Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

www.concienciadigital.org

Plan de mitigación de riesgos ante vulnerabilidades y amenazas presentes en un dispositivo IoT

Risk mitigation plan for vulnerabilities and threats in an IoT device

[1] John Fernando Calle Sarmiento https://orcid.org/0009-0009-4840-6433
Maestría en Ciberseguridad, Universidad Católica de Cuenca, Azuay, Cuenca, Ecuador.
jfcalles74@est.ucacue.edu.ec

[2] Juan Pablo Cuenca Tapia https://orcid.org/0000-0001-5982-634X
Maestría en Ciberseguridad, Universidad Católica de Cuenca, Azuay, Cuenca, Ecuador.
jpcuenca@ucacue.edu.ec

Artículo de Investigación Científica y Tecnológica
Enviado: 24/08/2023
Revisado: 22/09/2023
Aceptado: 09/10/2023
Publicado:06/11/2023
DOI: **https://doi.org/10.33262/concienciadigital.v6i4.2.2773**

Cítese: Calle Sarmiento , J. F., & Cuenca Tapia, J. P. (2023). Plan de mitigación de riesgos ante vulnerabilidades y amenazas presentes en un dispositivo IoT. ConcienciaDigital, 6(4.2), 141-160. https://doi.org/10.33262/concienciadigital.v6i4.2.2773

Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

www.concienciadigital.org

Palabras claves:
OWASP; vulnerabilidades; amenazas; mitigación; riesgos.

Resumen

Introducción. La rápida evolución tecnológica, en particular el Internet de las cosas (IoT), ha transformado la vida cotidiana. Sin embargo, las cámaras web, utilizadas para múltiples propósitos, enfrentan amenazas como el acceso no autorizado, la filtración de información y la transmisión de video en tiempo real a otros dispositivos. Esta problemática se centra en determinar si la cámara TP-Link Kasa Spot, un dispositivo IoT, está expuesta a vulnerabilidades que puedan comprometer la seguridad de datos. **Objetivo.** Llevar a cabo una evaluación de las amenazas y debilidades presentes en la cámara web y su aplicación móvil, utilizando herramientas de software especializadas, con la finalidad de preservar la confidencialidad, integridad y disponibilidad del dispositivo IoT. **Metodología.** Para llevar a cabo esta investigación, se ha optado por utilizar la metodología OWASP, ya que su estructura es práctica y adecuada para el proceso. **Resultados.** El estudio se enfocó en la creación de un plan exhaustivo de mitigación de riesgos para abordar las vulnerabilidades y amenazas presentes en la cámara web y la aplicación móvil. Con el propósito de brindar a los usuarios una mayor protección, concientización y confianza en el uso de la tecnología emergente. **Conclusión.** Después de analizar los resultados, se concluye que la implementación del plan de mitigación de riesgos ha contribuido a mejorar la experiencia de uso de esta tecnología, lo que a su vez ayuda a prevenir potenciales ataques en el futuro. **Área de estudio general:** Tecnologías de la Información. **Área de estudio específica:** Ciberseguridad.

Keywords:
OWASP; vulnerabilities; threats; mitigation; risks.

Abstract

Introduction. The Internet of Things (IoT) has drastically changed daily life because of the rapid advancement of technology. Webcams, which serve a variety of functions, are, nevertheless, vulnerable to dangers like illegal access, data leakage, and real-time video streaming to other devices. The goal of this investigation is to determine whether the IoT device, the TP-Link Kasa Spot camera, is vulnerable to flaws that could jeopardize data security. **Objective.** Using specialist software tools, evaluate the dangers and weaknesses inherent in the webcam and its mobile application to maintain the IoT device's

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

confidentiality, integrity, and availability. **Methodology.** We chose the OWASP methodology to conduct this research since its structure is practical and suited for the procedure. **Results.** The study aimed to develop a comprehensive risk mitigation strategy to address the vulnerabilities and threats found in the webcam and mobile application. With the goal of increasing user protection, awareness, and confidence in the use of modern technologies. **Conclusion.** Based on the results, it is considered that the risk mitigation plan's implementation has contributed to improving the experience of using this technology, which in turn helps prevent potential future attacks. **General Area of Study:** Information Technology. **Specific Area of Study:** Cybersecurity.

