia de configuración y expedición del certificado SSL en TPOT.



Figura D4. Evidencia de configuración y expedición del certificado SSL en ALEXA – TARGET

Remediación: Compre o genere un certificado SSL adecuado para este servicio.

Tabla D7. TLS Version 1.0 Protocol Detection.

Vulnerabilidad: TLS Version 1.0 Protocol Detection	**CVE:** -	
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Bajo
CVSS2: 6.1	**CVSS3:** 6.5	
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico. La vulnerabilidad se detecta en los puertos TCP: 10001		
Impacto de la vulnerabilidad: El servicio remoto acepta conexiones cifradas usando TLS 1.0. TLS 1.0 tiene un número de fallas en el diseño criptográfico. Implementaciones modernas de TLS 1.0 mitigar estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 son diseñado contra estos defectos y debe usarse siempre que sea posible.		
Evidencias de la vulnerabilidad: Se identifica el certificado con el uso de cifrado TLS 1.0. Por medio de una máquina virtual Ubuntu, se ejecuta el script testssl.sh con el objetivo de realizar una evaluación de seguridad sobre el dispositivo que se encuentra en la dirección IP 10.10.10.220 y en el puerto 10001.		

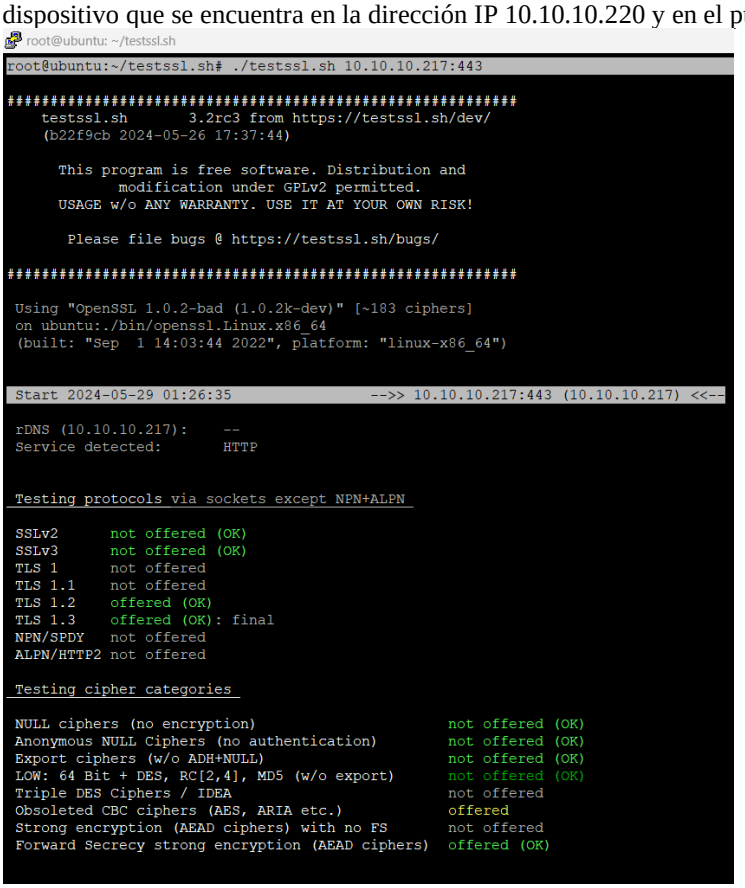


Figura D5. Evidencia de uso de cifrado TLSv1.0 en TPOT

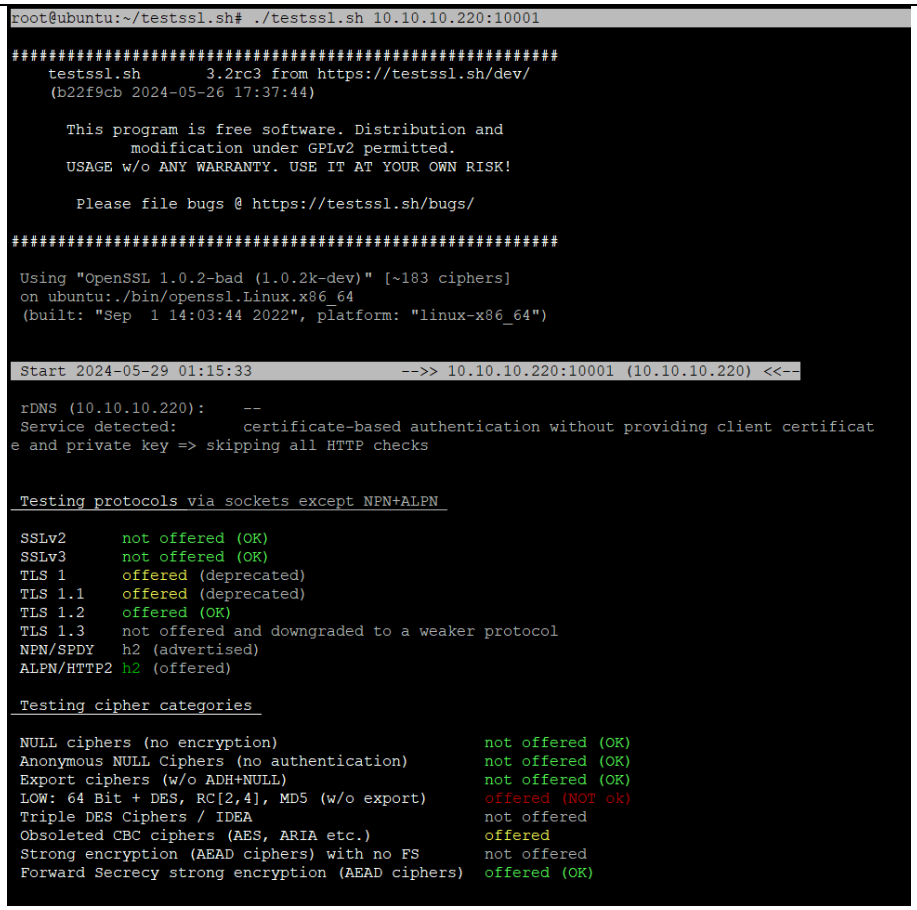


Figura D6. Evidencia de uso de cifrado TLSv1.0. en ALEXA – TARGET

Remediación: Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.

Tabla D8. SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Vulnerabilidad: SSL RC4 Cipher Suites Supported (Bar Mitzvah)		**CVE: CVE-2013-2566** **CVE-2015-2808**
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Bajo
CVSS2: 4.3		**CVSS3:** 5.9
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: "El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado.El cifrado RC4 tiene errores al generar un flujo pseudoaleatorio de bytes para que se introduzca una amplia variedad de pequeños sesgos en la corriente, disminuyendo su aleatoriedad. Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP), el atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados. La vulnerabilidad se detecta en los puertos TCP: 10001		
Impacto de la vulnerabilidad:		
Evidencias de la vulnerabilidad: La evidencia de suites de cifrado identificada incluye detalles del RC4 basado en el protocolo SSL/TLS		

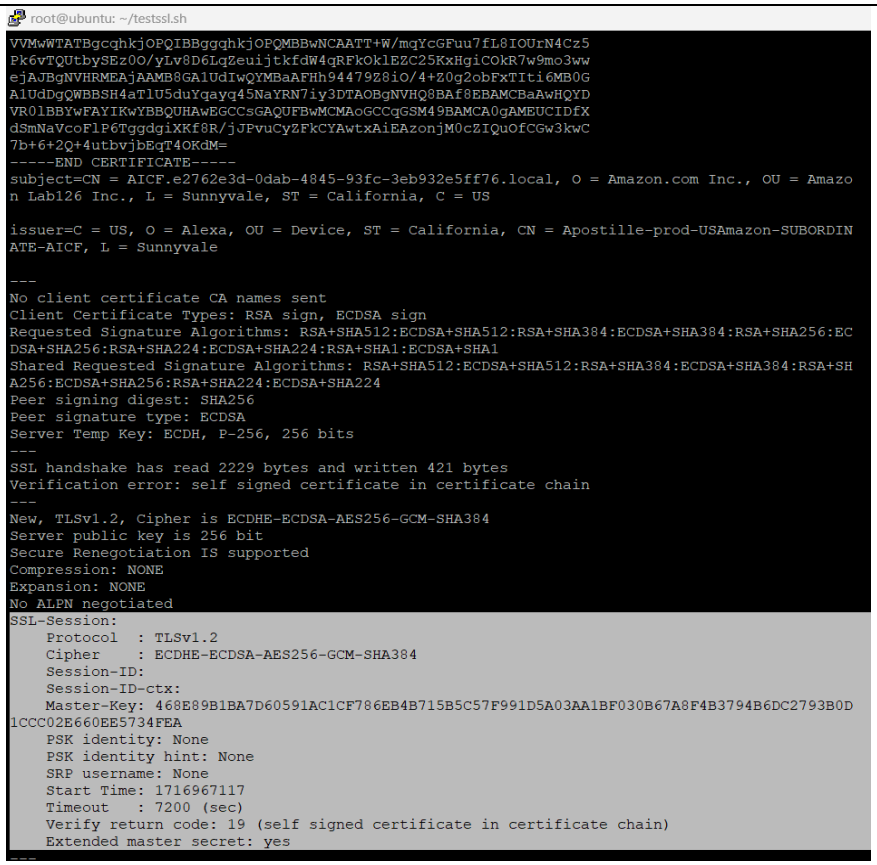


Figura D7. Evidencia de suit de cifrado identificados en ALEXA-TARGET.

Remediación: "Reconfigure la aplicación afectada, si es posible, para evitar el uso de RC4 cifrados. Considere usar TLS 1.2 con suites AES-GCM sujetas al navegador y soporte de servidor web."

Tabla D9. TLS Version 1.1 Deprecated Protocol

Vulnerabilidad: TLS Version 1.1 Deprecated Protocol		**CVE:** CVE-2020-7061, CVE-2020-7062, CVE-2020-7063
Impacto: Medio	**Probabilidad:** Baja	**Riesgo:** Bajo
CVSS2: 6.1		**CVSS3: 6**.5
IP Vulnerables: 10.10.10.220		
Descripción de vulnerabilidad: El servicio remoto acepta conexiones cifradas usando TLS 1.1. TLS 1.1 carece de soporte para las actualizaciones actuales y recomendadas. Cifrados que admiten cifrado antes del cálculo MAC y modos de cifrado autenticados como GCM no se puede utilizar con TLS 1.1 La vulnerabilidad se detecta en los puertos TCP: 10001		
Impacto de la vulnerabilidad: -		
Evidencias de la vulnerabilidad: Se identifica el certificado con el uso de cifrado TLS 1.1. Por medio de una máquina virtual Ubuntu, se ejecuta el script testssl.sh con el objetivo de realizar una evaluación de seguridad sobre el dispositivo que se encuentra en la dirección IP 10.10.10.220 y en el puerto 10001.		

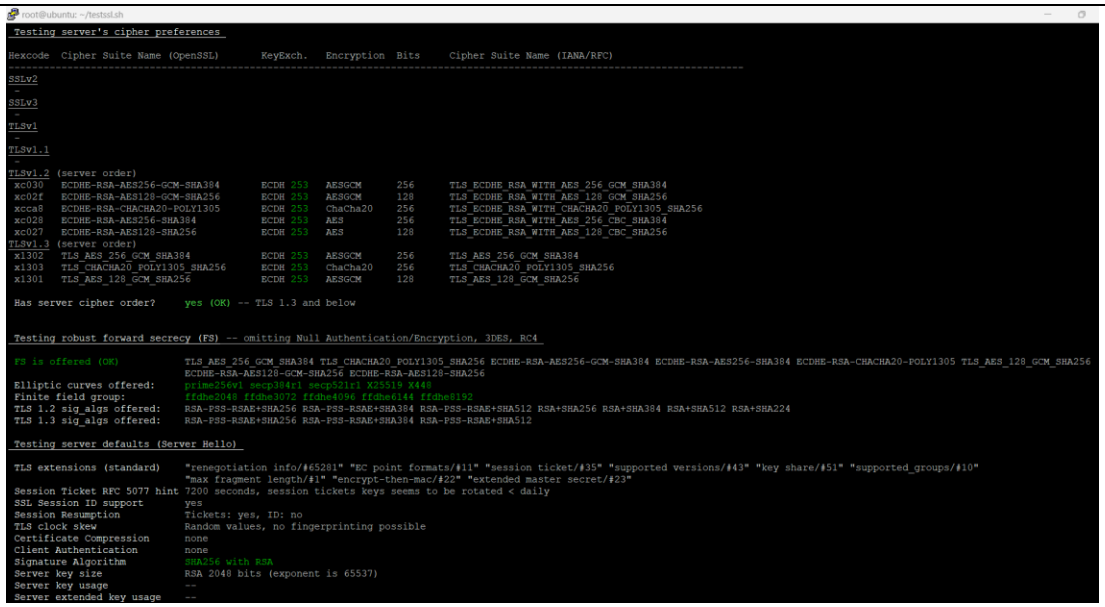


Figura D8. Evidencia de uso de versión de servicio TLS 1.1 en TPOT.

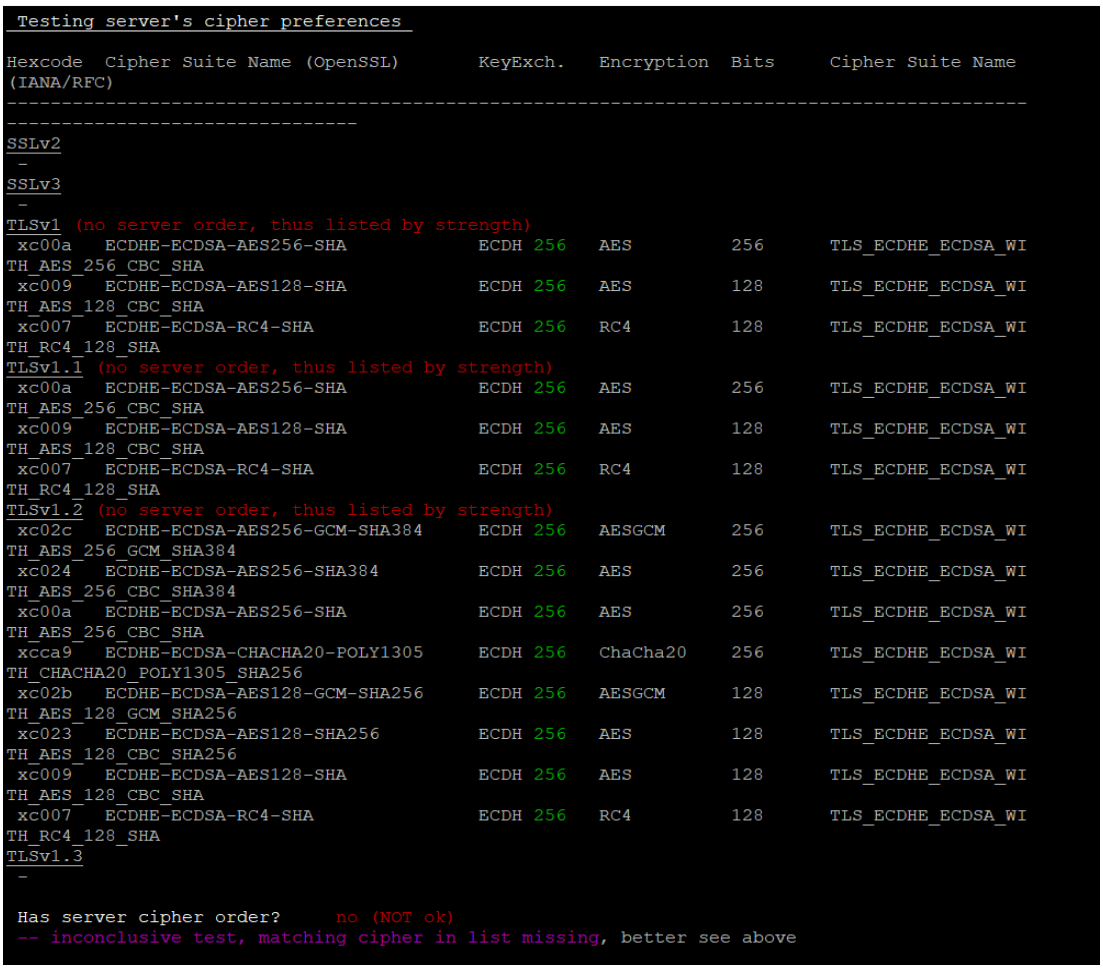


Figura D9. Evidencia de uso de versión de servicio TLS 1.1 en ALEXA-TARGET.

Remediación: Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.

4.1.3. Hacking Network Wireless

a. Identificación

El ataque se lleva a cabo utilizando una tarjeta WiFi en la máquina atacante con Kali Linux. Primero, se verifica que la tarjeta esté en modo Managed antes de iniciar el ataque, como se muestra en la Figura D10.

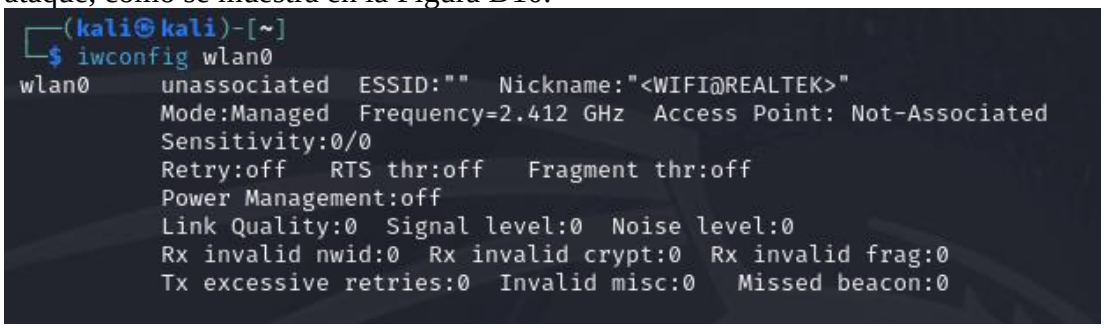


Figura D10. Verificación de la tarjeta WiFi

b. Ejecución

Desde la máquina Kali Linux, se realiza el ataque WPS Pixie-Dust, como se muestra en la Figura D11, a continuación, se detalla el proceso para este ataque:

1. El comando wifite --kill se ejecuta en la terminal de Kali Linux, iniciando la herramienta Wifite versión 2.7.0. Wifite es un auditor inalámbrico diseñado para automatizar la auditoría de redes WiFi.

2. Wifite detecta y finaliza dos procesos conflictivos:

- NetworkManager se detiene usando el comando systemctl stop NetworkManager.

- El proceso wpa_supplicant con el PID 2117 también se termina.

3. Configuración de la interfaz inalámbrica:

- La interfaz inalámbrica wlan0 con el controlador 88XXau (TP-Link AC600 wireless Realtek RTL8811AU [Archer T2U Nano]) se selecciona.

- Wifite habilita el modo monitor en wlan0, lo cual se confirma con el mensaje "enabled!".

4. Wifite escanea y muestra las redes WiFi-disponibles, listadas con los siguientes detalles:

- NUM: Número de identificación de la red.
- ESSID: Nombre de la red.
- CH: Canal de la red.
- ENCR: Tipo de encriptación (WPA, WPA2, etc.).
- PWR: Potencia de la señal.
- WPS: Indica si WPS está habilitado.
- CLIENT: Número de clientes conectados a la red.

5. La red seleccionada para el ataque es YULISA-HOME (número 7 en la lista), con WPS habilitado.

- El ataque comienza apuntando a la dirección MAC B8:69:F4:49:B5:45 de YULISA-HOME.
- Wifite utiliza un ataque conocido como "WPS Pixie-Dust", mostrando tiempos estimados de espera y ejecución:
- Espera de 5 minutos para que el objetivo aparezca.
- Después de 4 minutos y 56 segundos, Wifite comienza a enviar mensajes Pixiewps y a ejecutar el ataque Pixie-Dust.