Introducción

La gran evolución tecnológica que se han tenido en los últimos años ha influido en la forma y manera en la que se realizan ciertas actividades, por ejemplo "En la actualidad el internet de las cosas (IoT) ha producido un gran impacto en la sociedad, lo cual ha transformado nuestra vida cotidiana en todos los ámbitos, como laboral, empresarial, industrial, social" (Cruz et al., 2015), y considerando que "al ser equipos electrónicos, estos disponen de procesadores, tarjetas de red, memoria y sistemas operativos, por esta composición podría ocasionar vulnerabilidades que pueden ser aprovechado por los atacantes"(Arnau, 2023).

"La lucha constante de las personas por satisfacer sus propias necesidades de comunicación, es la fuerza impulsora detrás de la construcción de procesos de comunicación cada vez más potentes y rápidos en todo el mundo" (Bellasmil & Zúñiga, 2018), ante esto uno de los procesos ha sido el desarrollo de cámaras web para el control, monitoreo, seguridad, videoconferencias, entre otras.

Enfocándose en una cámara web, se debe prestar atención por la importancia de las mismas en los sistemas y entidades donde se implementan, como problemática se identifica el acceso no autorizado, filtración de información, grabación y transmisión de video en tiempo real, hacia otros dispositivos (Lluís & Robles, 2022). En cuanto a los riesgos y vulnerabilidades, se infiere que son versátiles y surgen a cada momento (aparecen nuevos ataques y atenuaciones), divididos en varios componentes, según su naturaleza (Cerasela, 2021).

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

Dicho lo anterior la problemática presentada surge de la necesidad de saber si un dispositivo IoT está expuesto a vulnerabilidades y brechas de seguridad que afecten alguno de los ejes de la triada CID, en este preciso caso la cámara TP-Link Kasa Spot (Tp-link, 2023).

Metodología

Para el desarrollo de esta investigación se utilizó la metodología OWASP propuesta por (Li & Mogos, 2023). En la figura 1 se muestra los pasos que dicha metodología recomienda utilizar para que los resultados tengan validez y sean óptimos.

Para desarrollar la metodología se utilizará el sistema operativo Kali Linux (Millán-Rojas et al., 2016). Dentro de una máquina virtual la cual ayudara a tener un mejor uso del sistema operativo (Ortiz et al., 2022).

En la figura 1, a continuación, muestra as fases de la metodología OWASP.

Figura 1

Fases de la Metodología OWASP

Fuente: basado en Hernández (2022)

Desarrollo

El análisis se llevó a cabo en un laboratorio controlado. Este enfoque permite garantizar que los resultados obtenidos no afecten a ninguno en particular, y se mantendrá la confidencialidad necesaria para preservar la seguridad de los datos. Además, el proyecto se centró en la detección de vulnerabilidades establecida en el marco de trabajo de OWASP, para llevar a cabo el análisis, se utilizarán herramientas de reconocimiento

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

como *Nmap y OpenVas*. Estas herramientas son ampliamente utilizadas en el análisis de vulnerabilidades y facilitan la exploración y el análisis del dispositivo IoT (Lyon, 2008).

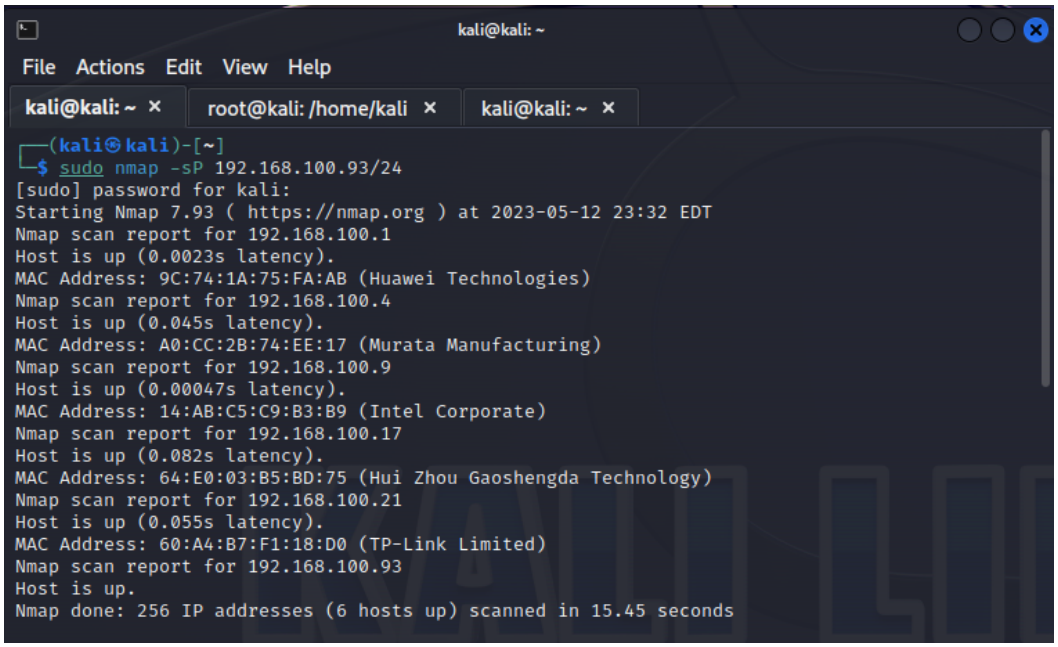
Fase 1: Recopilación de información

Recopilación de IPs y puertos: Se busca obtener la dirección IP de la cámara que se quiere analizar. Para lograr esto, se manejará diferentes herramientas y técnicas. Mediante un mapeo de la red se pretende obtener información necesaria que permita realizar un correcto análisis de las vulnerabilidades del dispositivo IoT (Álvarez, 2023).

Para la identificación de la IP y puertos abiertos se usa Nmap, con los siguientes comandos que se describe en la figura 2, a continuación.

Figura 2

Comando Nmap Para la Búsqueda de Dirección IP



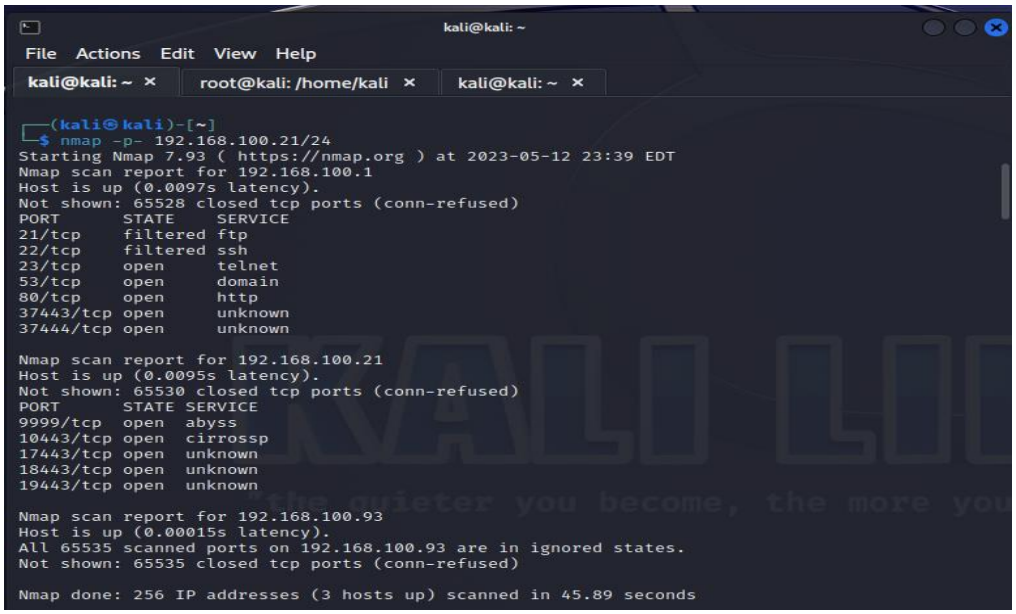
Fuente: basado en Lyon (2008)

Además, con el comando que especifica en la figura 3, muestra los puertos abiertos de la cámara web, dando así datos al ciber atacante para poder realizar el *pentesting* del dispositivo.

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

Figura 3

Comando Nmap para identificar puertos abiertos



En la tabla 1, se muestra cada uno de los puertos abiertos y cuál es su vulnerabilidad respectiva a la que afecta.

Tabla 1

Descripción de puertos

Puerto	Estado	Descripción	Posibles ataques
9999/tcp (Abyss Web Service)	Open	Utilizado para servicios y aplicaciones de red diferentes.	Ataque Dos
10443/tcp	Open	Servicios web seguro. Protocolos HTTPS para cifrar la comunicación entre cliente y el servidor.	Ataque de fuerza bruta (descubrir contraseñas débiles) Ataques de inyección SQL
17443/tcp	Open	Productos de seguridad como: firewall y sistemas de gestión de seguridad.	Ataques de denegación de servicios (DoS).
18443/tcp	Open	Servicios de mensajería.0	Ataque de hombre en el medio (MITM).
19443/tcp	Open	Servicios web seguros (HTTPS, SSL)	Ataques de phishing (engaño a los usuarios).