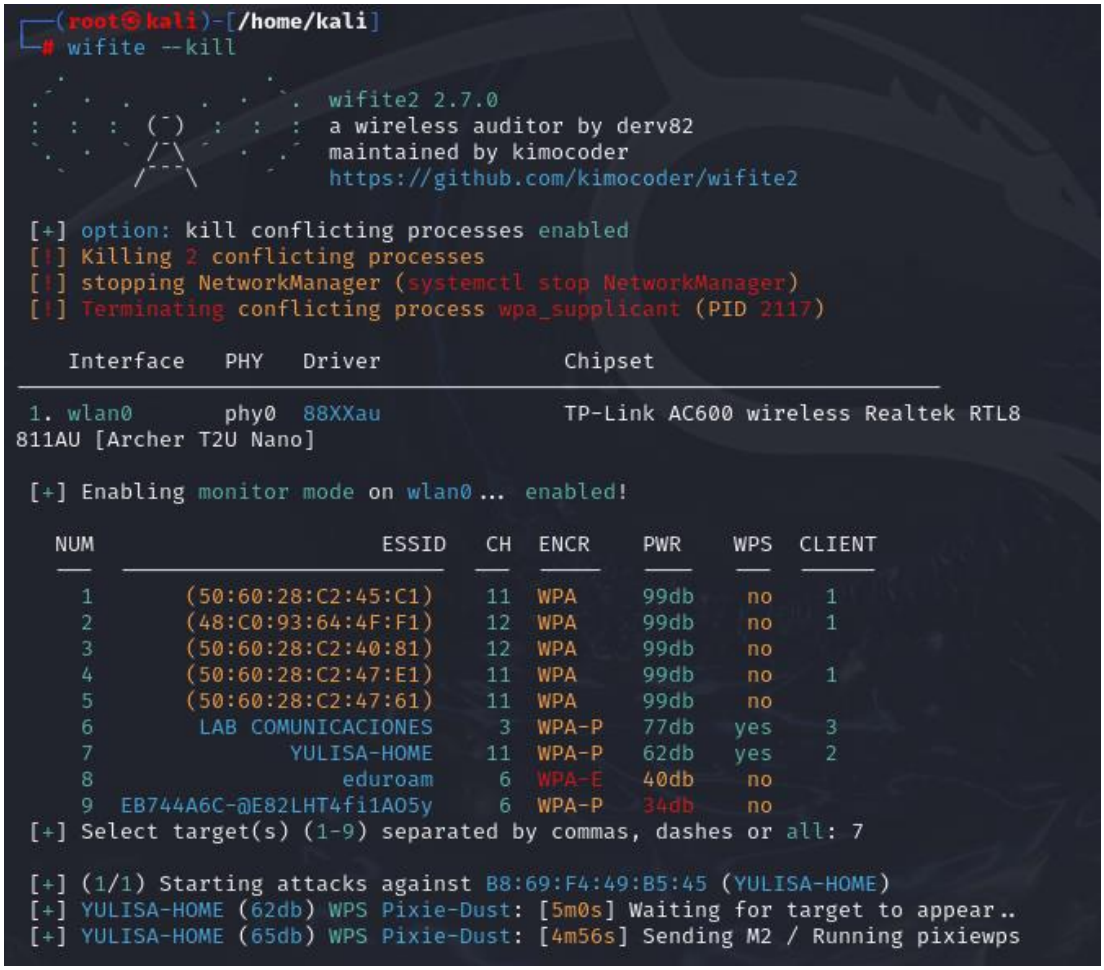


Figura D11. Escaneo de redes cercanas para realizar ataque

c. Verificación

La Figura D12, muestra la verificación del ataque a la red, descubriendo la contraseña de la red, a continuación, se detalla el proceso para descubrir la misma.

1. Análisis del archivo de handshake capturado:

- La herramienta tshark se utiliza para analizar el archivo .cap y confirmar que contiene un handshake válido para la dirección MAC 00:0b:82:e9:57:f5.

- Posteriormente, aircrack también confirma que el archivo .cap contiene un handshake válido para la misma dirección MAC.

2. Crackeo del handshake WPA:

- Se ejecuta aircrack-ng con un archivo de lista de palabras (wordlist-probable.txt) para intentar descifrar el handshake WPA.

- El proceso de crackeo comienza mostrando un avance del 0.01% y una ETA de 4 minutos y 30 segundos a una velocidad de 753.4 kps.

- El handshake WPA se crackea exitosamente, revelando la clave PSK: admin1234.

3. Información del punto de acceso:

- BSSID del punto de acceso: 00:08:82:E9:57

- Encriptación: WPA.

- Archivo de handshake: hs/handshake_Piso2_00-0B-82-E9-57-F5_2024-06-19T15-49-08.cap.

- Clave PSK (contraseña): admin1234.

4. Finalización del proceso:

- El ataque a 1 objetivo se completa y el proceso termina, indicando que la interfaz permanece en modo monitor.

- Para deshabilitar el modo monitor, se sugiere usar el comando airmon-ng stop wlan0.

- Se menciona que se puede reiniciar NetworkManager cuando se termine, utilizando el servicio NetworkManager.

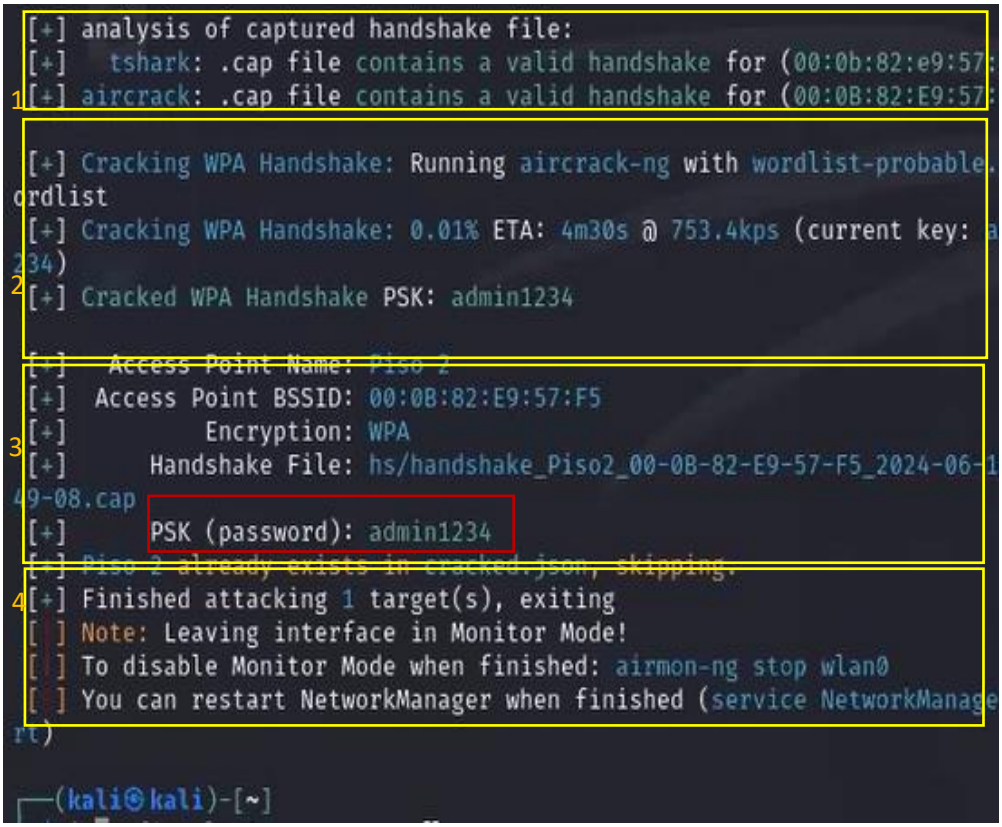


Figura D12. verificación del ataque a la red

Como resultado, se obtuvo la contraseña de la red del hogar, "admin1234", confirmando que el ataque para descubrir la contraseña de la red WiFi fue exitoso, permitiendo así el acceso no autorizado a la red del hogar.

4.1.4 Pruebas de denegación de servicio

Para ello en primera instancia se debe comprender como trabajan los dispositivos IoT, estos dispositivos en su mayoría son fabricados por Tuya

a. Identificación

Se procede con un mapeo a fin de identificar el dispositivo utilizando la herramienta Zenmap. Este proceso se inicia mediante la especificación de la dirección IP del dispositivo IoT, situada en el segmento de red 10.10.10.236. Una vez iniciado el escaneo, se observa en la Figura D13, que el mapeo muestra el servicio IRC con el puerto 6668/TCP abierto

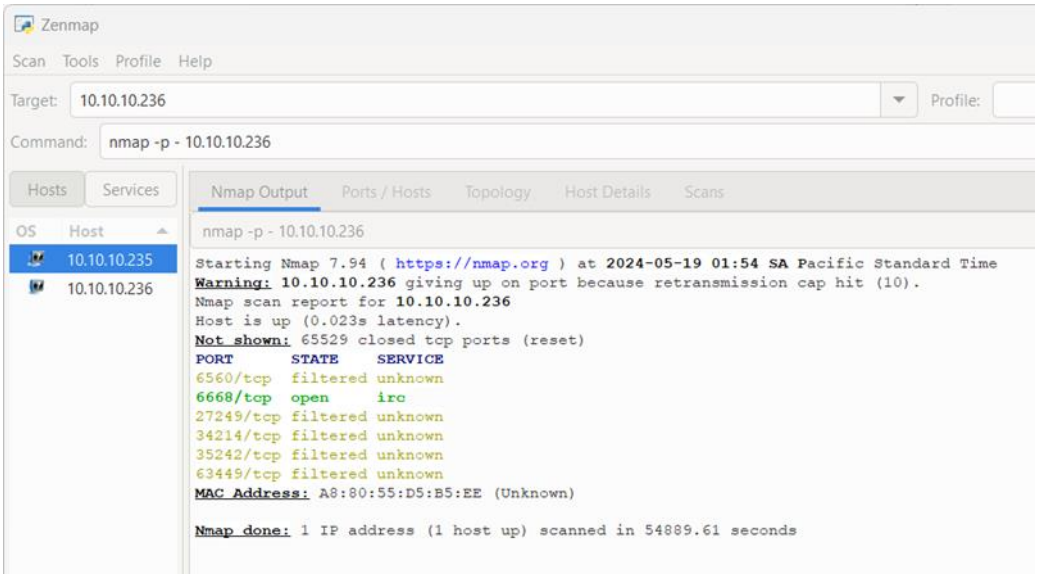


Figura D13. Mapeo de identificación

La herramienta Hércules se usa con el fin de corroborar la disponibilidad de acceso al dispositivo en cuestión por medio de TCP por el puerto 6668 como se muestra en la Figura D14. Mediante la evaluación de la conectividad se establece la capacidad de interactuar de manera efectiva con el dispositivo objetivo que en este caso es el interruptor de luz inteligente.

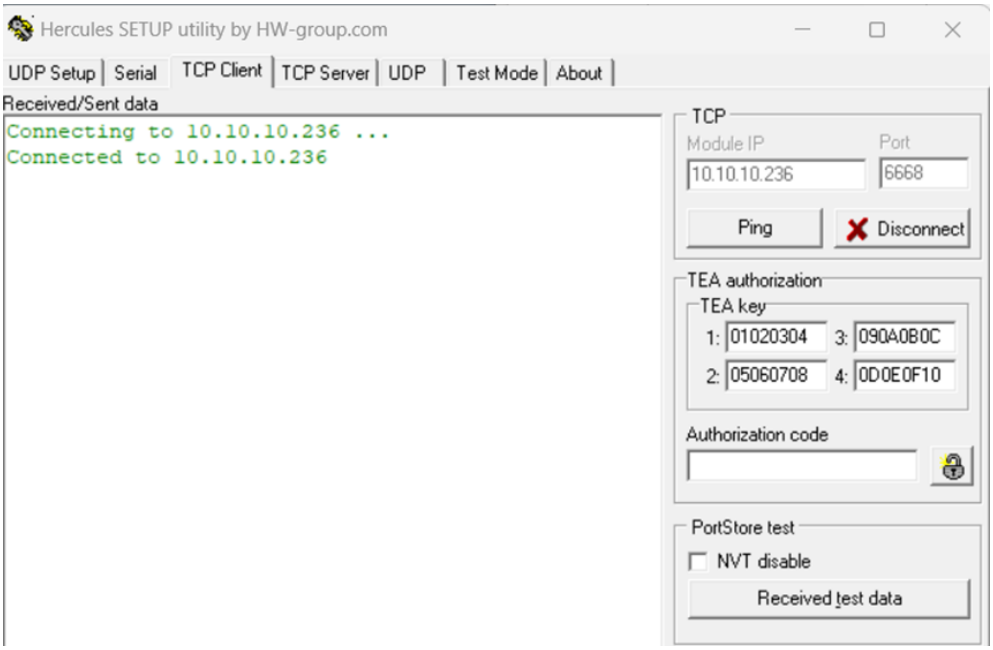


Figura D14. Acceso al dispositivo IoT con Hércules

b. Ejecución

Se realiza la captura de la trama de red utilizando la herramienta Wireshark, en la cual se observa que la dirección IP 10.10.10.236 emplea el protocolo TCP a través del puerto 6668 como se muestra en la Figura D15. Esta captura proporciona una visión detallada del tráfico de red asociado al dispositivo, permitiendo un análisis minucioso de sus comunicaciones y comportamientos en el entorno de red.

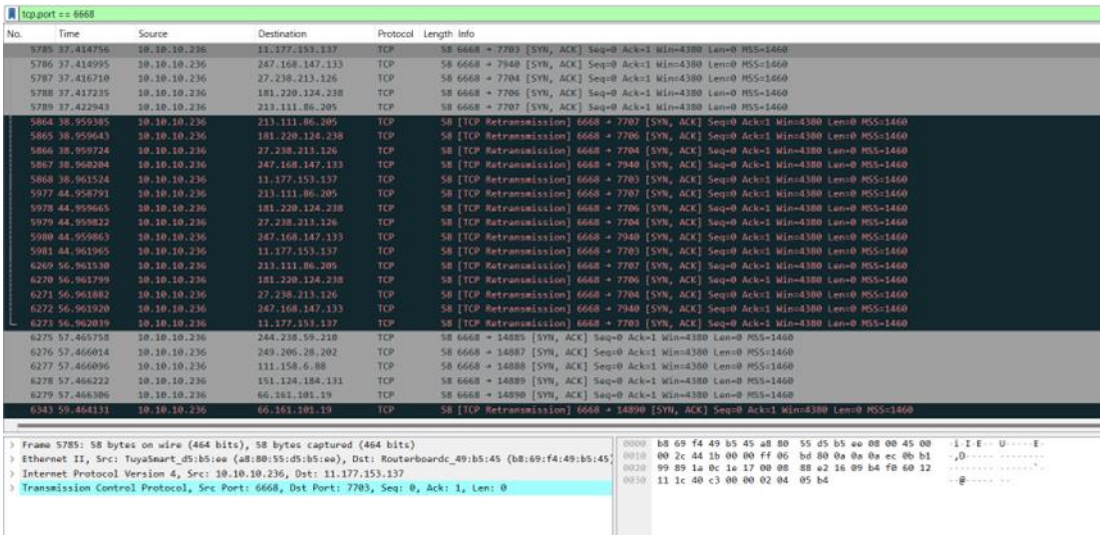


Figura D15. Captura del tráfico generado por el ataque

Utilizando la máquina Kali Linux como se muestra en la Figura D16, se ejecuta el comando hping3 –syn –rand-source –flood -p 6668 10.10.10.236 para llevar a cabo un ataque dirigido. Este comando envía un flujo continuo de paquetes SYN con direcciones de origen aleatorias hacia el puerto 6668 del dispositivo con la dirección IP 10.10.10.236, simulando un ataque de denegación de servicio (DoS) con el objetivo de evaluar la resiliencia del dispositivo frente a tales amenazas.

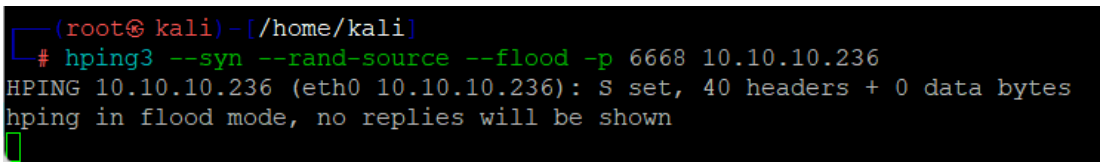


Figura D16. Ataque desde Kali Linux

Wireshark captura meticulosamente el tráfico generado por el ataque. La herramienta de análisis de red documenta cada paquete SYN enviado al puerto 6668 del dispositivo con la dirección IP 10.10.10.236 como se muestra en la Figura D17, proporcionando

una representación detallada del ataque y permitiendo una evaluación exhaustiva del impacto y la respuesta del dispositivo ante la simulación de una amenaza de denegación de servicio (DoS).

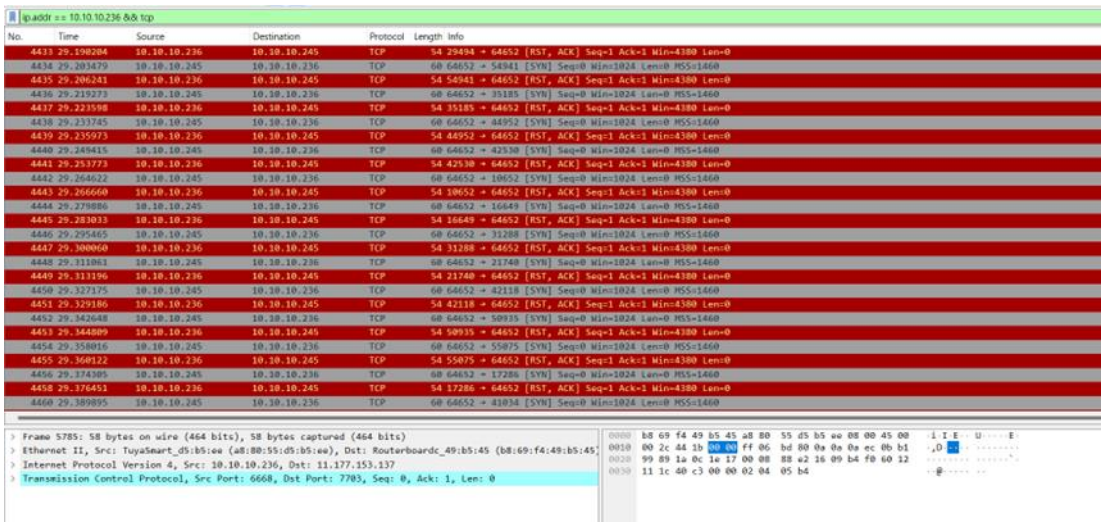


Figura D17. Captura de trama en IP 10.10.10.236

c. Verificación

Se observa en la Figura 40 que, al intentar establecer una nueva conexión mediante el protocolo TCP utilizando la herramienta Hércules y la dirección IP del dispositivo, la conexión no se establece. Cabe destacar que, durante la ejecución de este ataque, el dispositivo no muestra ninguna información ni emite alertas de intrusión, lo que indica una ausencia de mecanismos de detección o respuesta ante dicha amenaza.