Nota: Análisis realizado con la herramienta NMAP

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

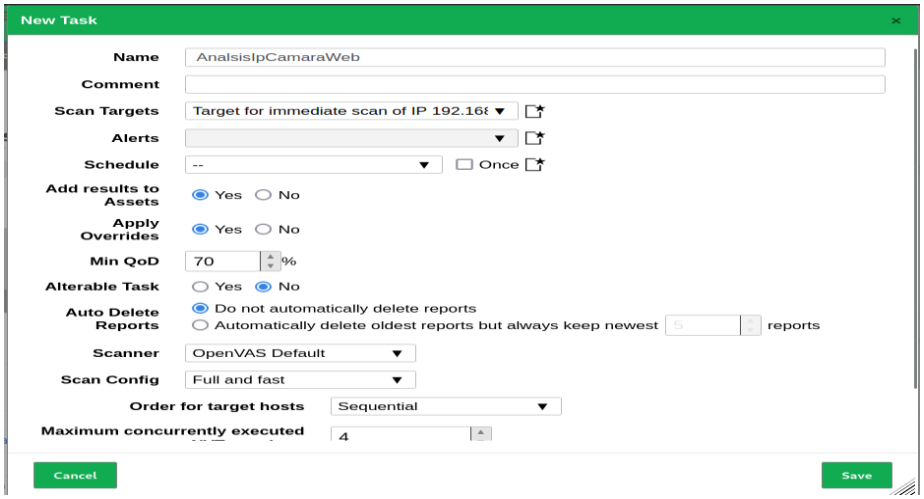
Fase 2: Análisis de vulnerabilidades

Según Díaz (2022), se utilizó la información obtenida en el paso previo para realizar un análisis en herramientas necesarias.

En las figuras 4 y 5, se muestra el proceso y análisis de las vulnerabilidades de acuerdo con la dirección IP encontrada en la fase anterior.

Figura 4

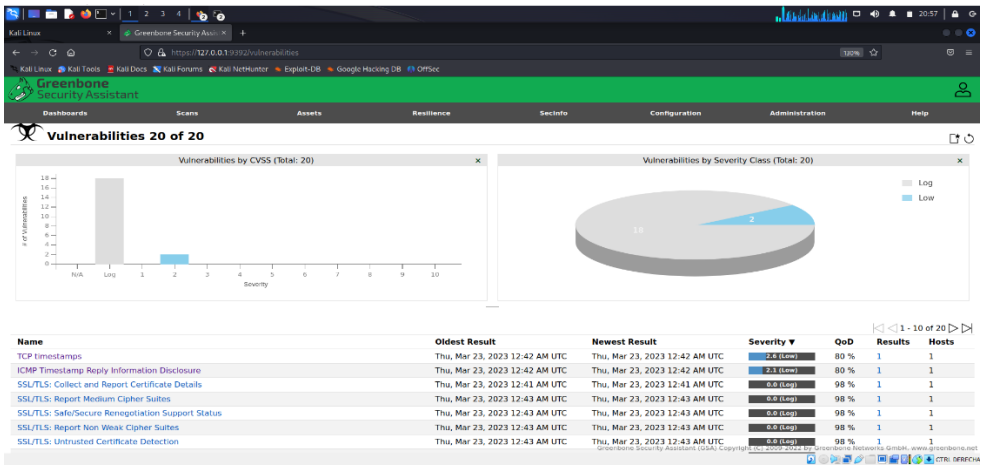
Especificación de dirección IP en OpenVAS



Fuente: basado en la herramienta OpenVAS, Chiluiza & Enciso (2023)

Figura 5

Resultado de análisis de vulnerabilidades



Nota: basado en la herramienta OpenVAS

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

En esta figura se muestra un resumen de las vulnerabilidades encontradas, en el siguiente orden:

- 18 vulnerabilidades de tipo log que representan una criticidad nula
- 2 vulnerabilidades de tipo low, que representan una criticidad baja.

Por lo tanto, se decidió utilizar estas últimas con la finalidad de mitigarlas.

Activos afectados por las vulnerabilidades

En la tabla 2, se muestra las vulnerabilidades encontradas en el análisis ejecutado en la herramienta OpenVAS, además se detalla su valoración de la triada CID.

Tabla 2

Listado de vulnerabilidades

Código de Vulnerabilidad	Código Activo	Activo de información	Vulnerabilidad	Disponibilidad	Integridad	Confidencialidad	Severidad	Impacto
Vul-01	Act-001	Cámara web	TCP Timestamps	Ninguna	Ninguna	Parcial	Bajo	Prescindible
Vul-02	Act-001	Cámara web	ICMP Timestamp Reply Information Disclosure	Ninguna	Ninguna	Parcial	Bajo	Prescindible

Análisis de vulnerabilidades

En la tabla 3 y 4, se detallan todo lo relacionado con las vulnerabilidades encontradas.