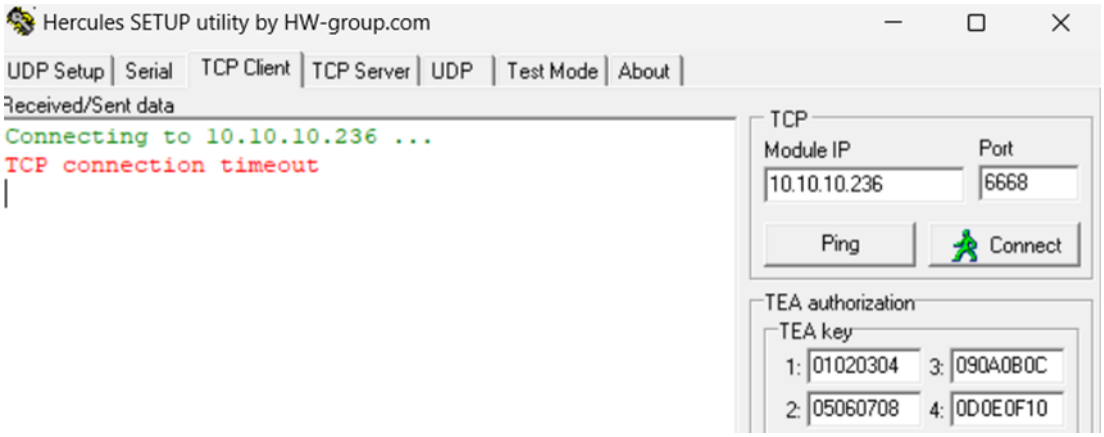


Figura D18. Resultado del ataque

4.3 Control del dispositivo IoT desde LAN

Teniendo en cuenta el funcionamiento de Tuya, se procede a controlar el dispositivo desde la LAN.

a. Identificación

A través de la utilización de Wireshark, se ha logrado identificar y capturar el tráfico de datos correspondiente al dispositivo Tuya como se observa en Figura D19. Esta captura permite un análisis detallado de las comunicaciones del dispositivo, proporcionando información sobre su comportamiento y los protocolos utilizados, lo que es fundamental para evaluar la seguridad y el funcionamiento del dispositivo en el entorno de red. Se identifica que se trata del sensor de contacto para puertas y ventanas con la IP 10.10.10.230

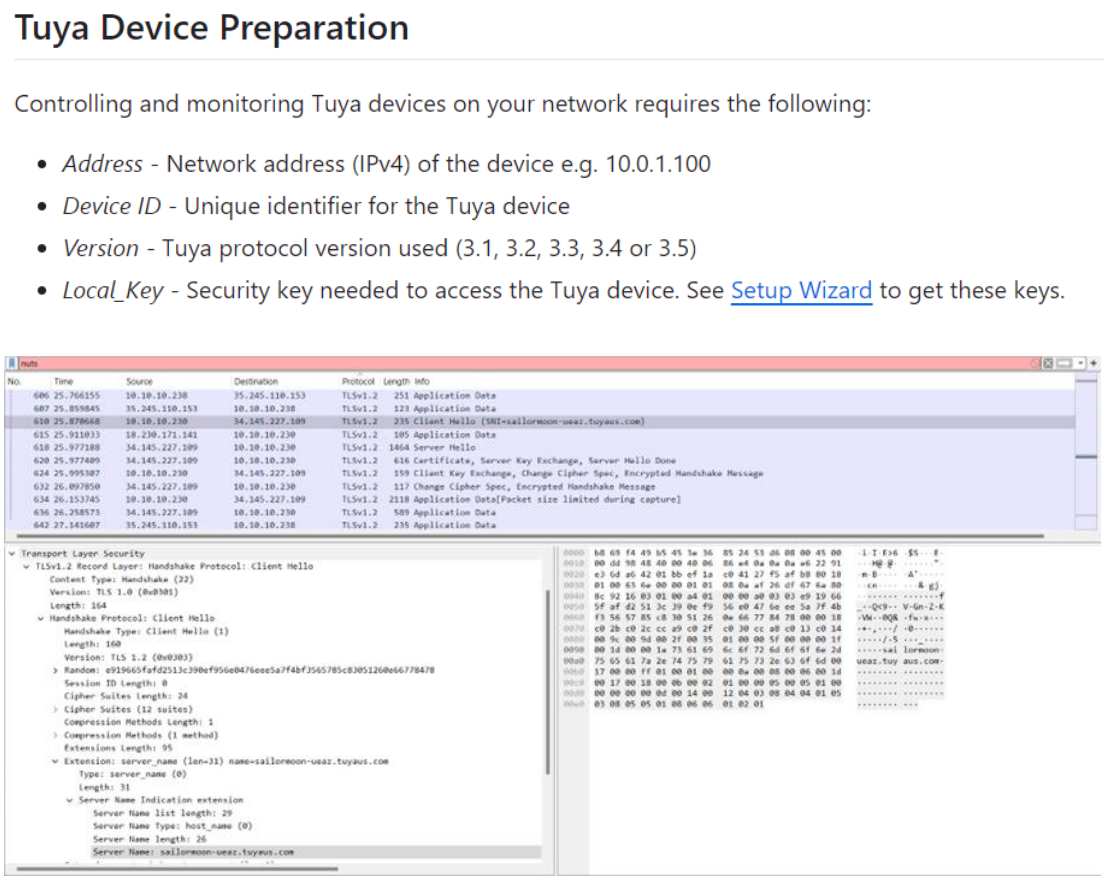


Figura D19. Captura para análisis detallado de las comunicaciones del dispositivo

La Figura D20, muestra que se usa el protocolo TLSv1.2

```
615 25.911033    18.230.171.141    10.10.10.230    TLSv1.2   105 Application Data
618 25.977188    34.145.227.109    10.10.10.230    TLSv1.2  1464 Server Hello
620 25.977409    34.145.227.109    10.10.10.230    TLSv1.2   616 Certificate, Server Key Exchange, Server Hello Done
```

Figura D20. protocolo TLSv1.2

b. Ejecución

Los dispositivos Tuya, para ser controlados y monitoreados eficazmente desde la red, presentan los siguientes requerimientos:

A través de un script desarrollado en Python, que observa en la Figura D21, se cumplen los requisitos necesarios para explotar la mencionada vulnerabilidad.


```
{
    "timestamp": 1716143549.4552615,
    "devices": [
        {
            "id": "eb172dafa876c22b295mgu",
            "ip": "10.10.10.237",
            "active": 2,
            "encrypt": true,
            "productKey": "keyjup78v54myhan",
            "token": true,
            "wf_cfg": true,
            "name": "",
            "key": "",
            "mac": "",
            "ability": 0,
            "dev_type": "default",
            "origin": "broadcast",
            "ver": "3.4"
        },
        {
            "id": "65bb4cb4fdcdfc4179qnwm",
            "ip": "10.10.10.239",
            "active": 2,
            "encrypt": true,
            "productKey": "keya4gvchmtapm8n",
            "name": "",
            "key": "",
            "mac": "",
            "ability": 0,
            "token": "",
            "wf_cfg": "",
            "dev_type": "default",
            "origin": "broadcast",
            "ver": "3.3"
        },
        {
            "id": "65b7db2d8d095c753e99vy",
            "ip": "10.10.10.235",
            "active": 2,
            "encrypt": true,
            "productKey": "7fegqgc8m0e5o7xt",
            "token": true,
            "name": "",
            "key": "",
            "mac": "",
            "ability": 0,
            "wf_cfg": "",
            "dev_type": "default",
            "origin": "broadcast",
            "ver": "3.3"
        },
        {
            "id": "eb9648371c69078677m6mn",
            "ip": "10.10.10.236",
            "active": 2,
            "encrypt": true,
            "productKey": "key5ckdnys3pqgec",
            "token": true,
            "wf_cfg": true,
            "name": "",
            "key": "",
            "mac": "",
```


Figura D21. Script para tener el control del dispositivo

c. Verificación

La Figura D22, muestra la ejecución del script diseñado para el control y monitoreo del dispositivo.

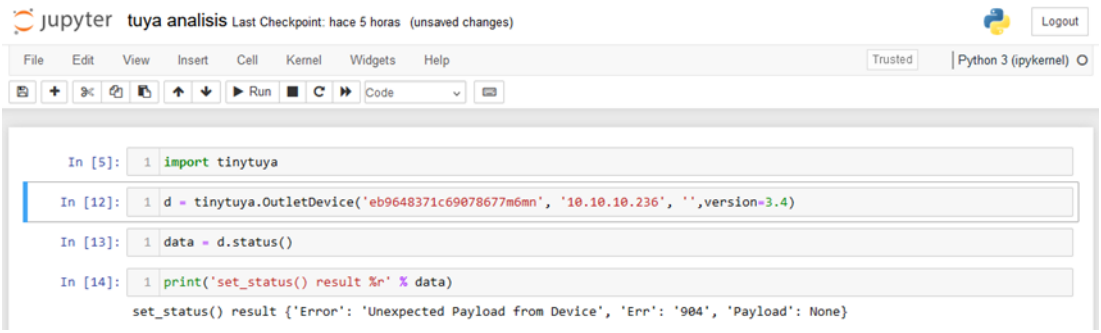


Figura D22. Verificación del control y monitoreo del dispositivo

Conclusiones

Durante el proceso de análisis y escaneo de vulnerabilidades en entornos domésticos utilizando la plataforma Nessus Tenable, se han identificado varios hallazgos significativos que requieren atención inmediata. Estas conclusiones se basan en la evaluación de la seguridad de datos, la privacidad de las personas y los dispositivos IoT, con el objetivo de fortalecer la protección de los hogares contra posibles amenazas cibernéticas. A continuación, se presentan las principales conclusiones derivadas del análisis:

Vulnerabilidades Críticas en Dispositivos IoT:

Se han identificado múltiples vulnerabilidades críticas en dispositivos IoT, incluyendo cámaras de seguridad inteligentes, termostatos conectados y dispositivos de domótica. Estas vulnerabilidades podrían ser explotadas por atacantes para acceder de forma no autorizada a datos sensibles o comprometer la integridad de los dispositivos.

- **Débil Configuración de Redes Domésticas:**

Se observó una configuración deficiente en las redes domésticas, con contraseñas predeterminadas y protocolos de seguridad débiles en routers y puntos de acceso Wi-Fi. Esto aumenta el riesgo de intrusiones externas y compromete la privacidad de la red doméstica.

- **Riesgos Asociados a la Privacidad:**

Se encontraron vulnerabilidades que podrían afectar la privacidad de las personas en el hogar, como la exposición de datos personales a través de dispositivos IoT comprometidos. Estos riesgos deben ser abordados para proteger la privacidad y la integridad de los datos de los residentes.

- **Necesidad de Actualizaciones y Parches:**

Se identificó la falta de actualizaciones y parches en varios dispositivos IoT y sistemas informáticos, lo que deja a los hogares vulnerables a exploits conocidos. Es crucial implementar medidas de seguridad proactivas, como la aplicación regular de parches y actualizaciones de firmware, para mitigar estos riesgos.

- **Importancia de la Educación en Seguridad Cibernética:**

Se destaca la importancia de la educación en seguridad cibernética para los usuarios domésticos, con el fin de concienciar sobre las prácticas seguras en el uso de dispositivos IoT y redes domésticas. La capacitación en seguridad cibernética puede ayudar a prevenir ataques y mejorar la resiliencia frente a amenazas emergentes.

En resumen, el análisis realizado resalta la necesidad urgente de mejorar la seguridad y privacidad en los entornos domésticos, mediante la implementación de medidas de mitigación adecuadas y la promoción de una cultura de seguridad cibernética. Al abordar las vulnerabilidades identificadas y fortalecer las defensas cibernéticas, se puede garantizar un entorno doméstico más seguro y protegido contra las amenazas digitales en constante evolución.

Recomendaciones

- **Actualización y Parcheo Regular de Dispositivos IoT y Sistemas Informáticos:**

Implementar un programa de actualización regular de firmware y aplicar parches de seguridad en todos los dispositivos IoT y sistemas informáticos del hogar. Esto ayudará a mitigar vulnerabilidades conocidas y a mantener los dispositivos protegidos contra exploits y ataques.

- **Fortalecimiento de la Configuración de Redes Domésticas:**

Configurar contraseñas seguras y únicas para todos los dispositivos de red, incluyendo routers, puntos de acceso Wi-Fi y dispositivos IoT. Además, activar la autenticación de dos factores cuando sea posible y deshabilitar el acceso remoto no necesario para reducir la superficie de ataque.

- **Educación en Seguridad Cibernética para los Residentes del Hogar:**

Proporcionar capacitación y concienciación en seguridad cibernética a todos los miembros del hogar, enfatizando la importancia de prácticas seguras, como la creación de contraseñas robustas, la identificación de correos electrónicos y enlaces sospechosos, y la actualización regular de software.

- **Implementación de Soluciones de Seguridad Adicionales:**

Considerar la instalación de soluciones de seguridad adicionales, como firewalls de próxima generación, software antivirus y soluciones de detección de intrusiones, para fortalecer las defensas cibernéticas del hogar. Estas medidas pueden ayudar a detectar y prevenir ataques cibernéticos antes de que causen daños significativos.

Firma de Responsabilidad

Nombre / Cargo	Institución / Empresa	Firma
Yulisa Acosta	**FAMILIA XYZ**	

Anexo E. Análisis de red con la herramienta Nessus

Una vez se ha ingresado a Nessus se realiza un nuevo escaneo de toda la red, para ello se coloca la IP de la red con la respectiva mascara como se muestra en la Tabla E1 y Figura E1.

Tabla E1. IPs de los dispositivos IoT

Dispositivo	**IP**
Camara inteligente para interiores	10.10.10.221
Sensor de contacto para puertas	10.10.10.230
Sensor de contacto para puertas	10.10.10.216
Enchufe inteligente	10.10.10.239
Enchufe inteligente	10.10.10.222
Interruptor de luz inteligente	10.10.10.236
Echo dot	10.10.10. 220
Bombilla inteligente	10.10.10.238
Bombilla inteligente	10.10.10.218

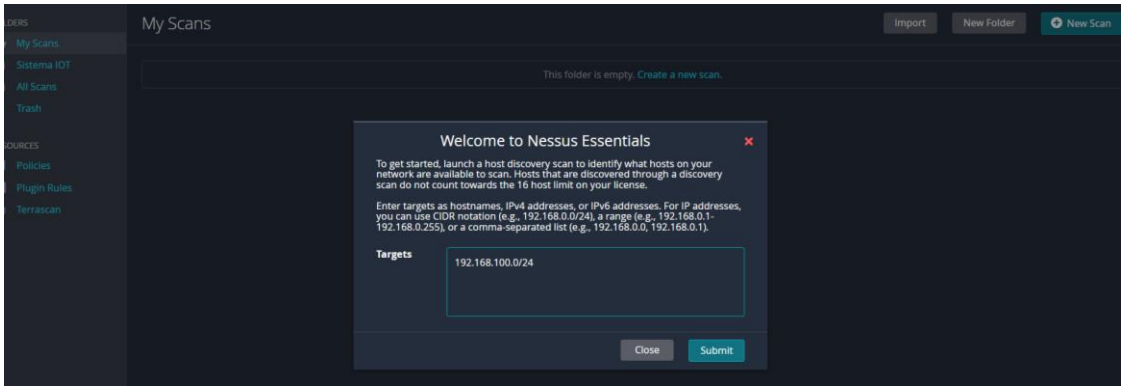


Figura E2. Nuevo escaneo en Nessus

Una vez transcurrido el tiempo de espera, concluye el escaneo de la red, dando lugar a una interfaz que facilita la observación detallada de los resultados obtenidos durante el escaneo, de la Figura E3 a la E11 se muestra el reporte generado por la herramienta Nessus.



tenable Nessus

Report generated by Nessus™

PRUEBA

Wed, 29 May 2024 01:04:07 SA Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.10.10.217
- 10.10.10.218
- 10.10.10.220
- 10.10.10.221
- 10.10.10.222
- 10.10.10.236
- 10.10.10.238
- 10.10.10.239
- 10.10.10.242

Vulnerabilities by Host

Collapse All | Expand All

10.10.10.217

0	1	3	1	1039
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.10.10.217
MAC Address:	04:EB:B9:91:62:2F
OS:	FreePBX SIP Device

Vulnerabilities

71783 - Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS

Synopsis

The remote NTP server is affected by a denial of service vulnerability.

Description

The version of ntpd running on the remote host has the 'monlist'
command enabled. This command returns a list of recent hosts that have connected to the service. However, it is affected by a denial of service vulnerability in ntp_request.c that allows an unauthenticated, remote attacker to saturate network traffic to a specific IP address by using forged REQ_MON_GETLIST or REQ_MON_GETLIST_1 requests.
Furthermore, an attacker can exploit this issue to conduct reconnaissance or distributed denial of service (DDoS) attacks.

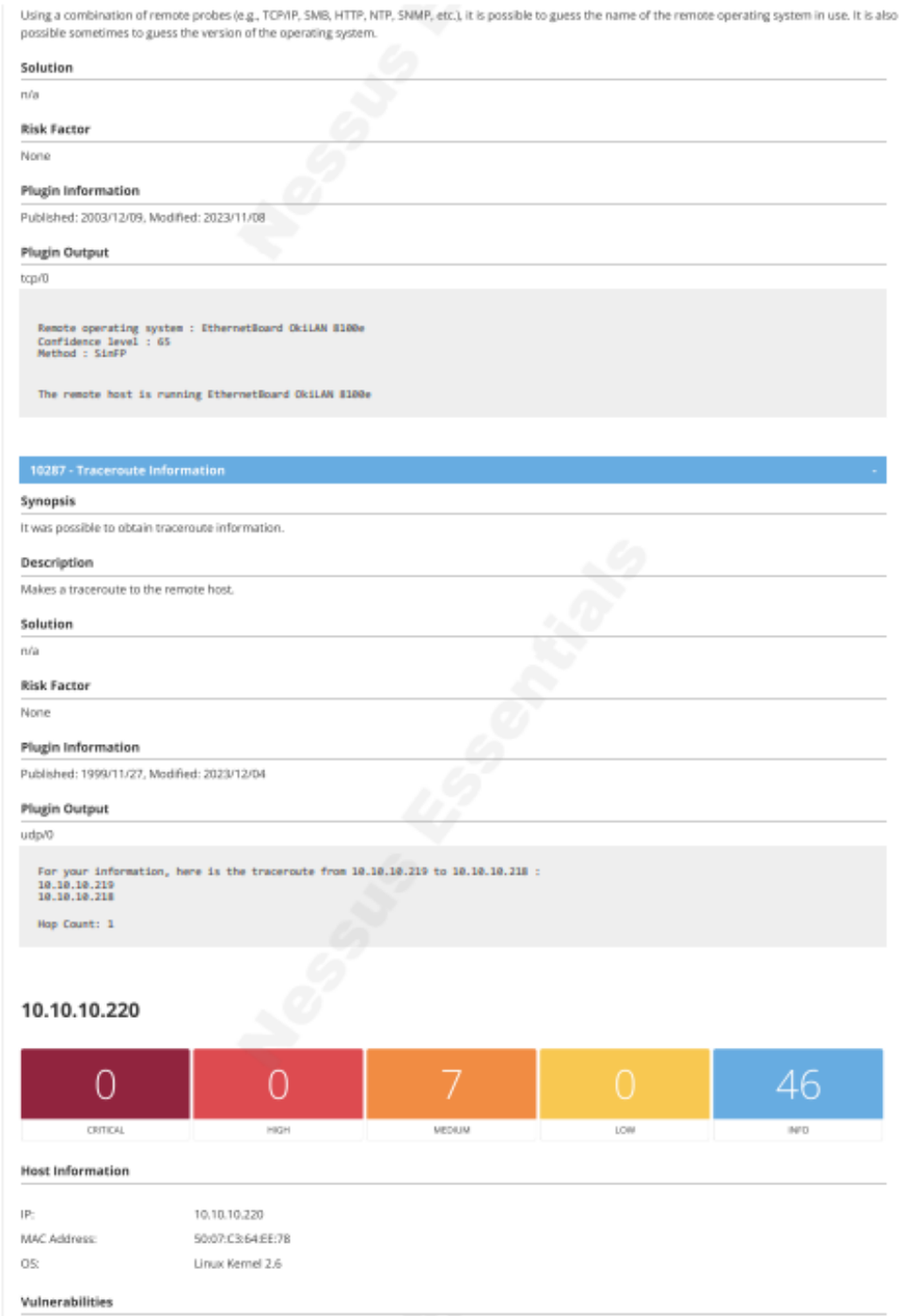
See Also

https://isc.sans.edu/diary/NTP+reflection+attack/17300
http://bugs.ntp.org/show_bug.cgi?id=1532
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10613

Figura E4. Reporte de Nessus



Figura E5. Reporte de Nessus IP 10.10.10.218



Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : EthernetBoard OkiLAN 8100e
Confidence level : 65
Method : SinFP

The remote host is running EthernetBoard OkiLAN 8100e
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.10.10.219 to 10.10.10.218 :
10.10.10.219
10.10.10.218