Tabla 3

Descripción a detalle de la vulnerabilidad

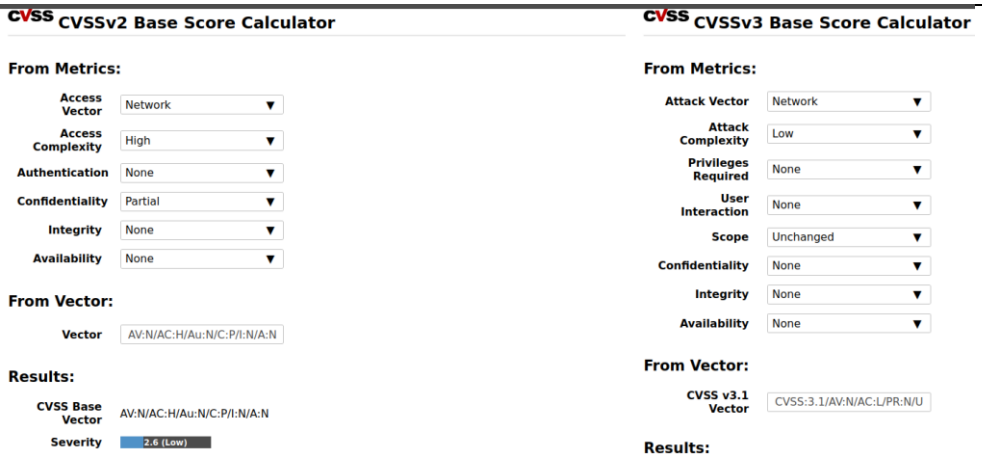
CODIGO	CVSS	TITULO
Vul-01	CVSS Base Vector: AV:/AC:H/Au:N/C:P/I:N/A:N CVSS Origin: N/A	TCP Timestamps

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Parcial	Ninguna	Alta

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

Tabla 3

Descripción a detalle de la vulnerabilidad (continuación)

DESCRIPCION
La vulnerabilidad de TCP Timestamps puede afectar la privacidad y seguridad en línea al permitir que los atacantes obtengan información sensible, identifiquen dispositivos y realicen ataques DoS y de inundación de paquetes.
REFERENCIAS
RFC 7323 - TCP Extensions for High Performance - This document defines the TCP Timestamps option and explains its use. RFC 1323 - TCP Extensions for High Performance - This document first introduced the TCP Timestamps option. Stevens, W. Richard. TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition). Addison-Wesley, 2011. - This book provides a detailed explanation of the TCP Timestamps option and its use. Kurose, James F., and Keith W. Ross. Computer Networking: A Top-Down Approach (7th Edition). Pearson, 2016. - This book introduces TCP and includes a discussion of the TCP Timestamps option.
EVIDENCIAS CVSS


Nota: basado en matriz de identificación de vulnerabilidades

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

Tabla 4

Descripción a detalle de la vulnerabilidad

CODIGO	CVSS	TITULO
Vul-02	CVSS Base Vector: AV: L/AC:L/Au:N/C:P/I:N/A: N CVSS: Origin N/A	ICMP Timestamp Reply Information Disclosure
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Parcial	Ninguna	Alta

DESCRIPCION

La vulnerabilidad de *ICMP Timestamp Reply Information Disclosure* permite a un atacante obtener información sensible a través de las respuestas de tiempo de los dispositivos en una red. Esto podría revelar detalles sobre el sistema, incluyendo su tiempo de actividad y posiblemente su ubicación. Los atacantes también podrían utilizar esta información para explotar vulnerabilidades y realizar ataques adicionales en la red. Es importante aplicar medidas de seguridad y configuración adecuadas para proteger contra esta vulnerabilidad.

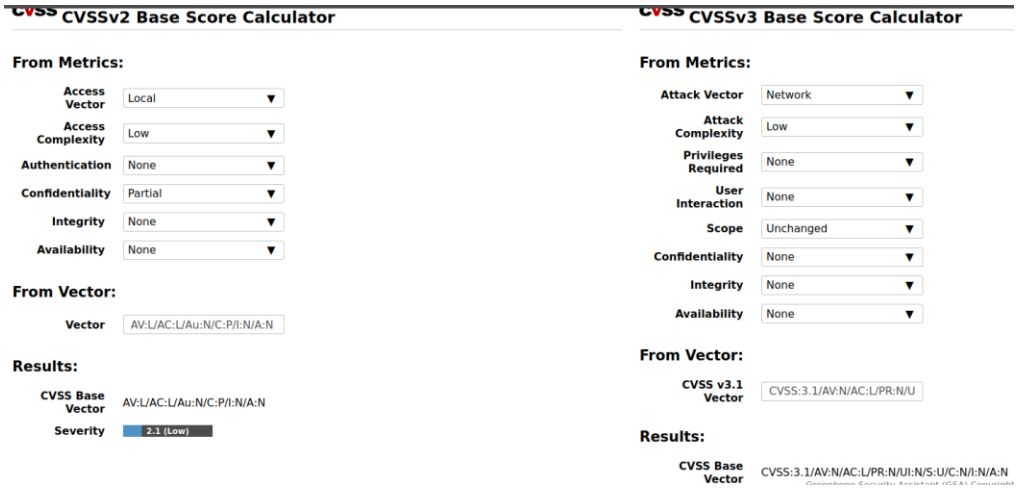
REFERENCIAS

MISC:http://descriptions.securescout.com/tc/11010

MISC:http://descriptions.securescout.com/tc/11011

MISC:http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1434

EVIDENCIAS



Nota: basado en matriz de identificación de vulnerabilidades

OWASP Mobile Top Ten

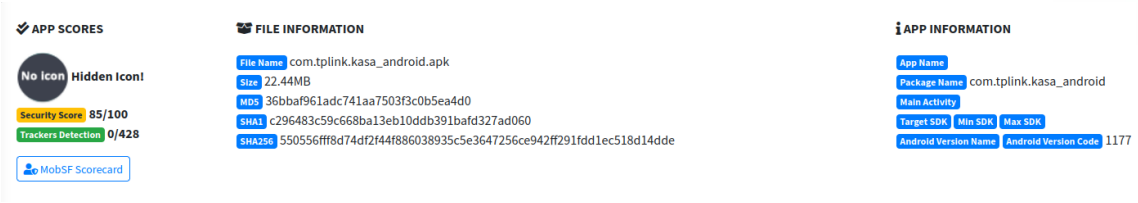
Se realizó un análisis de las vulnerabilidades mediante la herramienta MobSF, para identificar los riesgos y amenazas que se encuentra expuesta la aplicación móvil (Abdullah et al., 2022).

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

En la figura 6, se aprecia la información detallada de la aplicación móvil que se analizó.

Figura 6

Descripción de la Aplicación Móvil



Nota: basado en Bozzini & Bozzini (2023)

Análisis de seguridad

En la tabla 5, se identifica las vulnerabilidades encontradas en el análisis de la aplicación móvil, utilizando la herramienta MobSF.

Tabla 5

Análisis de manifiesto

Asunto	Severidad	Descripción
Los datos de la aplicación se pueden respaldar [android:allowBackup:true] flag is missing.	Medio	El indicador [android: allowBackup:true] de forma predeterminada, se establece en verdadero y permite que cualquier persona haga una copia de seguridad de los datos de su aplicación a través de ADB. Permite a los usuarios que han habilitado la depuración de USB copiar datos de aplicaciones fuera del dispositivo.

Análisis manual de aplicación móvil

- Vulnerabilidades de autenticación: La cámara utiliza un sistema de autenticación para permitir el acceso a la misma.
- Exposición de datos: Estas vulnerabilidades permiten a un atacante acceder a esos datos, incluyendo video o audio capturados por la cámara y alojados en la nube.
- Vulnerabilidades en la conexión wifi: La cámara se conecta a una red wifi, lo que la hace susceptible a posibles ataques como el robo de contraseñas, el ataque de hombre en el medio, la suplantación de identidad de la red wifi, entre otros.

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

En la tabla 6, de detalla las amenazas y la clasificación del CID, que se podrían encontrar en un ambiente común sobre la aplicación móvil que maneja el funcionamiento de las cámaras web TP-Link Kasa Spot.