Hop Count: 1
```

10.10.10.220

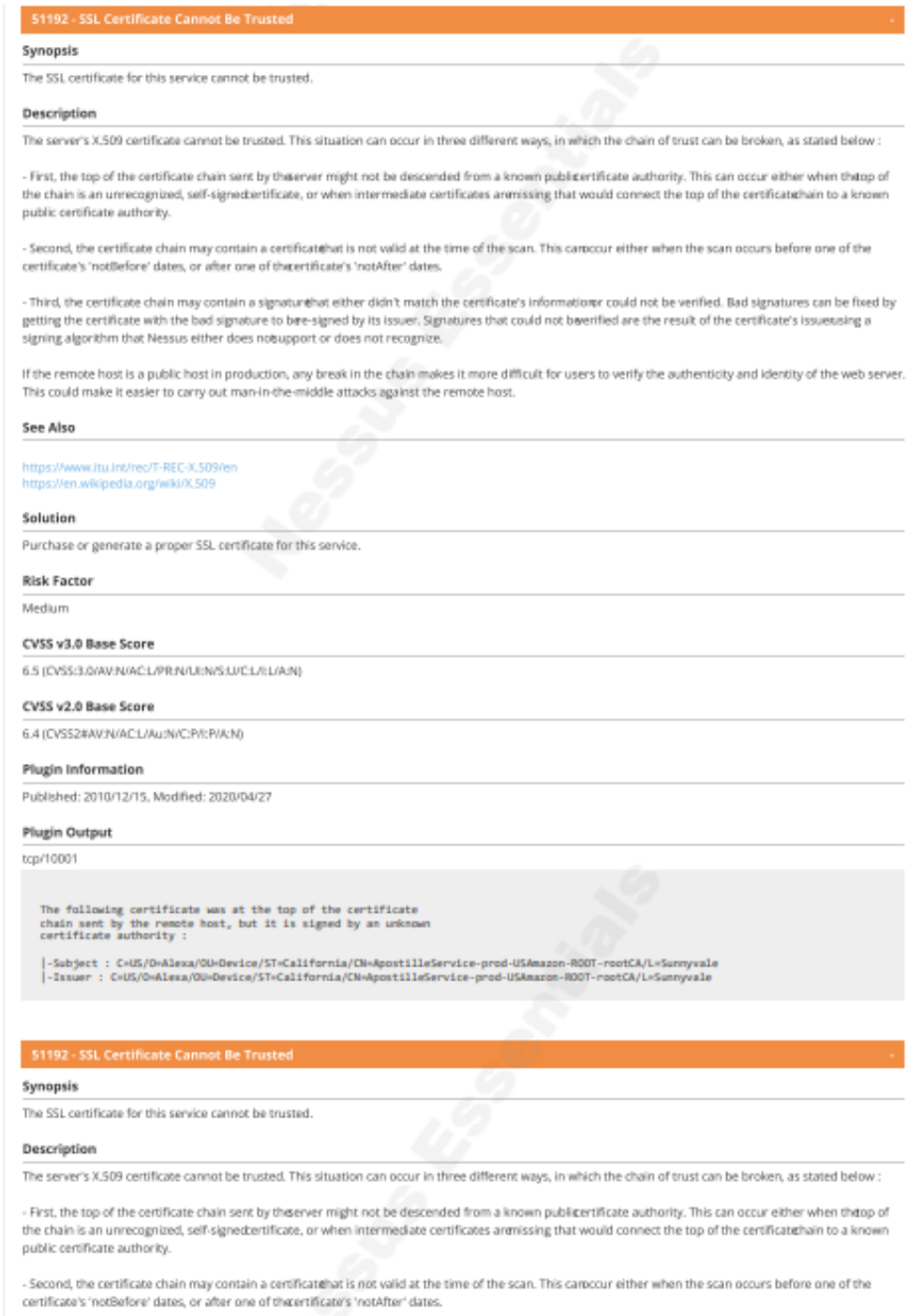
0	0	7	0	46
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.10.10.220
MAC Address:	50:07:C3:64:EE:78
OS:	Linux Kernel 2.6

Vulnerabilities

Figura E6. Reporte de Nessus IP 10.10.10.220



51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/10001

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/O=Alexa/OU=Device/ST=California/CN=ApostilleService-prod-USAmazon-ROOT-rootCA/L=Sunnyvale
|-Issuer : C=US/O=Alexa/OU=Device/ST=California/CN=ApostilleService-prod-USAmazon-ROOT-rootCA/L=Sunnyvale
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Figura E7. Reporte de Nessus IP 10.10.10.220



If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/55442/www

10.10.10.221

0	0	0	1	9
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.10.10.221
MAC Address:	A0:92:08:99:CE:7D
OS:	Linux Kernel 2.6

Vulnerabilities

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp requestThis allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

4.2

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

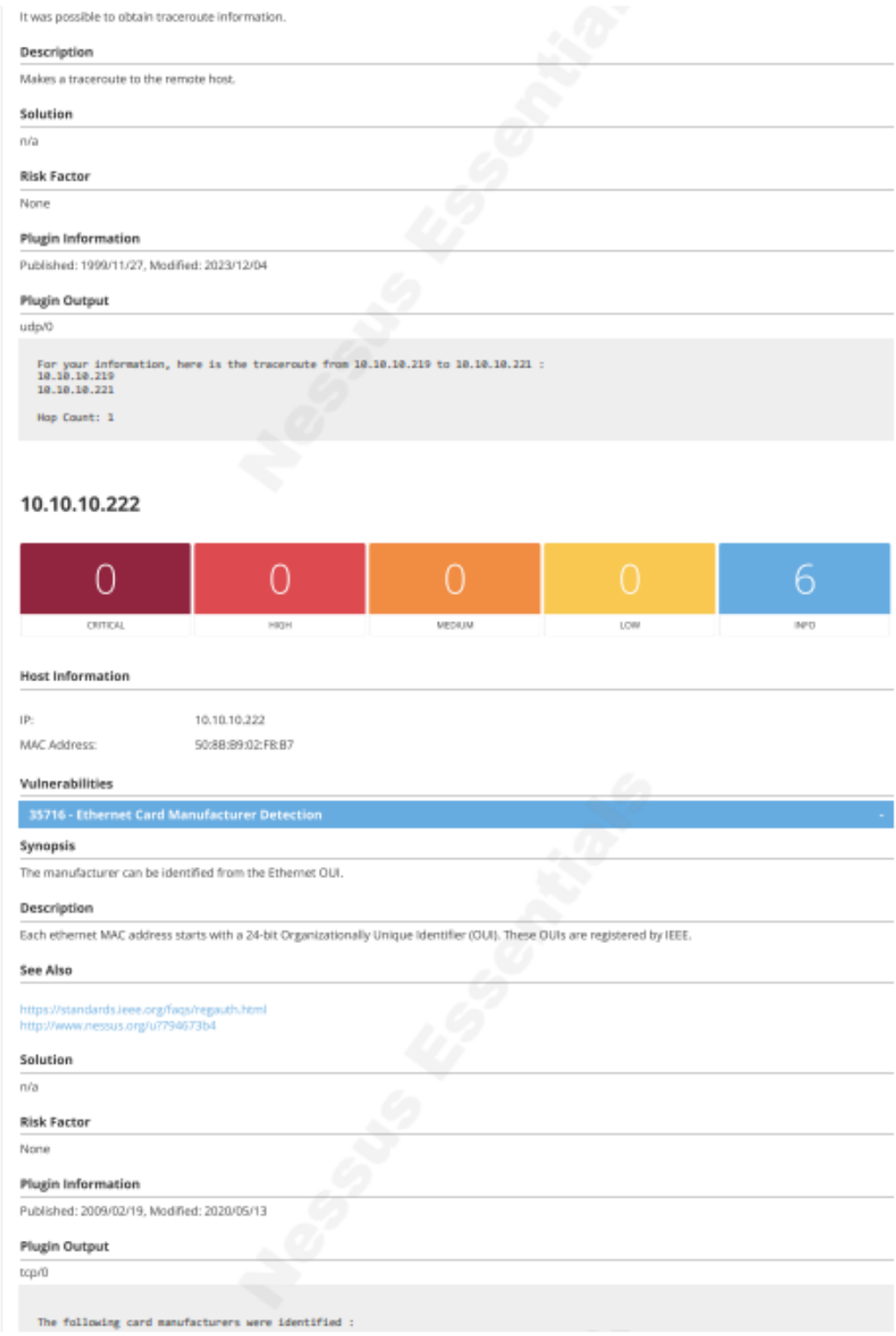
CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

Figura E8. Reporte de Nessus IP 10.10.10.221


It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.10.10.219 to 10.10.10.221 :
10.10.10.219
10.10.10.221

Hop Count: 1
```

10.10.10.222

0	0	0	0	6
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.10.10.222
MAC Address:	50:8B:B9:02:FB:B7

Vulnerabilities

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

Figura E9. Reporte de Nessus IP 10.10.10.222



Plugin Information

Published: 2010/10/26, Modified: 2020/01/22

Plugin Output

tcp/0

```
If you think these signatures would help us improve OS fingerprinting,
please send them to :

os-signatures@nessus.org

Be sure to include a brief description of the device itself, such as
the actual operating system or product / model names.

SinFP:!:
P1:B11013:F0x12:W4380:O0204ffff:M1460:
P2:B11013:F0x12:W4380:O0204ffff:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:190803_7_p=6668
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.10.10.219 to 10.10.10.222 :
10.10.10.219
10.10.10.222

Hop Count: 1
```

10.10.10.236

0	0	0	0	7
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.10.10.236
MAC Address:	A8:80:55:D5:B5:EE
OS:	EthernetBoard OkiLAN 8100e

Vulnerabilities

54615 - Device Type

Synopsis

Figura E10. Reporte de Nessus IP 10.10.10.236

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.10.10.219 to 10.10.10.236 :
10.10.10.219
10.10.10.236

Hop Count: 1
```

10.10.10.238

0	0	0	0	7
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.10.10.238
MAC Address:	1C:90:FF:EC:61:84
OS:	EthernetBoard OkiLAN 8100e

Vulnerabilities

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : switch
Confidence level : 65
```

35716 - Ethernet Card Manufacturer Detection

Figura E11. Reporte de Nessus IP 10.10.10.238



10.10.10.239

0	0	0	0	7
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP: 10.10.10.239
MAC Address: FC:67:1F:F9:C2:D1
OS: EthernetBoard OkiLAN 8100e

Vulnerabilities

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : switch
Confidence level : 65
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?7940573b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

Figura E12. Reporte de Nessus IP 10.10.10.239

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : EthernetBoard OkiLAN 8100e
Confidence level : 65
Method : SinFP

The remote host is running EthernetBoard OkiLAN 8100e
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.10.10.219 to 10.10.10.239 :
10.10.10.219
10.10.10.239

Hop Count: 1
```

10.10.10.242

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	1	20

Host Information

IP:	10.10.10.242
MAC Address:	04:EB:B9:91:62:2F
OS:	Linux Kernel 2.6

Vulnerabilities

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Nessus Essentials

Figura E13. Reporte de Nessus IP 10.10.10.242

Anexo F. Políticas

Se han establecido políticas para asegurar el sistema IoT doméstico, con el objetivo de proteger la integridad, confidencialidad y disponibilidad de los dispositivos conectados. Estas medidas buscan mitigar los riesgos asociados con el uso de dispositivos IoT en el hogar, garantizando un entorno más seguro y protegido contra posibles amenazas. Las políticas que se desarrollan son:

1. Política de Contraseñas Seguras
2. Política de Actualización de Software
3. Política de Acceso y Autorización
4. Política de Privacidad de Datos
5. Política de Monitoreo y Detección de Amenazas
6. Política de Respuesta a Incidente
7. Política de Educación y Concientización
8. Política de Evaluación de Riesgos y Cumplimiento

1. Política de Contraseñas Seguras

Objetivo:

Establecer directrices y procedimientos claros para garantizar la creación, gestión y protección adecuada de las contraseñas utilizadas en todos los sistemas de información de la organización.

Alcance:

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier otra entidad que acceda a los sistemas de información de la organización. Se extiende a todos los dispositivos y aplicaciones que requieren autenticación mediante contraseñas para acceder a los recursos de la organización, ya sea interna o externamente.

Definiciones:

Contraseña: Una secuencia de caracteres utilizada para autenticar la identidad de un usuario y permitir el acceso a sistemas, aplicaciones o datos protegidos.

Fuerza Bruta: Un método de ataque en el que un atacante intenta descubrir una contraseña probando todas las combinaciones posibles de caracteres hasta encontrar la correcta.

Hashing: Un proceso de transformación de una contraseña en una cadena de caracteres alfanuméricos irreconocible mediante un algoritmo matemático, utilizado para almacenar contraseñas de forma segura.

Salting: Un método de seguridad que consiste en agregar información adicional aleatoria a una contraseña antes de aplicar el hashing, con el fin de aumentar su seguridad y resistencia a los ataques de fuerza bruta.

Funciones y Responsabilidades:

El departamento de Seguridad de la Información (SI) será responsable de establecer y mantener las directrices y procedimientos relacionados con las contraseñas seguras, así como de monitorear su cumplimiento en toda la organización.

Los administradores de sistemas serán responsables de implementar controles técnicos para hacer cumplir las políticas de contraseñas seguras, incluyendo la configuración de políticas de contraseñas en sistemas y aplicaciones, así como la implementación de mecanismos de autenticación multifactorial cuando sea necesario.

Todos los usuarios serán responsables de crear contraseñas seguras, mantenerlas confidenciales, no compartirlas con otros y cambiarlas periódicamente de acuerdo con las políticas establecidas.

Descripción:

La Política de Contraseñas Seguras establece los requisitos mínimos para la creación, gestión y uso de contraseñas en la organización. Estos requisitos incluyen la longitud mínima, la complejidad, la caducidad y la prohibición de reutilización de contraseñas anteriores. Además, se establecen pautas para la protección de contraseñas durante su almacenamiento y transmisión, incluyendo el uso de técnicas de hashing y salting para protegerlas contra ataques de fuerza bruta y ataques de diccionario.

Principios:

Las contraseñas deben ser lo suficientemente complejas como para resistir ataques de fuerza bruta y no deben basarse en información fácilmente deducible, como nombres de usuario, fechas de nacimiento o palabras del diccionario.

Las contraseñas deben ser únicas para cada cuenta y no deben ser compartidas entre usuarios o servicios.

Las contraseñas deben ser cambiadas periódicamente, y nunca deben ser almacenadas en texto claro ni transmitidas sin cifrar.

Referencias:

Normativa de seguridad de la información de la organización.

Estándares y mejores prácticas de la industria en materia de seguridad de contraseñas, como NIST SP 800-63B y OWASP Password Guidelines.

2. Política de Actualización de Software

Objetivo:

Establecer directrices y procedimientos para garantizar que todos los sistemas y aplicaciones de la organización se mantengan actualizados con los últimos parches de seguridad y actualizaciones críticas.

Alcance:

Esta política se aplica a todos los sistemas y aplicaciones utilizados por la organización, incluyendo servidores, estaciones de trabajo, dispositivos móviles y cualquier otro dispositivo o software que pueda afectar a la seguridad de la información. Se extiende a todos los empleados, contratistas, proveedores y cualquier otra entidad que tenga acceso a los sistemas de información de la organización.

Definiciones:

Actualización de Software: Proceso de aplicar cambios a un programa informático con el fin de corregir errores, mejorar el rendimiento o añadir nuevas funcionalidades.

Parche de Seguridad: Actualización de software diseñada específicamente para corregir vulnerabilidades de seguridad y proteger el sistema contra posibles ataques.

Vulnerabilidad: Debilidad en un sistema o aplicación que puede ser explotada por un atacante para comprometer la seguridad del sistema.

Funciones y Responsabilidades:

El departamento de IT será responsable de establecer y mantener un proceso de gestión de parches de seguridad, incluyendo la identificación, evaluación, implementación y verificación de las actualizaciones de software en toda la organización.

Los administradores de sistemas serán responsables de implementar parches de seguridad en los sistemas y aplicaciones bajo su responsabilidad, siguiendo los procedimientos establecidos por el departamento de IT.

Todos los usuarios serán responsables de colaborar con el departamento de IT para facilitar la implementación de parches de seguridad en sus dispositivos y aplicaciones, así como de informar cualquier problema relacionado con las actualizaciones de software.

Descripción:

La Política de Actualización de Software establece los requisitos mínimos para la gestión de parches de seguridad en la organización. Esto incluye la implementación regular de actualizaciones de software, la evaluación de la criticidad de los parches, la programación de mantenimientos regulares y la realización de pruebas de compatibilidad antes de implementar las actualizaciones en producción.

Principios:

La seguridad de los sistemas y datos de la organización tiene prioridad sobre cualquier otra consideración al aplicar actualizaciones de software.

Las actualizaciones de software deben ser implementadas de manera oportuna y eficiente, minimizando el tiempo de exposición a posibles vulnerabilidades.

Se deben realizar pruebas exhaustivas de las actualizaciones de software antes de implementarlas en entornos de producción para evitar interrupciones y fallos inesperados.

Referencias:

Políticas y procedimientos de gestión de cambios de la organización.

Normativa de seguridad de la información y mejores prácticas de la industria en materia de gestión de parches, como ISO/IEC 27001 e ITIL.

3. Política de Acceso y Autorización

Objetivo:

Establecer directrices y procedimientos para gestionar el acceso a los sistemas de información y recursos de la organización de manera segura y controlada.

Alcance:

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier otra entidad que acceda a los sistemas de información de la organización, ya sea interna o externamente. Se extiende a todos los sistemas, aplicaciones, datos y recursos de la organización, incluyendo redes, servidores, bases de datos, aplicaciones en la nube y cualquier otro medio de almacenamiento o procesamiento de información.

Definiciones:

Acceso: La capacidad de un usuario para interactuar con un sistema o recurso de la organización, ya sea para leer, modificar o ejecutar acciones sobre la información contenida en dicho sistema o recurso.

Autorización: El proceso de conceder derechos de acceso específicos a un usuario o grupo de usuarios, basado en su identidad, roles y responsabilidades en la organización.

Principio de Menor Privilegio: El principio de seguridad que establece que los usuarios deben tener solo los privilegios de acceso necesarios para llevar a cabo sus funciones laborales, sin acceso innecesario a sistemas o datos sensibles.

Funciones y Responsabilidades:

El departamento de Seguridad de la Información (SI) será responsable de establecer y mantener un marco de gestión de acceso y autorización, incluyendo políticas, procedimientos y controles técnicos para garantizar el cumplimiento de esta política.

Los administradores de sistemas serán responsables de implementar y gestionar los controles de acceso en los sistemas y aplicaciones bajo su responsabilidad, asegurando que solo los usuarios autorizados tengan acceso a los recursos adecuados.

Todos los usuarios serán responsables de solicitar acceso solo a los recursos necesarios para llevar a cabo sus funciones laborales y de cumplir con las políticas y procedimientos de seguridad de la información establecidos por el departamento de SI.

Descripción:

La Política de Acceso y Autorización establece los requisitos mínimos para la gestión de acceso a los sistemas y recursos de la organización. Esto incluye la autenticación de usuarios, la asignación de roles y privilegios, la revisión y revocación periódica de accesos, y la implementación de controles de acceso basados en el principio de menor privilegio.

Principios:

El acceso a los sistemas y recursos de la organización debe basarse en la necesidad de conocer y el principio de menor privilegio, asegurando que los usuarios solo tengan acceso a los recursos necesarios para llevar a cabo sus funciones laborales.

La autenticación de usuarios debe ser realizada de manera segura y confiable, utilizando métodos como contraseñas seguras, autenticación multifactorial y biometría cuando sea necesario.

Los derechos de acceso de los usuarios deben ser revisados y actualizados regularmente para garantizar que sigan siendo adecuados y proporcionados a sus funciones laborales.

Referencias:

Normativa de seguridad de la información de la organización.

Estándares y mejores prácticas de la industria en materia de gestión de acceso y autorización, como ISO/IEC 27002 y NIST SP 800-53.

4. Política de Privacidad de Datos

Objetivo:

Establecer directrices y procedimientos para proteger la privacidad y confidencialidad de la información personal y sensible de los individuos y entidades con las que la organización interactúa.

Alcance:

Esta política se aplica a todos los datos personales y sensibles recopilados, procesados, almacenados o compartidos por la organización, ya sea en formato digital o físico, y se extiende a todos los empleados, contratistas, proveedores y terceros que tengan acceso o manejen dicha información en nombre de la organización.

Definiciones:

Datos Personales: Cualquier información relacionada con una persona física identificada o identificable, como nombres, direcciones, números de identificación, datos de contacto, historial médico, etc.

Datos Sensibles: Categorías especiales de datos personales que pueden revelar información sobre la salud, origen étnico, creencias religiosas, orientación sexual, afiliación política, etc., y que requieren una protección adicional.

Consentimiento: Autorización expresa o implícita dada por el titular de los datos para el procesamiento de sus datos personales con fines específicos.

Funciones y Responsabilidades:

El departamento de Protección de Datos será responsable de establecer y mantener un marco de gestión de privacidad de datos, incluyendo políticas, procedimientos y controles técnicos para garantizar el cumplimiento de esta política.

Los responsables de cada área de la organización serán responsables de identificar y clasificar los datos personales y sensibles bajo su responsabilidad, así como de implementar medidas para proteger dicha información de acuerdo con esta política.

Todos los empleados y terceros que manejen datos personales serán responsables de cumplir con las políticas y procedimientos de privacidad de datos establecidos por la organización, incluyendo la protección de la información confidencial y el respeto a los derechos de los titulares de los datos.

Descripción:

La Política de Privacidad de Datos establece los principios y procedimientos para el manejo responsable de los datos personales y sensibles en la organización. Esto incluye la recopilación adecuada de datos con el consentimiento del titular, la protección de la información mediante medidas de seguridad técnicas y organizativas, la limitación de acceso y divulgación, la retención y eliminación segura de datos, y el cumplimiento de las leyes y regulaciones de protección de datos aplicables.

Principios:

Transparencia: La organización debe informar claramente a los individuos sobre cómo se recopilan, utilizan, almacenan y comparten sus datos personales, así como sobre sus derechos en relación con dichos datos.

Consentimiento: El procesamiento de datos personales debe basarse en el consentimiento del titular de los datos o en otra base legal válida, y debe limitarse a los fines para los que se recopilaron los datos.

Seguridad: Los datos personales deben ser protegidos mediante medidas técnicas y organizativas adecuadas para prevenir el acceso no autorizado, la divulgación, la alteración o la destrucción de la información.

Referencias:

Leyes y regulaciones de protección de datos aplicables, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea y la Ley de Protección de Datos Personales en otros países.

Normativa interna de la organización relacionada con la privacidad de datos, incluyendo políticas y procedimientos específicos.

5. Política de Monitoreo y Detección de Amenazas

Objetivo:

Proteger la confidencialidad, integridad y disponibilidad de la información y los recursos de la organización, mediante la detección temprana de actividades maliciosas y la implementación de medidas de respuesta adecuadas.

Alcance:

Esta política se aplica a todos los sistemas, redes y recursos de la organización, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y cualquier otro medio de procesamiento o almacenamiento de información. Se extiende a todos los empleados, contratistas, proveedores y terceros que tengan acceso o manejen información sensible en nombre de la organización.

Definiciones:

Monitoreo de Seguridad: Proceso continuo de supervisión y análisis de los eventos y actividades en los sistemas y redes de la organización para detectar posibles amenazas y vulnerabilidades.

Detección de Amenazas: Proceso de identificar actividades maliciosas o anómalas en los sistemas y redes de la organización, utilizando herramientas y tecnologías de seguridad.

Incidente de Seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de la información o los recursos de la organización, y que requiere una respuesta adecuada.

Funciones y Responsabilidades:

El departamento de Seguridad de la Información (SI) será responsable de establecer y mantener un programa de monitoreo y detección de amenazas, incluyendo la implementación de herramientas de seguridad, la configuración de alertas y la respuesta a incidentes.

Los administradores de sistemas serán responsables de configurar y mantener los sistemas y herramientas de monitoreo de seguridad, así como de responder a las alertas y eventos de seguridad según los procedimientos establecidos por el departamento de SI.

Todos los usuarios serán responsables de reportar cualquier actividad sospechosa o incidente de seguridad al departamento de SI, así como de cumplir con las políticas y procedimientos de seguridad establecidos por la organización.

Descripción:

La Política de Monitoreo y Detección de Amenazas establece los requisitos mínimos para identificar y responder a posibles amenazas a la seguridad de la información en la organización. Esto incluye la implementación de herramientas de monitoreo de seguridad, la configuración de alertas y notificaciones, la revisión y análisis de registros de eventos, y la respuesta adecuada a incidentes de seguridad.

Principios:

Proactividad: La organización debe anticiparse a posibles amenazas mediante el monitoreo continuo de los sistemas y redes, y la detección temprana de actividades maliciosas.

Colaboración: La detección y respuesta a amenazas debe ser un esfuerzo colaborativo entre el departamento de SI, los administradores de sistemas y todos los usuarios de la organización.

Mejora Continua: La organización debe revisar y mejorar continuamente sus procesos y controles de monitoreo y detección de amenazas para adaptarse a los cambios en el panorama de seguridad.

Referencias:

Normativa y estándares de seguridad de la información, como ISO/IEC 27001 y NIST SP 800-61.

Herramientas y tecnologías de seguridad, como SIEM (Security Information and Event Management), IDS (Intrusion Detection System) y IPS (Intrusion Prevention System).

6. Política de Respuesta a Incidentes

Objetivo:

Minimizar el impacto de los incidentes en la confidencialidad, integridad y disponibilidad de la información y los recursos de la organización, y garantizar una respuesta oportuna y coordinada para mitigar cualquier daño potencial.

Alcance:

Esta política se aplica a todos los sistemas, redes y recursos de la organización, así como a todos los empleados, contratistas, proveedores y terceros que tengan acceso o manejen información sensible en nombre de la organización. Se extiende a todos los tipos de incidentes de seguridad de la información, incluyendo brechas de seguridad, intrusiones, malware, fallos de seguridad, etc.

Definiciones:

Incidente de Seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de la información o los recursos de la organización, y que requiere una respuesta adecuada.

Equipo de Respuesta a Incidentes: Grupo de personas designadas para coordinar y llevar a cabo la respuesta a incidentes de seguridad de la información en la organización.

Recuperación de Incidentes: Proceso de restaurar los sistemas y recursos afectados por un incidente de seguridad a un estado operativo normal.

Funciones y Responsabilidades:

El Equipo de Respuesta a Incidentes será responsable de coordinar la respuesta a incidentes de seguridad, incluyendo la detección, evaluación, contención, recuperación y análisis de incidentes.

Los administradores de sistemas serán responsables de reportar cualquier incidente de seguridad a la línea de mando y al Equipo de Respuesta a Incidentes, así como de colaborar en la investigación y resolución del incidente.

Todos los empleados serán responsables de reportar cualquier incidente de seguridad que observen a su supervisor o al Equipo de Respuesta a Incidentes, y de seguir los procedimientos establecidos para la notificación y respuesta a incidentes.

Descripción:

La Política de Respuesta a Incidentes establece los procedimientos y protocolos para responder de manera efectiva a los incidentes de seguridad de la información en la organización. Esto incluye la detección temprana de incidentes, la evaluación de su impacto, la contención de la situación, la recuperación de los sistemas afectados y el análisis post-incidente para prevenir futuros incidentes similares.

Principios:

Rapidez: La respuesta a incidentes debe ser rápida y oportuna para minimizar el impacto en la organización.

Coordinación: La respuesta a incidentes debe ser coordinada entre todos los equipos y personas involucradas para garantizar una acción eficiente y efectiva.

Aprendizaje: Cada incidente debe ser analizado y documentado para identificar lecciones aprendidas y mejorar los procesos de respuesta a incidentes en el futuro.

Referencias:

Normativa y estándares de seguridad de la información, como ISO/IEC 27001 y NIST SP 800-61.

Procedimientos y protocolos internos de la organización relacionados con la gestión de incidentes de seguridad.

7. Política de Educación y Concientización

Objetivo:

Promover una cultura de seguridad de la información en toda la organización mediante la capacitación y sensibilización de los empleados sobre las mejores prácticas de seguridad y la importancia de proteger la información y los recursos de la organización.

Alcance:

Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que tengan acceso o manejen información sensible en nombre de la organización. Se extiende a todos los aspectos de la seguridad de la información, incluyendo la protección de datos, la seguridad informática, la conciencia de phishing, el manejo de contraseñas, etc.

Definiciones:

Concientización de Seguridad: Grado en el que los empleados comprenden la importancia de la seguridad de la información y adoptan comportamientos seguros en el manejo de la información y los recursos de la organización.

Capacitación en Seguridad: Programas educativos diseñados para proporcionar a los empleados los conocimientos y habilidades necesarios para proteger la información y los recursos de la organización.

Phishing: Técnica utilizada por los atacantes para engañar a los usuarios y obtener información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos fraudulentos o sitios web falsos.

Funciones y Responsabilidades:

El departamento de Recursos Humanos será responsable de desarrollar y coordinar programas de capacitación y concientización en seguridad de la información para todos los empleados.

Los supervisores y gerentes serán responsables de fomentar una cultura de seguridad de la información en sus equipos, proporcionando apoyo y recursos para la capacitación y concientización en seguridad.

Todos los empleados serán responsables de participar en los programas de capacitación y concientización en seguridad de la información, así como de aplicar los conocimientos adquiridos en su trabajo diario.

Descripción:

La Política de Educación y Concientización establece los requisitos para proporcionar a los empleados la capacitación y sensibilización necesarias para proteger la información y los recursos de la organización contra las amenazas de seguridad. Esto incluye la realización de programas de capacitación periódicos, la difusión de información sobre las últimas amenazas de seguridad, y la promoción de comportamientos seguros en el manejo de la información.

Principios:

Compromiso: La alta dirección debe demostrar un compromiso firme con la seguridad de la información mediante la asignación de recursos y el apoyo a programas de capacitación y concientización.

Personalización: Los programas de capacitación y concientización deben adaptarse a las necesidades y roles específicos de cada empleado en la organización.

Evaluación: La efectividad de los programas de capacitación y concientización debe ser evaluada regularmente para identificar áreas de mejora y garantizar el cumplimiento de los objetivos de seguridad.