Tabla 6

Amenazas encontradas

Amenaza	Descripción	C	I	D	Impacto
Acceso no autorizado	Terceras personas pueden acceder a la cámara web sin permiso, ya sea de manera física o remota, así teniendo acceso a la privacidad del usuario afectando la confidencialidad, integridad y disponibilidad.	Alto	Bajo	Alto	Importante
Descarga de aplicación de tienda no oficial	Las descargas de sitios no oficiales	Alto	Alto	Alto	Grave
Malware	Existen varias maneras de infectar una cámara web. Dando acceso al atacante teniendo así acceso al dispositivo.	Alto	Alto	Alto	Grave
Intercepción de datos (MiTM)	El atacante puede interceptar los datos de la cámara web y utilizar con fines maliciosos.	Alto	Bajo	Bajo	Importante
Configuración inadecuada	Configuración incorrecta o insegura	Bajo	Bajo	Bajo	Prescindible
Espionaje corporativo	Las cámaras pueden ser utilizadas en el trabajo para controlar a los empleados.	Bajo	Bajo	Bajo	Prescindible
Ataque de fuerza bruta	Técnica utilizada para descifrar contraseñas.	Medio	Alto	Medio	Importante
Ataque de denegación de servicios (DoS)	Busca la forma de abrumar al servidor o al tráfico de red así dejando inaccesible.	Bajo	Bajo	Alto	Importante

Fase 3: Explotación de vulnerabilidades

Se utilizó herramientas alojadas en Kali Linux con la finalidad de verificar la seguridad que posee el dispositivo.

Prueba de marca de tiempo

Se realizó una prueba de tempo del análisis TCP/IP para verificar las marcas de tiempo de la vulnerabilidad *ICMP Timestamp Reply Information Disclosure*, que se encontró en el análisis de vulnerabilidades.

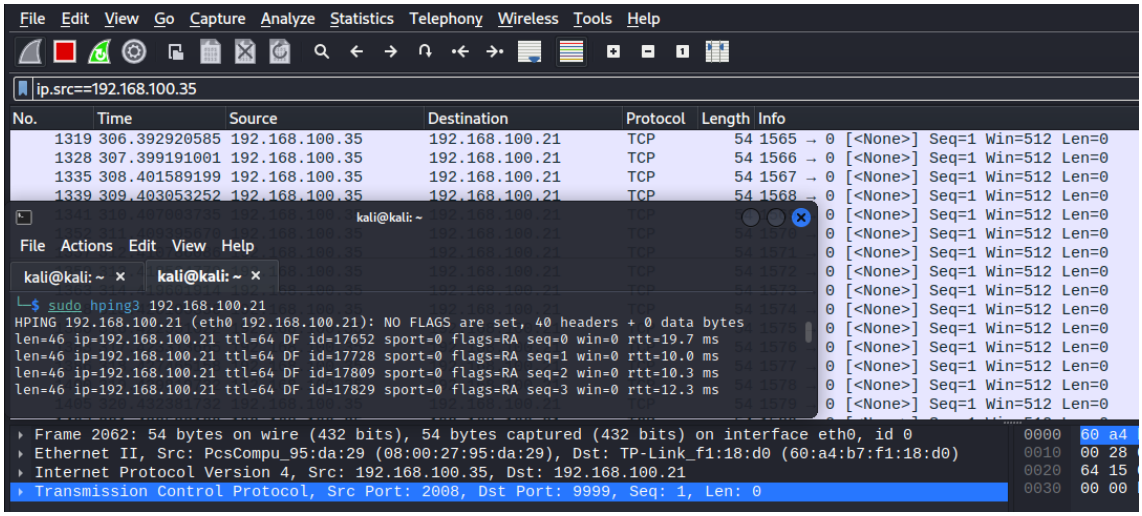
Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

Para el desarrollo de las siguientes pruebas se usó las herramientas Wireshark para el control de tráfico de red y hping3, para él envió de comandos para verificar el *Timestamp* (Castro, 2023).

En la figura 7, se muestra el comando de conexión del dispositivo IoT y el filtrado de la dirección IP de la maquina atacante para la verificación del tráfico de datos.

Figura 7

Detalle de la Conexión



Nota: basado en la herramienta Kali Linux y Wireshark

En la figura 8, se muestra el comando con la función de disparar paquetes al dispositivo para obtener el tiempo de respuesta.