Referencias:

Normativa y estándares de seguridad de la información, como ISO/IEC 27002 y NIST SP 800-50.

Recursos y materiales de capacitación proporcionados por organizaciones de seguridad y proveedores de tecnología.

8. Política de Educación y Concientización

Objetivo:

Promover una cultura de seguridad de la información en toda la organización mediante la capacitación y sensibilización de los empleados sobre las mejores prácticas de seguridad y la importancia de proteger la información y los recursos de la organización.

Alcance:

Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que tengan acceso o manejen información sensible en nombre de la organización. Se extiende a todos los aspectos de la seguridad de la información, incluyendo la protección de datos, la seguridad informática, la conciencia de phishing, el manejo de contraseñas, etc.

Definiciones:

Concientización de Seguridad: Grado en el que los empleados comprenden la importancia de la seguridad de la información y adoptan comportamientos seguros en el manejo de la información y los recursos de la organización.

Capacitación en Seguridad: Programas educativos diseñados para proporcionar a los empleados los conocimientos y habilidades necesarios para proteger la información y los recursos de la organización.

Phishing: Técnica utilizada por los atacantes para engañar a los usuarios y obtener información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos fraudulentos o sitios web falsos.

Funciones y Responsabilidades:

El departamento de Recursos Humanos será responsable de desarrollar y coordinar programas de capacitación y concientización en seguridad de la información para todos los empleados.

Los supervisores y gerentes serán responsables de fomentar una cultura de seguridad de la información en sus equipos, proporcionando apoyo y recursos para la capacitación y concientización en seguridad.

Todos los empleados serán responsables de participar en los programas de capacitación y concientización en seguridad de la información, así como de aplicar los conocimientos adquiridos en su trabajo diario.

Descripción:

La Política de Educación y Concientización establece los requisitos para proporcionar a los empleados la capacitación y sensibilización necesarias para proteger la información y los recursos de la organización contra las amenazas de seguridad. Esto incluye la realización de programas de capacitación periódicos, la difusión de información sobre las últimas amenazas de seguridad, y la promoción de comportamientos seguros en el manejo de la información.

Principios:

Compromiso: La alta dirección debe demostrar un compromiso firme con la seguridad de la información mediante la asignación de recursos y el apoyo a programas de capacitación y concientización.

Personalización: Los programas de capacitación y concientización deben adaptarse a las necesidades y roles específicos de cada empleado en la organización.

Evaluación: La efectividad de los programas de capacitación y concientización debe ser evaluada regularmente para identificar áreas de mejora y garantizar el cumplimiento de los objetivos de seguridad.

Referencias:

Normativa y estándares de seguridad de la información, como ISO/IEC 27002 y NIST SP 800-50.

Recursos y materiales de capacitación proporcionados por organizaciones de seguridad y proveedores de tecnología.

Anexo G. Controles

Para garantizar la seguridad de un sistema IoT doméstico, se han establecido varios controles esenciales. Estos controles están diseñados para fortalecer la defensa del sistema IoT doméstico contra una variedad de amenazas cibernéticas y van a la par con las políticas del Anexo F. Los controles que aplican para el sistema IoT domestico son:

1. Firewall
2. Actualización regular
3. Encriptación
4. Políticas de gestión

1. Control de Firewall

Descripción

Los controles de Firewall son esenciales para proteger la red de la organización contra accesos no autorizados y garantizar la seguridad de la comunicación remota. A continuación, se detallan las medidas de hardening recomendadas y un checklist para verificar la configuración adecuada de estos controles.

Hardening de Firewall

A continuación, se presentan las medidas recomendadas en la **¡Error! No se encuentra el origen de la referencia.** a la H5 para fortalecer la seguridad del Firewall:

Tabla G1. Restringir el tráfico de entrada solo a los puertos necesarios.

Restringir el tráfico de entrada solo a los puertos necesarios.
Auditora: Nmap #ip
Remediación: /ip firewall filter add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list address-list=port-scanners address-list-timeout=1w comment="Detectar escaneadores de puertos" add chain=input src-address-list=port-scanners action=drop comment="Bloquear escaneadores de puertos conocidos"
Impacto: Medio

Tabla G2. Implementar listas de control de acceso (ACLs) para filtrar el tráfico entrante y saliente.

Implementar listas de control de acceso (ACLs) para filtrar el tráfico entrante y saliente.
Auditoria: / ip firewall filter print
Remediación: /ip firewall filter add chain=forward action=accept src-address=192.168.2.0/24 dst-address=192.168.4.0/24 add chain=forward action=accept src-address=192.168.4.0/24 dst-address=192.168.2.0/24 add chain=forward action=drop src-address=192.168.2.0/24 dst-address=192.168.5.0/24 add chain=forward action=drop src-address=192.168.5.0/24 dst-address=192.168.2.0/24 add chain=forward action=accept
Impacto: Alto

Tabla G3. Configurar reglas de firewall para bloquear tráfico malicioso, como ataques de denegación de servicio (DoS) e intrusiones.

Configurar reglas de firewall para bloquear tráfico malicioso, como ataques de denegación de servicio (DoS) e intrusiones.
Auditoria: / ip firewall filter print
Remediación: /ip firewall filter add chain=input protocol=tcp tcp-flags=syn connection-limit=30,32 action=drop comment="Drop excess SYN packets to prevent SYN flood add chain=input protocol=udp action=drop comment="Drop UDP packets to prevent UDP flood add chain=input protocol=icmp action=drop comment="Drop ICMP packets to prevent ICMP flood add chain=input src-address-list=bad_ips action=drop comment="Drop traffic from known malicious Ips add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop comment="Block unauthorized SSH attempts add chain=input action=accept
Impacto: Alto

Tabla G4. Mantener actualizado el firmware y software del Firewall para parchear vulnerabilidades conocidas.

Mantener actualizado el firmware y software del Firewall para parchear vulnerabilidades conocidas.
Auditoria: /system package update check-for-updates
Remediación: /system package update check-for-updates /system package update install /system reboot /system package upgrade
Impacto: Alto

Tabla G1. Realizar pruebas periódicas de penetración para evaluar la efectividad de las reglas de Firewall.

Realizar pruebas periódicas de penetración para evaluar la efectividad de las reglas de Firewall.
Auditoria: nmap -sS -p 1-65535 <firewall_ip>
Remediación: Establecer un calendario regular para realizar pruebas de penetración Utilizar herramientas como Nmap, Metasploit, y otros escáneres de vulnerabilidades Realizar pruebas de penetración y escaneos de puertos y servicios Revisar los resultados de las pruebas para identificar fallos y vulnerabilidades Modificar y ajustar las reglas del firewall según sea necesario Documentar los hallazgos y las acciones tomadas
Impacto: Alto

Checklist de Controles

Este Checklist sirve para realizar una auditoría o revisión de la configuración y seguridad del firewall en un entorno IoT doméstico. Se aplica durante evaluaciones de seguridad para asegurar que el firewall está configurado correctamente y que las mejores prácticas de seguridad se están siguiendo. Cada control listado en la tabla es fundamental para mantener una defensa sólida contra posibles amenazas y vulnerabilidades. La auditoría se realiza marcando "SI" o "NO" para cada control, permitiendo identificar áreas que requieren mejoras para asegurar la protección efectiva del sistema.

Tabla G2. Checklist de control de firewall

Control	Descripción	SI	NO
Firewall	¿Se ha configurado correctamente el Firewall?		
Configuración de puertos	¿Se restringe el tráfico a los puertos necesarios?		
Listas de control de acceso	¿Se han implementado ACLs para filtrar el tráfico?		
Reglas de firewall	¿Se han configurado reglas para bloquear tráfico malicioso?		
Actualización del firmware	¿Se mantiene actualizado el firmware del Firewall?		
Monitoreo de eventos	¿Se registran y monitorean los eventos de Firewall?		
Pruebas de penetración	¿Se realizan pruebas periódicas de penetración?		

2. Control de Actualización Regular

Descripción

El control de actualización regular se refiere a la práctica de mantener actualizados los sistemas y software de la organización mediante la aplicación de parches de seguridad y actualizaciones. Esta medida es fundamental para proteger contra vulnerabilidades conocidas y minimizar el riesgo de ataques cibernéticos.

Funciones y Responsabilidades

Para garantizar una actualización regular efectiva, se asignan las siguientes funciones y responsabilidades:

- *Equipo de TI:* El equipo de TI es responsable de gestionar y aplicar las actualizaciones de seguridad en todos los sistemas y software de la organización. Esto incluye la identificación de parches críticos, la programación de instalaciones y la realización de pruebas de parches.

- *Usuarios Finales:* Los usuarios finales tienen la responsabilidad de informar al equipo de TI sobre cualquier problema relacionado con las actualizaciones y seguir las políticas y procedimientos establecidos para la instalación de parches. También deben estar atentos a las comunicaciones del equipo de TI sobre las actualizaciones y seguir las instrucciones proporcionadas.

- *Gestión de Riesgos:* La gestión de riesgos es responsable de supervisar el cumplimiento de la política de actualización regular y de evaluar el impacto de posibles vulnerabilidades no parcheadas en la seguridad de la organización. Esto incluye la realización de evaluaciones de riesgos periódicas y la coordinación con el equipo de TI para abordar cualquier problema de seguridad identificado.

Principios del Control

Los siguientes principios guían la implementación y gestión del control de actualización regular:

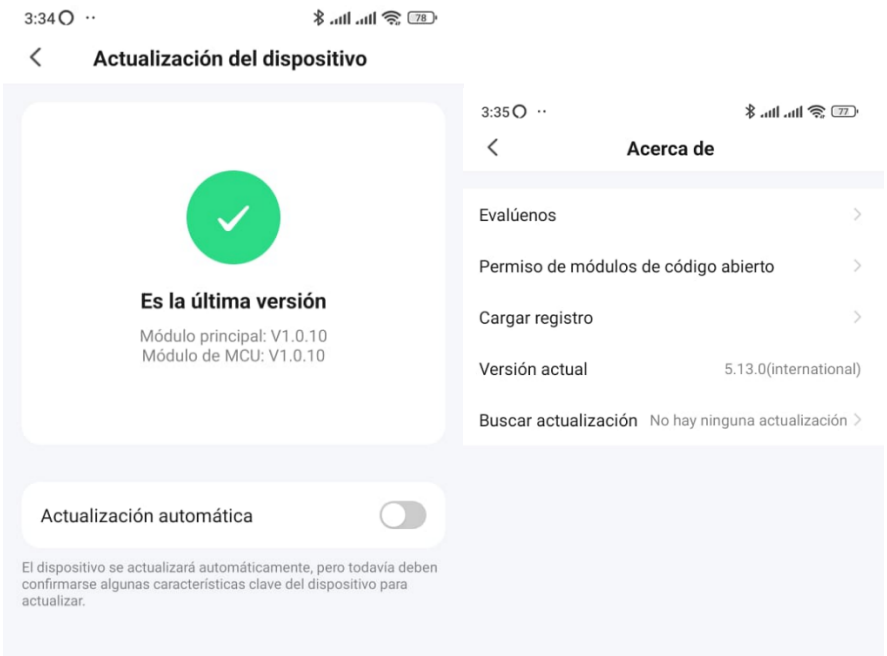
Proactividad: Se adopta un enfoque proactivo para identificar y abordar las vulnerabilidades de seguridad mediante la aplicación oportuna de parches y actualizaciones.

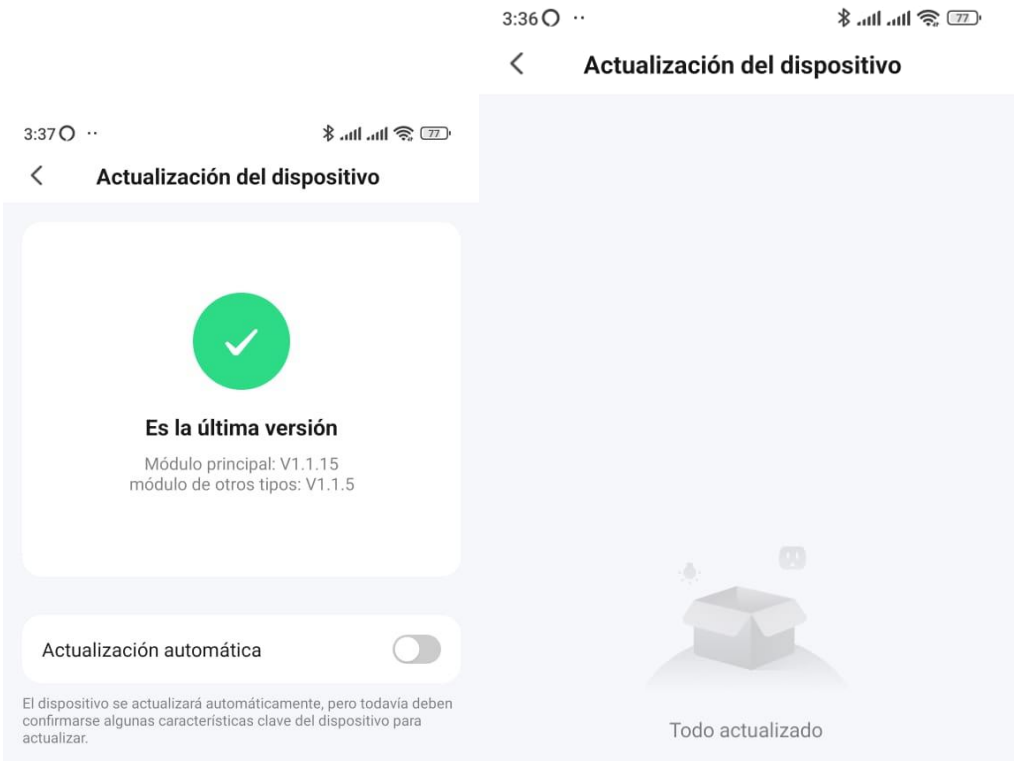
Priorización: Se priorizan las actualizaciones de seguridad críticas de acuerdo con su impacto potencial en la organización y se implementan en un plazo adecuado.

Comunicación: Se establece una comunicación clara y efectiva entre el equipo de TI y los usuarios finales para informar sobre las actualizaciones disponibles y proporcionar orientación sobre su instalación.

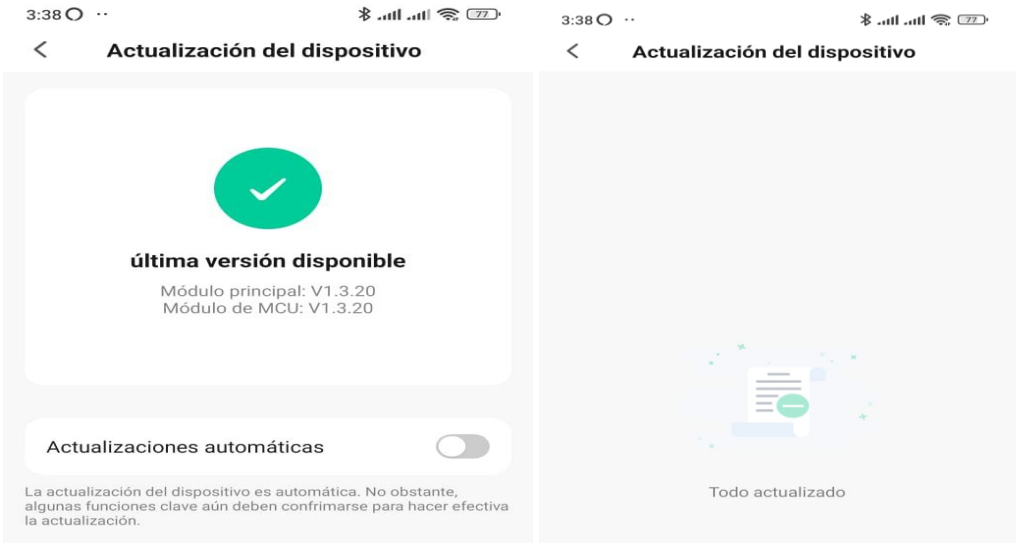
Evaluación continua: Se realiza una evaluación continua de las políticas y procedimientos de actualización regular para garantizar su eficacia y relevancia en un entorno cambiante.

Tabla G3. Procedimientos de implementación

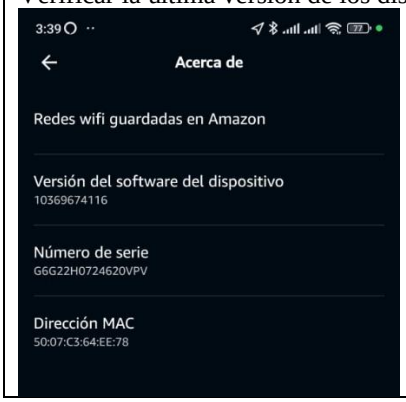
Dispositivos IoT
Auditoria: Verificar la última versión de los dispositivos Tuya y en la App Tuya  Verificar la última versión de los dispositivos Smart Life y en la App Smart Life



Verificar la última versión de los dispositivos Nexxt Solutions y en la App Nexxt Solutions



Verificar la última versión de los dispositivos Amazon



Remediación: Tener activada la opción de actualización automática en las aplicaciones de los dispositivos 
Impacto: Alto

Checklist de Control

Esta checklist sirve para realizar una auditoría o revisión de la gestión de actualizaciones de seguridad en un entorno de red, especialmente en sistemas IoT domésticos. La auditoría se realiza marcando "SI" o "NO" para cada aspecto, permitiendo identificar áreas que requieren mejoras para asegurar la protección efectiva del sistema.

Tabla G4. Checklist de control de actualización regular

Aspecto	Descripción	SI	NO
Identificación de Actualizaciones	¿Se identifican y priorizan las actualizaciones de seguridad críticas?		
Programación de Actualizaciones	¿Se programa la instalación de actualizaciones de acuerdo con un calendario establecido?		

3. Control de Encriptación

Descripción

La encriptación es una técnica fundamental en ciberseguridad que se utiliza para proteger la confidencialidad de la información mediante la conversión de datos en un formato ilegible para cualquier persona no autorizada. Este control establece las políticas y procedimientos para la implementación y gestión efectiva de la encriptación en la organización.

Funciones y Responsabilidades

Para garantizar una implementación eficaz de la encriptación, se asignan las siguientes funciones y responsabilidades:

- *Equipo de Seguridad de la Información*: Responsable de diseñar e implementar políticas y procedimientos de encriptación, así como de seleccionar y gestionar las soluciones de encriptación utilizadas en la organización.

- *Administradores de Sistemas:* Encargados de configurar y mantener las soluciones de encriptación en los sistemas y dispositivos de la organización, así como de supervisar su correcto funcionamiento.

- *Usuarios Finales:* Responsables de cumplir con las políticas de encriptación establecidas, incluida la utilización adecuada de herramientas de encriptación para proteger la información confidencial.

Principios del Control

Los siguientes principios guían la implementación y gestión del control de encriptación:

Confidencialidad: La encriptación se utiliza para proteger la confidencialidad de la información sensible y asegurar que solo las personas autorizadas puedan acceder a ella.

Integridad: La encriptación garantiza la integridad de los datos al detectar cualquier intento de modificación no autorizada.

Disponibilidad: La encriptación contribuye a garantizar la disponibilidad de los datos al protegerlos contra el acceso no autorizado y los ataques de denegación de servicio.

Checklist de Control

Este checklist sirve para realizar una auditoría o revisión de la implementación y gestión de la encriptación en un entorno de sistemas IoT domésticos. Se aplica durante evaluaciones de seguridad para asegurar que la encriptación se utiliza de manera efectiva para proteger la información confidencial. La auditoría se realiza marcando "SI" o "NO" para cada aspecto, permitiendo identificar áreas que requieren mejoras para asegurar la protección efectiva del sistema.

Tabla G5. Checklist de encriptación

Aspecto	Descripción	SI	NO
Política de Encriptación	¿Existe una política de encriptación que establece los requisitos y procedimientos para el uso de la encriptación?		
Selección de Algoritmos	¿Se han seleccionado algoritmos de encriptación sólidos y ampliamente aceptados para proteger los datos?		
Implementación en Sistemas	¿Se ha implementado la encriptación en todos los sistemas y dispositivos que manejan información confidencial?		
Gestión de Claves	¿Se tiene un proceso para la gestión segura de claves de encriptación, incluida su generación, almacenamiento y distribución?		
Auditoría y Monitoreo	¿Se realizan auditorías periódicas y se monitorean los sistemas de encriptación para detectar y responder a posibles incidentes de seguridad?		

4. Control de Políticas de Gestión

Descripción

La gestión de políticas es un componente fundamental de la seguridad de la información que implica el desarrollo, implementación y mantenimiento de políticas y procedimientos para proteger los activos de la organización y garantizar el cumplimiento de los requisitos legales y regulatorios.

Funciones y Responsabilidades

Para garantizar una gestión efectiva de las políticas, se asignan las siguientes funciones y responsabilidades:

- *Equipo de Seguridad de la Información:* Responsable de desarrollar y mantener políticas y procedimientos de seguridad de la información, así como de comunicar y hacer cumplir las políticas en toda la organización.

- *Directores y Gerentes:* Encargados de respaldar las políticas de seguridad de la información y garantizar que se asignen recursos adecuados para su implementación y cumplimiento.

- *Usuarios y Empleados:* Responsables de cumplir con las políticas y procedimientos de seguridad de la información en el curso de sus actividades laborales y reportar cualquier incidente o violación de seguridad.

Principios del Control

Los siguientes principios guían la gestión de políticas de seguridad de la información:

Consistencia: Las políticas deben ser coherentes en toda la organización y aplicarse equitativamente a todos los empleados y usuarios.

Claridad: Las políticas deben redactarse de manera clara y comprensible para que todos los usuarios puedan entender sus responsabilidades y obligaciones.

Revisión y Actualización: Las políticas deben revisarse y actualizarse regularmente para garantizar que sigan siendo relevantes y efectivas en un entorno cambiante de amenazas y tecnologías.

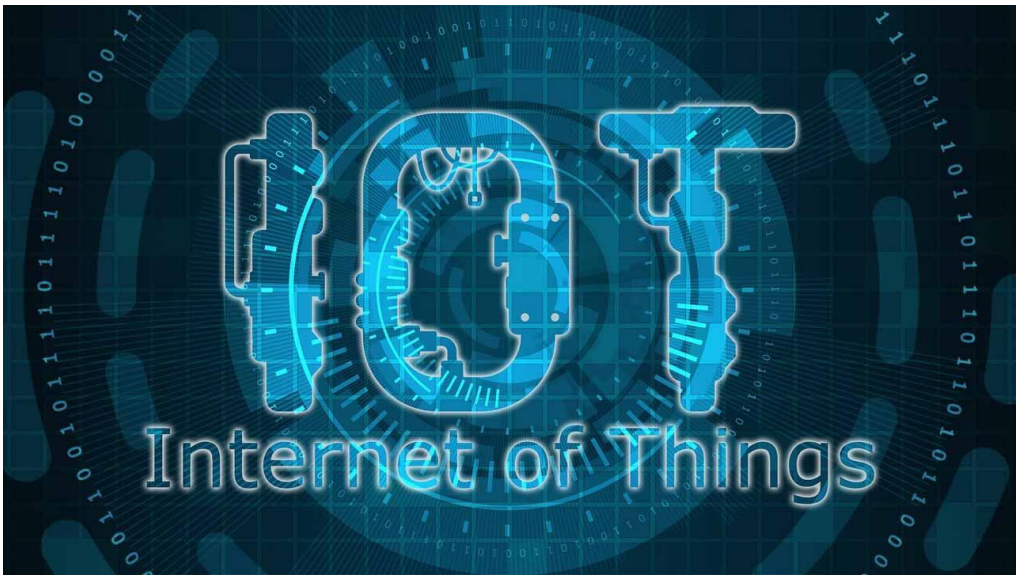
Checklist de Control

Este checklist sirve para realizar una auditoría o revisión de las políticas de seguridad de la información en un entorno de sistemas IoT domésticos. Se aplica durante evaluaciones de seguridad para asegurar que las políticas de seguridad estén bien desarrolladas, comunicadas, implementadas y actualizadas. La auditoría se realiza marcando "SI" o "NO" para cada aspecto, permitiendo identificar áreas que requieren mejoras para asegurar la protección efectiva del sistema.

Tabla G6. Checklist de control de políticas de gestión

Aspecto	Descripción	SI	NO
Desarrollo de Políticas	¿Se ha desarrollado un conjunto completo de políticas de seguridad de la información que abordan los requisitos de cumplimiento y las mejores prácticas?		
Comunicación de Políticas	¿Las políticas de seguridad de la información se han comunicado claramente a todos los usuarios relevantes?		
Capacitación y Concientización	¿Se proporciona capacitación periódica sobre las políticas de seguridad de la información y se lleva a cabo concientización para garantizar la comprensión y el cumplimiento de las políticas?		
Revisión y Actualización	¿Se lleva a cabo una revisión regular de las políticas de seguridad de la información y se actualizan según sea necesario para reflejar los cambios en el entorno de amenazas?		

Plan de Tratamiento de Riesgos



VERSIÓN: 1.0

FECHA EDICIÓN: 25/06/24

HERRAMIENTAS DE EDICIÓN: Microsoft Office Word

ELABORADO POR:

Acosta Proaño Yulisa Francisca
Ing. Andrea Patricia Sánchez Zumba, Mg.

Ambato-2024

1.Introducción:

En un mundo cada vez más interconectado, la seguridad de los datos, la privacidad de las personas y la protección de dispositivos IoT (Internet de las cosas) en entornos domésticos se han convertido en prioridades críticas...

2. Objetivos:

El objetivo primordial de este plan es garantizar la seguridad y privacidad de los datos personales, así como la protección de los dispositivos IoT en entornos domésticos...

3.Alcance del Documento:

Este plan se aplica a todos los dispositivos conectados a Internet y redes domésticas, incluidos pero no limitados a computadoras, teléfonos inteligentes, tabletas, dispositivos de domótica y dispositivos portátiles...

4. Documentos de Soporte:

Para respaldar la implementación de este plan, se recomienda la consulta de recursos adicionales, como guías de seguridad del hogar, tutoriales en línea sobre configuración segura de dispositivos IoT, y políticas de privacidad y seguridad proporcionadas por los fabricantes de dispositivos.

Descripción General

Este plan de tratamiento de riesgos está enfocado en la seguridad de los datos, la privacidad de las personas y los dispositivos IoT en entornos domésticos. El objetivo es mitigar los riesgos identificados mediante la implementación de medidas de seguridad adecuadas.

Proceso de Evaluación de Riesgos de la Información:

El proceso de evaluación de riesgos se centra en identificar las posibles amenazas a la seguridad de los datos y la privacidad en entornos domésticos. Esto incluye evaluar la vulnerabilidad de los dispositivos IoT a intrusiones externas, así como la seguridad de las redes domésticas y las prácticas de gestión de credenciales de los usuarios.

Proyectos del Plan de Tratamiento de Riesgos:

Acceso no autorizado a la red

Riesgo: Acceso no autorizado a la red doméstica.
Amenaza: Actores maliciosos obtienen acceso no autorizado a la red.
Vulnerabilidad: Puertos abiertos, contraseñas débiles y configuraciones de seguridad deficientes.
Consecuencia: Acceso a datos sensibles, instalación de malware, interrupción de servicios.
Tratamiento:

- Configuración segura del enrutador doméstico, incluida la activación de cifrado WPA2/WPA3 y la configuración de contraseñas fuertes para evitar el acceso no autorizado a la red.

- Implementación de segmentación de red para aislar dispositivos IoT de los dispositivos personales y de trabajo, reduciendo así el riesgo de propagación de malware.

Medida: Implementar un firewall robusto y una VPN.
Descripción:

- Firewall: Configurar un firewall de última generación (Next-Generation Firewall, NGFW) que no solo filtre el tráfico basado en reglas predefinidas, sino que también analice el contenido del tráfico en tiempo real, detectando y bloqueando amenazas avanzadas.

Responsable: Propietario del hogar/Administrador de red.
Fecha de Implementación: Inmediato.
Estado: Abierto.

Versiones desactualizadas de software/firmware

Riesgo: Vulnerabilidades en software/firmware debido a versiones desactualizadas.
Amenaza: Explotación de vulnerabilidades conocidas en software/firmware desactualizado.
Vulnerabilidad: Software y firmware obsoletos que no reciben parches de seguridad.
Consecuencia: Compromiso de dispositivos IoT, pérdida de control sobre dispositivos, acceso a datos personales.
Tratamiento:

- Actualización regular de software y firmware en todos los dispositivos IoT y dispositivos personales para eliminar vulnerabilidades conocidas y mejorar la seguridad.

- Utilización de herramientas de escaneo de vulnerabilidades para identificar y remediar rápidamente posibles brechas de seguridad en los dispositivos conectados.

Medida: Implementar un programa de actualización regular de software y firmware.
Descripción:

- Sistema de Actualización Automática: Configurar todos los dispositivos IoT para que realicen actualizaciones automáticas del software y firmware. Asegurarse de que los dispositivos se actualicen automáticamente a las versiones más recientes disponibles tan pronto como se publiquen.

- Gestión Centralizada de Actualizaciones: Utilizar una solución de gestión de dispositivos que permita centralizar y automatizar la distribución de actualizaciones a todos los dispositivos conectados.

Beneficios: Reduce significativamente el riesgo de explotación de vulnerabilidades

conocidas y mejora la resiliencia general de la red doméstica. *Responsable:* Propietario del hogar/Proveedor de servicios. *Fecha de Implementación:* Mensual. *Estado:* Abierto.

Protocolos de comunicación no encriptados

Riesgo: Intercepción de datos transmitidos sin encriptación. *Amenaza:* Eavesdropping, Man-in-the-Middle (MitM) attacks. *Vulnerabilidad:* Uso de protocolos de comunicación no seguros (por ejemplo, HTTP en lugar de HTTPS). *Consecuencia:* Robo de información sensible, como credenciales y datos personales. *Tratamiento:*

- Configuración de protocolos de encriptación fuertes, como SSL/TLS, en dispositivos IoT y comunicaciones domésticas para proteger la confidencialidad de los datos transmitidos.

Medida: Implementar encriptación de extremo a extremo. *Descripción:*

- Wi-Fi Security: Configurar la red Wi-Fi para utilizar el protocolo WPA3, que ofrece mejoras significativas en seguridad con respecto a WPA2, incluyendo una encriptación más fuerte y protección contra ataques de fuerza bruta.

- TLS/SSL: Asegurar que todas las comunicaciones web utilicen HTTPS con TLS 1.2 o superior. Implementar certificados SSL/TLS para todos los dispositivos y servicios web que se utilicen en el entorno doméstico.

Beneficios: Protege la integridad y confidencialidad de los datos en tránsito, asegurando que los datos no puedan ser interceptados ni alterados por actores maliciosos.
Responsable: Propietario del hogar/Administrador de red.
Fecha de Implementación: Inmediato.
Estado: Abierto.

Gestión inadecuada de credenciales

Riesgo: Fuga de información debido a la gestión inadecuada de credenciales. *Amenaza:* Robo de credenciales, ataques de phishing, ataques de fuerza bruta. *Vulnerabilidad:* Uso de contraseñas débiles, reutilización de contraseñas, falta de rotación de contraseñas. *Consecuencia:* Acceso no autorizado a cuentas y dispositivos, pérdida de datos sensibles, compromisos de privacidad. *Tratamiento:*

- Implementación de autenticación multifactorial en dispositivos y aplicaciones sensibles para proteger las cuentas contra el acceso no autorizado.
- Educar a los usuarios sobre la importancia de usar contraseñas únicas y complejas para cada cuenta y proporcionar herramientas para gestionar de manera segura sus credenciales.

Medida: Implementar una gestión segura de credenciales. *Descripción:*

- Gestor de Contraseñas: Usar un gestor de contraseñas que genere y almacene contraseñas fuertes y únicas para cada cuenta y dispositivo.
- Autenticación Multifactor (MFA): Implementar MFA en todas las cuentas críticas y dispositivos. MFA añade una capa adicional de seguridad al requerir múltiples formas de verificación (algo que sabes, algo que tienes, y algo que eres).
- Políticas de Contraseñas: Establecer políticas de contraseñas estrictas que incluyan requisitos de longitud mínima, complejidad, y periodicidad de cambios.

Beneficios: Reduce significativamente el riesgo de acceso no autorizado debido a credenciales comprometidas, asegurando que incluso si una contraseña se ve comprometida, los atacantes no puedan acceder fácilmente a las cuentas o dispositivos.

Responsable: Propietario del hogar/Proveedor de servicios.
Fecha de Implementación: Inmediato.
Estado: Abierto.

Resumen del Plan de Tratamiento de Riesgos

Tabla H1. Plan de tratamiento de riesgos resumido.

Riesgo	Medida	Descripción	Responsable	Fecha de Implementación	Estado
Acceso no autorizado a la red	Implementar firewall y VPN	Configurar firewall y usar VPN	Propietario del hogar/Administrador de red	Inmediato	Abierto
Versiones desactualizadas de software/firmware	Actualización regular	Implementar actualizaciones automáticas	Propietario del hogar/Proveedor de servicios	Mensual	Abierto
Protocolos de comunicación no encriptados	Implementar encriptación de extremo a extremo	Usar WPA3 y TLS	Propietario del hogar/Administrador de red	Inmediato	Abierto
Gestión inadecuada de credenciales	Gestión segura de credenciales	Usar gestor de contraseñas y MFA	Propietario del hogar/Proveedor de servicios	Inmediato	Abierto

Validez y Gestión de Documentos:

Este plan será revisado y actualizado periódicamente para reflejar los cambios en el panorama de amenazas y las mejores prácticas de seguridad. Se recomienda a los usuarios mantener registros de auditoría y documentación de seguridad para garantizar la validez y la efectividad continua de las medidas implementadas.

Firmas de Documentos:

Este plan ha sido revisado y aprobado por el equipo de seguridad de la información, y cualquier revisión posterior requerirá la aprobación de las partes interesadas relevantes.

Tabla I1. Recopilación de marcos de referencia: IoT SF, IIC, CIS para modelo de línea base

IoT Security Foundation			IIC (Industry IoT Consortium)				CIS (Center for Internet Security)		
Dominio	Descripción	ID	Categoría	Dominio	Descripción	ID	Categoría	Dominio	ID
Seguridad empresarial Procesos, Políticas y Responsabilidades	Gestión responsable de la gobernanza de una empresa que desarrolla e implementa dispositivos IoT	2.4.3	Gobernancia	Estrategia y gobernanza	Gestión del programa de seguridad, Gestión de cumplimiento	1	Aplicable salvaguardias al más del 60%	Inventario y Control de Activos Er	1
Hardware del dispositivo y Seguridad física	Personal de Diseño y Producción responsable de la calidad del hardware y mecánica.	2.4.4		Modelados de amenazas y evaluacion de riesgos	Modelado de amenazas, Actitud de riesgo	2		Protección de Datos	2
Software del dispositivo	Gestión de la calidad de las aplicaciones de dispositivos por parte de arquitectos de software, propietarios de productos y administradores de versiones.	2.4.5		Gestión de la cadena de suministro y dependencias	Gestion de riesgos de la cadena de suministro de productos, Gestión de dependencia de terceros	3		Administración de cuentas	3
Sistema operativo del dispositivo	Personal de gestión y diseño responsable de la selección de un sistema operativo de terceros o de evaluar la calidad del software desarrollado "interno".	2.4.6	Habilitacion	Gestion de identidad y acceso	Establecer y mantener identidades, Control de acceso	4		Gestión continua de vulnerabilidad	4
Dispositivo cableado y Interfaces inalámbricas	Personal de Diseño y Producción responsable de la seguridad de las comunicaciones de los dispositivos.	2.4.7		Proteccion de activos	Gestión de activos, cambios y configuración - Protección física	5		Gestión de registros de auditoria	5
Autenticación y Autorización	El requisito es directamente aplicable al software del dispositivo o servicio	2.4.8		Proteccion de datos	Política de protección de datos, Implementación de controles de protección de datos	6		Defensas contra malware	6
Cifrado y clave Gestión para Hardware	Personal de diseño y producción responsable de la seguridad de las interfaces de los sistemas IoT y los fundamentos de la autenticación.	2.4.9	Endurecimiento	Gestion de vulnerabilidades y parches	Evaluación de Vulnerabilidades, Gestión de parches	7		Recuperación de datos	7
Interfaz de usuario web	Personal de diseño y producción responsable de la seguridad de la gestión de claves de hardware y cifrado de los sistemas IoT	2.4.10		Conciencia de la situación	Practicas de seguimiento, conciencia de la situación e intercambio de información	8		Gestión de infraestructura de red	8
Aplicación movil	Personal de Diseño y Producción responsable de la seguridad de los Sistemas Web de los Productos o Servicios IoT.	2.4.11		Respuestas a eventos e incidentes	Plan de detección y respuesta a eventos - Remediación, Recuperación y continuidad de operaciones	9		Monitoreo y Defensa de Redes	9
Privacidad	Personal de Diseño y Producción responsable de la seguridad de la Aplicación Móvil del Producto o Servicios IoT.	2.4.12						Concientización sobre seguridad y	10
Nube y red Elementos	Dirección y personal responsable del cumplimiento normativo de Protección de Datos y Privacidad.	2.4.13						Gestión de proveedores de servicio	11
Cadena de suministro y producción seguras	Personal de diseño y producción responsable de la seguridad de los sistemas de red o nube del producto o servicio IoT	2.4.14						Seguridad del software de aplicaci	12
Configuración	Personal de diseño y producción responsable de la seguridad del dispositivo y las configuraciones de los servicios IoT.	2.4.15						Gestión de respuesta a incidentes	13
Propiedad del dispositivo Transferir	Personal de Gestión, Diseño y Producción responsable de la Cadena de Suministro de productos y servicios.	2.4.16						Pruebas de penetración	14
							Aplicable salvaguardias entre el 1% y 60%	Inventario y Control de Activos de	15
								Configuración segura de activos y	16
								Gestión de control de acceso	17
								Protecciones de correo electrónico	18

Tabla I2. Recopilación de marcos de referencia: NIST, CSA, SCF para modelo de línea base, PARTE 1

NIST				Cloud Security Alliance			SECURE CONTROLS FRAMEWORK		
Gobernanza	Contexto organizacional	Se comprenden las decisiones de gestión de riesgos de ciberseguridad de la organización.	1	Gestión de activos	Convención de nomenclatura, inventario de activos, supervisión de activos	1	Gobernanza de la ciberseguridad y la privacidad de los datos	Ejecutar un programa documentado y basado en riesgos que respalde los objetivos comerciales y al mismo tiempo abarque los principios de ciberseguridad y privacidad de datos	1
	Estrategia de gestión de riesgos	Se utiliza para respaldar las decisiones de riesgo operativo.	2	Gestión de configuración	Archivos de configuración, actualizaciones de firmware, control de configuración, planificación de fin de vida útil	2	Tecnología artificial y autónoma	Garantizar una Inteligencia Artificial (IA) y tecnologías autónomas confiables y resilientes para lograr un impacto beneficioso informando, asesorando o simplificando las tareas, minimizando al mismo tiempo las propiedades emergentes o las consecuencias no deseadas	2
	Funciones, responsabilidades y autoridades	fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua	3	Comunicaciones Seguras	Comunicaciones confiables, seguridad del transporte de telemetría de colas de mensajes (MQTT), comunicaciones cifradas	3	Gestión de activos	Administre todos los activos tecnológicos desde la compra hasta la disposición, tanto físicos como virtuales, para garantizar un uso seguro, independientemente de la ubicación del activo.	3
	Política	Se establece, comunica y aplica la política de ciberseguridad organizacional.	4	Datos seguros	Clasificación y taxonomía de datos, limpieza de datos cifrados en reposo	4	Continuidad del negocio y recuperación ante desastres	Las organizaciones establecen procesos que ayudarán a la organización a recuperarse de situaciones adversas con un impacto mínimo	4
	Vigilancia	Se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos.	5	Gobernancia	Marco de gobernanza, requisitos regulatorios y legales, gestión de cumplimiento, privacidad, seguridad	5	Planificación de capacidad y rendimiento	Las organizaciones evitan interrupciones comerciales evitables causadas por limitaciones de capacidad y desempeño planificando proactivamente el crecimiento y pronosticando, además de requerir que tanto la tecnología como el liderazgo empresarial	5
	Gestión de riesgos de la cadena de suministro de ciberseguridad	Los procesos de gestión de riesgos de la cadena de suministro cibernético son identificados, establecidos, gestionados, monitoreados y mejorados por las partes interesadas de la organización.	6	Gestión de identidad y acceso	Gestión de contraseñas, autenticación, autorización, control de acceso, gestión de claves, gestión de anclaje desconfianza, bootstrap, auditoría de cuentas	6	Gestión del cambio	Las organizaciones garantizan que tanto la tecnología como el liderazgo empresarial gestionen proactivamente los cambios, incluida la evaluación, autorización y seguimiento de los cambios técnicos en toda la empresa para no afectar el tiempo de actividad de los sistemas de producción	6
	Gestión de activos	Se comprenden los riesgos actuales de ciberseguridad de la organización.	7	Administración de incidentes	Respuesta al incidente	7	Seguridad en la nube	Las organizaciones rigen el uso de entornos de nube pública y privada (por ejemplo, IaaS, PaaS y SaaS) para gestionar de manera integral los riesgos asociados con la participación de terceros	7
Identificar (ID)	Evaluación de riesgos	La organización comprende el riesgo de ciberseguridad para la organización, los activos y las personas.	8	Seguridad de dispositivos IoT	Dispositivos certificados, plataforma segura, configuración segura	8	Cumplimiento	Las organizaciones garantizan que existan controles para garantizar el cumplimiento de las obligaciones de cumplimiento legales, reglamentarias y contractuales aplicables	8
	Mejora	Se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos de ciberseguridad organizacional	9	Legal	Evaluación Legal, Plan de Implementación Legal, Medidas Documentales para Fines Legales, Términos y Condiciones y Politica de Privacidad, Contratos, Descargos de Responsabilidad, Divulgaciones, Notificaciones Renuncias, Responsabilidad, Transferencia de Datos	9	Gestión de configuración	Las organizaciones establecen y mantienen la integridad de los sistemas	9
	Gestión de identidad, autenticación y control de acceso	El personal de la organización recibe sensibilización y formación en ciberseguridad	10	Monitoreo y registro	Inteligencia de amenazas, búsqueda de amenazas, gestión automatizada de registros de malware, análisis, definición de eventos, monitoreo de radiofrecuencia (RF)	10	Monitoreo continuo	Las organizaciones establecen y mantienen un conocimiento situacional continuo en toda la empresa a través de la recopilación y revisión centralizada de registros de eventos relacionados con la seguridad.	10

Tabla I3. Recopilación de marcos de referencia: NIST, CSA, SCF para modelo de línea base, PARTE 2

NIST				Cloud Security Alliance			SECURE CONTROLS FRAMEWORK		
Categoría	Dominio	Descripción	ID	Dominio	Descripción	ID	Dominio	Descripción	ID
Proteger (PR)	Gestión de identidad, autenticación y control de acceso	El personal de la organización recibe sensibilización y formación en ciberseguridad	10	Monitoreo y registro	Inteligencia de amenazas, búsqueda de amenazas, gestión automatizada de registros de malware, análisis, definición de eventos, monitoreo de radiofrecuencia (RF)	10	Monitoreo continuo	Las organizaciones establecen y mantienen un conocimiento situacional continuo en toda la empresa a través de la recopilación y revisión centralizada de registros de eventos relacionados con la seguridad.	10
	Concientización y Capacitación	El hardware, software y los servicios de plataformas físicas y virtuales se gestionan de manera consistente con la estrategia de riesgo de la organización para proteger su confidencialidad, integridad y disponibilidad	11	Disponibilidad operativa	Mantenimiento, conmutación por error, protección de denegación de servicio distribuido (DDoS), acuerdos de nivel de servicio	11	Protecciones criptográficas	Utilice soluciones criptográficas adecuadas y prácticas de gestión de claves reconocidas en la industria para proteger la confidencialidad.	11
	Seguridad de datos	Los datos se gestionan de manera consistente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información	12	Seguridad física	Controles de acceso físico	12	Clasificación y manejo de datos	Las organizaciones se aseguran de que los activos tecnológicos, tanto electrónicos como físicos, estén clasificados adecuadamente y se implementen medidas para proteger los datos de la organización contra la divulgación o modificación no autorizada	12
	Seguridad de la plataforma	El hardware, software y los servicios de plataformas físicas y virtuales se gestionan de manera consistente con la estrategia de riesgo de la organización para proteger su confidencialidad, integridad y disponibilidad	13	Política	Definición de Política, Política de Seguridad de Adquisición, disposición Segura	13	Tecnología integrada	Las organizaciones especifican el desarrollo, la gestión proactiva y la revisión continua de las tecnologías integradas de seguridad, incluido el refuerzo de la "pila" desde el hardware, el firmware y el software hasta los protocolos de transmisión y servicio utilizados para los dispositivos de Internet de las cosas (IoT) y tecnología operativa (OT).	13
	Resiliencia de la infraestructura tecnológica	Las arquitecturas de seguridad se gestionan con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de los activos, y resiliencia organizacional	14	Gestión de riesgos	Estrategia de gestión de riesgos, ejecución de la gestión de riesgos, limitación de responsabilidad	14	Punto final de Seguridad	Las organizaciones se aseguran de que los dispositivos terminales estén adecuadamente protegidos contra amenazas de seguridad al dispositivo y sus datos.	14
Detectar (DE)	Monitoreo continuo	Los activos son monitoreados para encontrar anomalías, indicadores de compromiso y otros eventos potencialmente adversos	15	Aplicaciones seguras	Aplicaciones Móviles, Servicios en la Nube, Sistemas autónomos	15	Seguridad de Recursos Humanos	Las organizaciones crean una fuerza laboral preocupada por la ciberseguridad y la privacidad de los datos y una entorno propicio para la innovación	15
	Análisis de eventos adversos	Se analizan anomalías, indicadores de compromiso y otros eventos potencialmente adversos para caracterizar los eventos y detectar incidentes de ciberseguridad.	16	Ciclo de vida de desarrollo de sistemas seguros	Seguridad de procesos, cadena de suministro/adquisición, prácticas de desarrollo seguro, pruebas de seguridad	16	Identificación y autenticación	Las organizaciones implementan el concepto de "privilegio mínimo" limitando el acceso a los sistemas y datos de la organización únicamente a usuarios autorizados.	16
Responder (RS)	Administracion de incidentes	Se gestionan las respuestas a los incidentes de ciberseguridad detectados	17	Redes seguras	Descubrimiento seguro, refuerzo de red, confianza cero, visualización de red	17	Respuesta al incidente	Las organizaciones establecen y mantienen una capacidad viable y probada para responder a incidentes relacionados con la ciberseguridad o la privacidad de datos de manera oportuna	17
	Análisis de incidentes	Se llevan a cabo investigaciones para garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación.	18	Conexión inalámbrica segura	Arquitectura RF, Seguridad Bluetooth, Seguridad de comunicación de campo cercano (NFC), Seguridad Zigbee	18	Aseguramiento de información	Las organizaciones garantizan los controles adecuados de ciberseguridad y privacidad de datos en entornos de desarrollo, pruebas y producción.	18
	Informes y comunicación de respuesta a incidentes	Las actividades de respuesta se coordinan con las partes interesadas internas y externas según lo exigen las leyes, regulaciones o políticas.	19	Capacitación	Formación de administradores, formación de usuarios	19	Mantenimiento	Las organizaciones se aseguran de que los activos tecnológicos se mantengan adecuadamente para garantizar el rendimiento y la eficacia continuos.	19
	Mitigación de incidentes	Se realizan actividades para prevenir la expansión de un evento y mitigar sus efectos.	20	Gestión de vulnerabilidades	Programa de divulgación responsable, escaneo de vulnerabilidades, actualizaciones y parches	20	Gestión de dispositivos móviles	Las organizaciones controlan los riesgos asociados con los dispositivos móviles, independientemente de su propiedad (propiedad de la organización, de los empleados o de terceros)	20
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	Se realizan actividades de restauración para garantizar la disponibilidad operativa de los sistemas y servicios afectados por incidentes de ciberseguridad.	21	Pruebas de seguridad	Alcance y planificación de evaluaciones, pruebas de penetración, Red Teaming, evaluaciones de terceros, recompensas por errores, aplicaciones y servicios de IoT (desarrollados internamente)	21	Seguridad de la red	Las organizaciones garantizan que se diseñen suficientes controles de ciberseguridad y privacidad de datos para proteger la confidencialidad, integridad, disponibilidad y seguridad de la [illegible] de la red	21
	Comunicación de recuperación de incidentes	Las actividades de restauración se coordinan con partes internas y externas	22				Seguridad física y ambiental	Las organizaciones limitan el acceso físico a los sistemas y datos de la organización abordando los controles de seguridad física aplicables y garantizando que existan controles ambientales apropiados y monitoreados	22
	Concientización y capacitación sobre seguridad	Las organizaciones desarrollan una fuerza laboral preocupada por la ciberseguridad y la privacidad de los datos a través de actividades de educación continua y ejercicios prácticos.	28				Privacidad de datos	Las organizaciones alinean las decisiones de ingeniería de privacidad de datos con la estrategia general de privacidad de datos de la organización y las prácticas líderes reconocidas en la industria	23
	Desarrollo y adquisición de tecnología	Las organizaciones se aseguran de que los principios de ciberseguridad y privacidad de datos se implementen en cualquier producto/solución, ya sea desarrollado internamente o adquirido, para garantizar que se incorporen los [illegible]	29				Gestión de proyectos y recursos	Las organizaciones garantizan que los proyectos relacionados con la seguridad tengan recursos y apoyo a la gestión de proyectos/programas para garantizar la [illegible]	24
	Gestión de terceros	Las organizaciones garantizan que los riesgos de ciberseguridad y privacidad de datos asociados con terceros se minimicen y permiten medidas para sostener las [illegible] en caso de	30				Gestión de riesgos	Las organizaciones se aseguran de que las unidades de negocio propietarias de los activos y/o procesos involucrados conozcan y comprendan todos los riesgos aplicables relacionados con la ciberseguridad y la privacidad de los datos	25
	Gestión de amenazas	Las organizaciones establecen una capacidad para identificar y gestionar proactivamente las amenazas relacionadas con la tecnología a la ciberseguridad y la privacidad de los datos de los sistemas, datos y procesos	31				Ingeniería y arquitectura segura	Las organizaciones alinean las decisiones de arquitectura e ingeniería de ciberseguridad con la estrategia de arquitectura tecnológica general de la organización [illegible]	26
	Gestión de vulnerabilidades y parches	Las organizaciones gestionan de forma proactiva los riesgos asociados con la gestión de vulnerabilidades técnicas, lo que incluye garantizar que se utilicen [illegible]	32				Operaciones de seguridad	Las organizaciones garantizan que existan recursos adecuados y una estructura de gestión para permitir la prestación de servicios de ciberseguridad, seguridad física y privacidad de datos	27
	Seguridad Web	Las organizaciones abordan los riesgos asociados con las tecnologías accesibles a Internet fortaleciendo los dispositivos, monitoreando la integridad de los archivos del sistema, permitiendo la auditoría y [illegible]	33						

Tabla I4. Análisis GAP inicial

MODELO DE LINEA BASE PARA SEGURIDAD DE LOS DATOS, PRIVACIADAD DE LAS PERSONAS Y DISPOSITIVOS IoT PARA ENTORNOS HOME			CONTROL				REFERENCIAS
DOMINIO	DETALLE	REQUERIMIENTO	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	
GESTION - GOBERNANZA - DIRECCION	La gestión de ciberseguridad y privacidad de datos implica procesos, políticas y responsabilidades que contribuyen a la seguridad de la informacion y los dispositivos. La gobernanza organiza las decisiones de gestión de riesgos cibernéticos y establece estrategias, políticas y vigilancia.	Estable objetivos para proteger la seguridad de los datos, de la privacidad de las personas y los dispositivos IoT					IoTSF Security Assurance Framework - 2.4.3 ;2.4.4 The NIST Cybersecurity Framework (CSF) 2.0- 1 a 6 CSA Guide to the IoT Security Controls Framework-5,9,13,14 Industry Internet of Things Security Framework 1-3 Center for Internet Security -11 Secure Controls Framework-1,2,8,19,24,25,30
		Establece un modelo o estrategia para la gestion de riesgos					
		Establece politicas y procesos alineados a los objetivos de seguridad y de gestion de riesgos					
		Estable responsabilidades y roles					
HABILITACION E IDENTIFICACION	El conjunto de directrices aborda los aspectos físicos, de hardware y software de los dispositivos, asegurando la gestión efectiva de activos, configuraciones seguras y control de acceso. Se enfoca en la protección de activos, la identificación y autenticación de usuarios, así como en la gestión de dispositivos móviles y el desarrollo de tecnología, todo con el objetivo de garantizar un entorno seguro y minimizar los riesgos asociados con los activos tecnológicos	Software, Hardware y Objeto físico, se encuentran inventariados o identificados de manera clara					IoTSF Security Assurance Framework - 2.4.5-2.4.9;2.4.14-2.4.16 The NIST Cybersecurity Framework (CSF) 2.0- 7,10 CSA Guide to the IoT Security Controls Framework-1,2,6 Industry Internet of Things Security Framework 4,5 Center for Internet Security -1,3,8,15,16,17 Secure Controls Framework-3,6,9,16,20,29
		Se lleva un registro sobre la configuracion, la actualizacion, mantenimientos y cambios realizados en software, hardware y objeto físico					
		Se gestione de manera segura las contrasneas, autenticacion, autorizacion, control de acceso, gesntion de claves, implementan el concepto de "privilegio mínimo" limitando el acceso únicamente a usuarios autorizados.					
FORTALEZA CIBERNÉTICA (HARDENING - PROTECCION)	Garantiza la seguridad y proteccion de los dispositivos por medio de implementación de medidas de seguridad adicionales. Estas prácticas son esenciales para proteger la integridad, confidencialidad y disponibilidad de los dispositivos IoT y los datos que manejan	Gestión de datos de manera consistente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información. Clasificacion de datos					IoTSF Security Assurance Framework - 2.4.10-2.4.13 The NIST Cybersecurity Framework (CSF) 2.0- 12,13,14 CSA Guide to the IoT Security Controls Framework-3,4,8,12,15,17,18 Industry Internet of Things Security Framework 6,7 Center for Internet Security -2,12,18 Secure Controls Framework-7,11,12,14,15,21,22,23,26,27,32,33
		Comunicaciones seguras y confiables, comunicaciones cifradas, aplicaciones seguras, redes seguras, conexión inalámbrica segura, protecciones criptográficas					
		Gestion de estrategias de riesgo, evaluacion de vulnerabilidades y parches para proteccion de la confidencialidad, integridad y disponibilidad de activos y resilencia organizacional					
		Dispositivos IoT con configuración segura, plataforma segura, controles de acceso físico, Gestion de vulnerabilidades y parches					
		proteger la confidencialidad, integridad y disponibilidad por medio de el hardware, software y servicios de plataformas físicas y virtuales					
SEGUIMIENTO - MONITOREO	Los activos son monitoreados para encontrar anomalías, indicadores de compromiso para caracterizar los eventos y detectar incidentes de ciberseguridad.	Monitoreo continuo y analisis de eventos adversos					The NIST Cybersecurity Framework (CSF) 2.0- 15,16 CSA Guide to the IoT Security Controls Framework-10 Center for Internet Security -5,9 Secure Controls Framework-10,13
		Gestión de registros y Defensa de redes					
EDUCACIÓN DIGITAL AVANZADA (CAPACITACION - EDUCACION)	gestión de hardware, software y servicios de plataformas virtuales y físicas de manera consistente con la estrategia de riesgo de la organización para proteger su confidencialidad, integridad y disponibilidad	Concientizacion de la situación e intercambio de información, a travez de actividades de educación continua y ejercicios prácticos.					The NIST Cybersecurity Framework (CSF) 2.0- 11 CSA Guide to the IoT Security Controls Framework-19 Industry Internet of Things Security Framework 8 Center for Internet Security -10 Secure Controls Framework-28
		Capacitacion y concientizacion para administradores y usuarios					
CONTINUIDAD Y ANTIDESASTRE	Se gestionan las vulnerabilidades, se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos. Se lleva a cabo respuestas a los incidentes de ciberseguridad detectados. Se realizan pruebas de seguridad y respuestas a eventos e incidentes	Evaluacion de riesgos y mejoras en los procesos, procedimientos y actividades de gestion de riesgos					The NIST Cybersecurity Framework (CSF) 2.0- 8,9,17-22 CSA Guide to the IoT Security Controls Framework-7,11,16,20,21 Industry Internet of Things Security Framework 9 Center for Internet Security -4,6,7,13,14 Secure Controls Framework-4,5,13,17,18,31
		Análisis, administracion y mitigación de incidentes					
		Ejecucion y comunicación de plan de recuperación de incidentes					
		Gestión de vulnerabilidades, amenazas, pruebas de seguridad y penetración					

Tabla I5. Análisis GAP esperado

MODELO DE LINEA BASE PARA SEGURIDAD DE LOS DATOS, PRIVACIADAD DE LAS PERSONAS Y DISPOSITIVOS IoT PARA ENTORNOS HOME				CONTROL	REFERENCIAS
DOMINIO	DETALLE	CATEGORIA	REQUERIMIENTO	MADUREZ	
GESTION - GOBERNANZA - DIRECCION	La gestión de ciberseguridad y privacidad de datos implica procesos, políticas y responsabilidades que contribuyen a la seguridad de la información y los dispositivos. La gobernanza organiza las decisiones de gestión de riesgos cibernéticos y establece estrategias, políticas y vigilancia.	CAT1	Estable objetivos para proteger la seguridad de los datos, de la privacidad de las personas y los dispositivos IoT	1	IoTSF Security Assurance Framework - 2.4.3 ;2.4.4 The NIST Cybersecurity Framework (CSF) 2.0- 1 a 6 CSA Guide to the IoT Security Controls Framework-5,9,13,14 Industry Internet of Things Security Framework 1-3 Center for Internet Security -11 Secure Controls Framework-1,2,8,19,24,25,30
		CAT2	Establece un modelo o estrategia para la gestion de riesgos	1	
		CAT3	Establece políticas y procesos alineados a los objetivos de seguridad y de gestion de riesgos	1	
		CAT4	Estable responsabilidades y roles	1	
HABILITACION E IDENTIFICACION	El conjunto de directrices aborda los aspectos físicos, de hardware y software de los dispositivos, asegurando la gestión efectiva de activos, configuraciones seguras y control de acceso. Se enfoca en la protección de activos, la identificación y autenticación de usuarios, así como en la gestión de dispositivos móviles y el desarrollo de tecnología, todo con el objetivo de garantizar un entorno seguro y minimizar los riesgos asociados con los activos tecnológicos	CAT5	Software, Hardware y Objeto físico, se encuentran inventariados o identificados de manera clara	1	IoTSF Security Assurance Framework - 2.4.5-2.4.9;2.4.14-2.4.16 The NIST Cybersecurity Framework (CSF) 2.0- 7,10 CSA Guide to the IoT Security Controls Framework-1,2,6 Industry Internet of Things Security Framework 4,5 Center for Internet Security -1,3,8,15,16,17 Secure Controls Framework-3,6,9,16,20,29
		CAT6	Se lleva un registro sobre la configuracion, la actualizacion, mantenimientos y cambios realizados en software, hardware y objeto físico	1	
		CAT7	Se gestione de manera segura las contrasenas, autenticacion, autorizacion, control de acceso, gestion de claves, implementan el concepto de "privilegio mínimo" limitando el acceso únicamente a usuarios autorizados.	1	
FORTALEZA CIBERNÉTICA (HARDENING - PROTECCION)	Garantiza la seguridad y proteccion de los dispositivos por medio de implementación de medidas de seguridad adicionales. Estas prácticas son esenciales para proteger la integridad, confidencialidad y disponibilidad de los dispositivos IoT y los datos que manejan	CAT8	Gestión de datos de manera consistente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información. Clasificacion de datos	1	IoTSF Security Assurance Framework - 2.4.10-2.4.13 The NIST Cybersecurity Framework (CSF) 2.0- 12,13,14 CSA Guide to the IoT Security Controls Framework-3,4,8,12,15,17,18 Industry Internet of Things Security Framework 6,7 Center for Internet Security -2,12,18 Secure Controls Framework-7,11,12,14,15,21,22,23,26,27,32,33
		CAT9	Comunicaciones seguras y confiables, comunicaciones cifradas, aplicaciones seguras, redes seguras, conexión inalámbrica segura, protecciones criptográficas	1	
		CAT10	Gestion de estrategias de riesgo, evaluacion de vulnerabilidades y parches para proteccion de la confidencialidad, integridad y disponibilidad de activos y resilencia organizacional	1	
		CAT11	Dispositivos IoT con configuración segura, plataforma segura, controles de acceso físico, Gestion de vulnerabilidades y parches	1	
		CAT12	proteger la confidencialidad, integridad y disponibilidad por medio de la gestion de el hardware, software y servicios de plataformas físicas y virtuales	1	
SEGUIMIENTO - MONITOREO	Los activos son monitoreados para encontrar anomalías, indicadores de compromiso para caracterizar los eventos y detectar incidentes de ciberseguridad.	CAT13	Monitoreo continuo y analisis de eventos adversos	1	CSA Guide to the IoT Security Controls Framework-10 Center for Internet Security -5,9
		CAT14	Gestión de registros y Defensa de redes	1	
EDUCACIÓN DIGITAL AVANZADA (CAPACITACION - EDUCACION)	gestión de hardware, software y servicios de plataformas virtuales y físicas de manera consistente con la estrategia de riesgo de la organización para proteger su confidencialidad, integridad y disponibilidad	CAT15	Concientizacion de la situación e intercambio de información, a travez de actividades de educación continua y ejercicios prácticos.	1	The NIST Cybersecurity Framework (CSF) 2.0- 11 CSA Guide to the IoT Security Controls Framework-19 Industry Internet of Things Security Framework 8 Center for Internet Security -10 Secure Controls Framework-28
		CAT16	Capacitacion y concientizacion para administradores y usuarios	1	
CONTINUIDAD Y ANTIDESASTRE	Se gestionan las vulnerabilidades, se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos. Se lleva a cabo respuestas a los incidentes de ciberseguridad detectados. Se realizan pruebas de seguridad y respuestas a eventos e incidentes	CAT17	Evaluacion de riesgos y mejoras en los procesos, procedimientos y actividades de gestion de riesgos	1	The NIST Cybersecurity Framework (CSF) 2.0- 8,9,17-22 CSA Guide to the IoT Security Controls Framework-7,11,16,20,21 Industry Internet of Things Security Framework 9 Center for Internet Security -4,6,7,13,14 Secure Controls Framework-4,5,13,17,18,31
		CAT18	Análisis, administracion y mitigación de incidentes	1	
		CAT19	Ejecucion y comunicación de plan de recuperación de incidentes	1	
		CAT20	Gestion de vulnerabilidades, amenazas, pruebas de seguridad y penetración	1	
		REF		6	

Tabla I6. Análisis por capas de los dispositivos IoT

MODELO	INTERRUPTOR DE LUZ INTELIGENTE	bombilla inteligente2-nexxt	ENCHUFE INTELIGENTE - nexxt	ENCHUFE INTELIGENTE - smart life	CAMARA INTELIGENTE PARA INTERIORES	echo dot	Bombilla Inteligente1-nexxt	SENSOR DE CONTACTO PARA PUERTA	SENSOR DE CONTACTO PARA PUERTA
S.O	Sistema operativo remoto: EthernetBoard OkiLAN 8100e	Sistema operativo remoto: EthernetBoard OkiLAN 8100e	Sistema operativo remoto: Emerson Liebert IntelliSlot Web Card	Sistema operativo remoto: EthernetBoard OkiLAN 8100e	Sistema operativo remoto: Linux Kernel 2.6	Sistema operativo remoto: Linux Kernel 2.6	Sistema operativo remoto: EthernetBoard OkiLAN 8100e	Sistema operativo remoto: EthernetBoard OkiLAN 8100e	Sistema operativo remoto: EthernetBoard OkiLAN 8100e
	Confianza: 65%	Confianza: 65%	Confianza: 70%	Confianza: 65%	Confianza: 65%		Confianza: 65%	Confianza: 65%	Confianza: 65%
Capa 7	Servicio asociado: IRC (Internet Relay Chat)	Servicio asociado: IRC (Internet Relay Chat)	Servicio asociado: IRC (Internet Relay Chat)	Servicio asociado: IRC (Internet Relay Chat)	Servicio asociado: IRC (Internet Relay Chat)	Web Server (HTTPS)	Servicio asociado: IRC (Internet Relay Chat)	Servicio asociado: IRC (Internet Relay Chat)	Servicio asociado: IRC (Internet Relay Chat)
Capa 6						TLSv1.2			
Capa 5	SESION								
Capa 4	TCP Puerto abierto detectado: 6668/tcp	Puerto abierto detectado: 6668/tcp	Puerto abierto detectado: 6668/tcp	Puerto abierto detectado: 6668/tcp	Puerto abierto detectado: 6668/tcp	Puerto abierto detectado: 1080/tcp , 4070/tcp, 6543/tcp , 8888/tcp, 10001/tcp, 55442/tcp, 55443/tcp	Puerto abierto detectado: 6668/tcp	Puerto abierto detectado: 6668/tcp	Puerto abierto detectado: 6668/tcp
Capa 3	IP v4 **Dirección IP del dispositivo: 192.168.100.40**	**Dirección IP del dispositivo: 192.168.100.30**	**Dirección IP del dispositivo: 192.168.100.24**	**Dirección IP del dispositivo: 192.168.100.28**	**Dirección IP del dispositivo: 192.168.100.27**	**Dirección IP del dispositivo: 192.168.100.22**	**Dirección IP del dispositivo: 192.168.100.29**	**Dirección IP del dispositivo: 192.168.100.23**	**Dirección IP del dispositivo: 192.168.100.41**
Capa 2	**Dirección MAC del dispositivo: A8:80:55:D5:B5:EE** Fabricante de tarjetas identificado: Tuya Smart Inc.	**Dirección MAC del dispositivo: 1C:90:FF:75:1D:6D** Fabricante de tarjetas identificado: Tuya Smart Inc.	**Dirección MAC del dispositivo: FC:67:1F:F9:C2:D1** Fabricante de tarjetas identificado: Tuya Smart Inc.	**Dirección MAC del dispositivo: 50:88:B9:02:F8:B7** Fabricante de tarjetas identificado: Tuya Smart Inc.	**Dirección MAC del dispositivo: A0:92:08:99:CE:7D** Fabricante de tarjetas identificado: Tuya Smart Inc.	**Dirección MAC del dispositivo: 50:07:C3:64:EE:78** Fabricante de tarjetas identificado: Amazon Technologies Inc.	**Dirección MAC del dispositivo: 1C:90:FF:EC:61:84** Fabricante de tarjetas identificado: Tuya Smart Inc.	**Dirección MAC del dispositivo: FC:67:1F:7B:5C:A3** Fabricante de tarjetas identificado: Tuya Smart Inc.	**Dirección MAC del dispositivo: FC:67:1F:78:64:92** Fabricante de tarjetas identificado: Tuya Smart Inc.
Capa 1	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**	**Estandar 802.11 b/g/n**

Tabla I7. Análisis generado por Nessus de los dispositivos IoT

Plugin ID	CVE	CVSS v2.0 Base Score	Risk	Host	Protocol	Port	Name	Description	Solution	CVSS v3.0 Base Score
51192			64 Medium	10.10.10.220	tcp	10001	**SSL Certificate Cannot Be Trusted**	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.	Purchase or generate a proper SSL certificate for this service.	6.5
51192			64 Medium	10.10.10.220	tcp	55443	**SSL Certificate Cannot Be Trusted**	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.	Purchase or generate a proper SSL certificate for this service.	6.5
57582			64 Medium	10.10.10.220	tcp	10001	**SSL Self-Signed Certificate**	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.	Purchase or generate a proper SSL certificate for this service.	6.5
57582			64 Medium	10.10.10.220	tcp	55443	**SSL Self-Signed Certificate**	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.	Purchase or generate a proper SSL certificate for this service.	6.5
65821	CVE-2013-2566		43 Medium	10.10.10.220	tcp	10001	**SSL RC4 Cipher Suites Supported (Bar Mitzvah)**	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	5.9
65821	CVE-2015-2808		43 Medium	10.10.10.220	tcp	10001	**SSL RC4 Cipher Suites Supported (Bar Mitzvah)**	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	5.9
104743			61 Medium	10.10.10.220	tcp	10001	**TLS Version 1.0 Protocol Detection**	The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	6.5
157288			61 Medium	10.10.10.220	tcp	10001	TLS Version 1.1 Deprecated Protocol	The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	6.5
10114			Low	10.10.10.221			ICMP Timestamp Request Remote Date Disclosure	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).	4.2

Tabla I8. Análisis del impacto de los activos del hogar

Nombre de Activo	Fabricante	Número de Serie	Tipo	Sistema Operativo	Propietario (Responsable)	Usuario / Custodio	Ubicación Física	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)	Valor de Impacto (VA)
Teléfono Inteligente	Xiaomi	2201117TL	Dispositivo	Android	Jefe de Hogar	Yulisa Acosta	Casa	Alto	Alto	Alto	Alto
Cámara Inteligente para Interiores	Nexxt Home	AHIMPFI4U1	Dispositivo	Firmware	Jefe de Hogar	Francisco Acosta	Sala	Medio	Medio	Medio	Medio
Aplicación Cámara Vigilancia	Nexxt Home		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Sensor de Contacto para Puertas y Ventanas	Tuya	LR03DC	Dispositivo	Firmware	Jefe de Hogar	Francisco Acosta	Puerta Principal	Medio	Medio	Medio	Medio
Aplicación Sensor Puerta	Tuya		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Sensor de Contacto para Puertas y Ventanas	Tuya	LR03DA	Dispositivo	Firmware	Jefe de Hogar	Francisco Acosta	Puerta Secundaria	Medio	Medio	Medio	Medio
Aplicación Sensor Puerta	Tuya		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Enchufe Inteligente	Smart Life	PT2024	Dispositivo	Firmware	Jefe de Hogar	Carmen Proaño	Sala de estar	Bajo	Bajo	Bajo	Bajo
Aplicación Enchufe Inteligente	Smart Life		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Enchufe Inteligente	Nexxt Home	AHIWPSO4U1	Dispositivo	Firmware	Jefe de Hogar	Francisco Acosta	Cocina	Bajo	Bajo	Bajo	Bajo
Aplicación Enchufe Inteligente	Nexxt Home		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Bombilla Inteligente	Nexxt Home	X4YHABUW110	Dispositivo	Firmware	Jefe de Hogar	Carmen Proaño	Habitacion Principal	Bajo	Bajo	Bajo	Bajo
Aplicación Bombilla Inteligente	Nexxt Home		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Bombilla Inteligente	Nexxt Home	X4WHABCY110	Dispositivo	Firmware	Jefe de Hogar	Yulisa Acosta	Habitacion Huespedes	Bajo	Bajo	Bajo	Bajo
Aplicación Bombilla Inteligente	Nexxt Home		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Interruptor de Luz Inteligente	Teclam	PS0213	Dispositivo	Firmware	Jefe de Hogar	Francisco Acosta	Sala/Cocina	Bajo	Bajo	Bajo	Bajo
Aplicación Interruptor Inteligente	Teclam		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto
Echo Dot	Amazon	G6G22H0724620VPV	Dispositivo	Firmware	Jefe de Hogar	Francisco Acosta	Sala	Alto	Alto	Alto	Alto
Aplicación Alexa	Amazon		Aplicación	Android/iOS	Jefe de Hogar	Francisco Acosta		Alto	Alto	Alto	Alto

Tabla I9. Plan de acción de tratamiento de riesgos del sistema IoT

Actividad	Objetivo	Tiempo	Responsable	Descripción	Riesgos	Indicadores de Éxito	Entregables
Implementar Medidas de Seguridad	Mejorar la seguridad de la infraestructura de TI mediante la implementación de medidas de seguridad adicionales.	3 meses	Equipo de Seguridad de la Información	La actividad consiste en identificar y poner en práctica medidas de seguridad adicionales para proteger la infraestructura de TI de la organización. Esto puede incluir la instalación de firewalls, antivirus, sistemas de detección de intrusiones, y políticas de seguridad más estrictas.	Los riesgos asociados pueden incluir la falta de recursos adecuados, resistencia al cambio por parte de los usuarios y posibles interrupciones en el servicio durante la implementación.	Reducción de incidentes de seguridad, mejora en la detección y respuesta a amenazas, y cumplimiento con estándares de seguridad reconocidos.	Informe de Evaluación de Riesgos Plan de Implementación de Medidas de Seguridad Configuración de Firewall Actualizada Informe de Monitoreo de Seguridad Capacitación del Personal de TI Auditoría de Seguridad de Infraestructura
Actualizar Software	Mejorar la seguridad de los sistemas mediante la actualización regular del software.	Continuo	Equipo de IT	Esta actividad implica establecer un proceso regular para identificar, descargar e instalar actualizaciones de software y parches de seguridad en todos los sistemas y aplicaciones de la organización. Se deben seguir las mejores prácticas de gestión de cambios para minimizar el impacto en las operaciones.	Los riesgos incluyen interrupciones en el servicio debido a actualizaciones fallidas, incompatibilidad con sistemas existentes y posibles vulnerabilidades no parcheadas.	Aumento en la seguridad de los sistemas, reducción de vulnerabilidades conocidas y cumplimiento con los requisitos de seguridad y regulaciones.	Calendario de Actualización de Software Informe de Actualización de Software Política de Actualización de Software Registro de Incidencias de Seguridad Capacitación en Gestión de Actualizaciones Informe de Pruebas de Compatibilidad
Utilizar Comunicaciones Encriptadas	Proteger la confidencialidad de la información durante la transmisión mediante el uso de comunicaciones encriptadas.	6 meses	Equipo de Seguridad de la Información	Esta actividad implica implementar y configurar comunicaciones encriptadas, como SSL/TLS, para proteger la confidencialidad de los datos durante la transmisión a través de redes públicas o no seguras. Se debe realizar un análisis de riesgos para identificar las comunicaciones que requieren encriptación y seleccionar los protocolos de encriptación adecuados.	Los riesgos pueden incluir la complejidad de implementación, la falta de compatibilidad con sistemas heredados y la degradación del rendimiento debido al cifrado.	Reducción en el número de datos interceptados, cumplimiento con requisitos de seguridad de la información y mejora en la confianza del cliente y la reputación de la organización.	Plan de Implementación de Encriptación Informe de Auditoría de Encriptación Configuración de Protocolos de Seguridad Informe de Pruebas de Seguridad Manual de Políticas de Comunicación Segura Capacitación en Seguridad de la Información
Implementar Gestión Segura de Credenciales	Fortalecer la seguridad de la autenticación y prevenir el acceso no autorizado mediante la implementación de una gestión segura de credenciales.	4 meses	Equipo de Seguridad de la Información	Esta actividad implica establecer políticas y procedimientos para la gestión segura de credenciales, incluida la implementación de autenticación multifactorial, el uso de contraseñas seguras y la revisión regular de permisos de acceso. Se deben utilizar herramientas de gestión de identidades y accesos para centralizar y automatizar la administración de credenciales.	Los riesgos pueden incluir la resistencia al cambio por parte de los usuarios, la pérdida de productividad durante la implementación y posibles violaciones de la privacidad de los empleados.	Reducción en el número de violaciones de credenciales, mejora en la seguridad de la autenticación y cumplimiento con regulaciones de privacidad de datos.	Política de Gestión de Credenciales Informe de Implementación de Autenticación Multifactor Registro de Acceso Seguro Informe de Auditoría de Seguridad de Acceso Capacitación en Seguridad de Acceso Evaluación de Herramientas de Gestión de Identidad