Figura 8

Verificación del tiempo de respuesta

Nota: basado en la herramienta hping3 (Kali Linux)

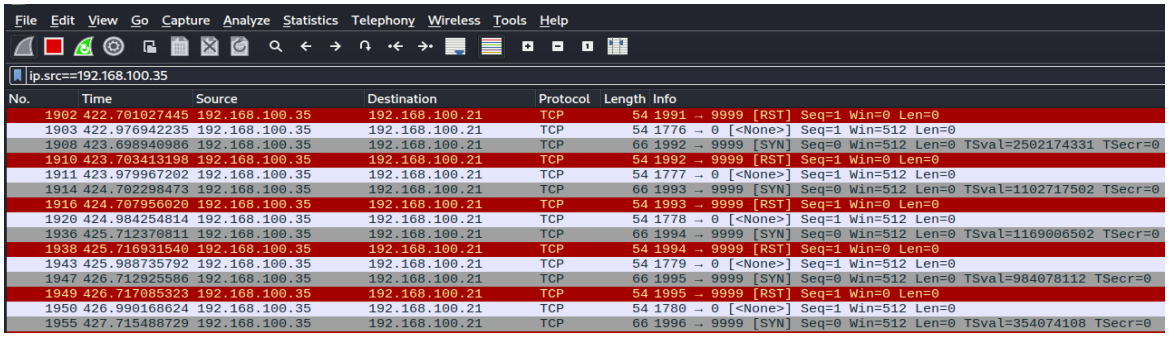
Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

En la figura 8, se pudo apreciar la ejecución de comando con el objetivo de obtener el tiempo de respuesta que se obtuvo en la vulnerabilidad TCP Timestamp, mediante el puerto que se usa por defecto en el dispositivo IoT.

En la figura 9, se muestra la evidencia que se tiene en cuanto a los paquetes que fueron disparados para verificar el Timestamp.

Figura 9

Verificación de paquetes enviados



Nota: basado en la herramienta de Wireshark

Fase 4: Informe de resultados

Se presenta un resumen detallado una vez concluido el desarrollo de la metodología; los resultados que se presentaran surgen del análisis realizado en la cámara web TP-Link Kasa Spot, bajo el desarrollo de un laboratorio en un ambiente controlado.

En la tabla 7, se muestra la descripción detallada de las vulnerabilidades más influyentes.

Tabla 7

Descripción de vulnerabilidades

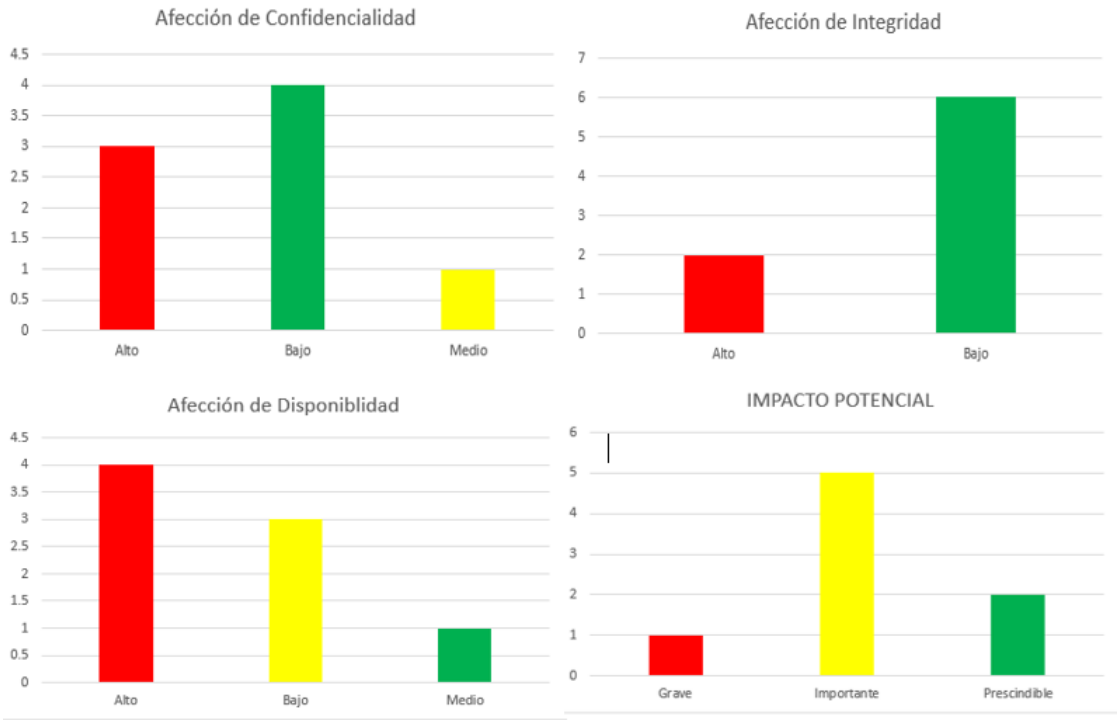
Vulnerabilidad	Descripción	Gravedad	Expuesto ataque	Consecuencias
TCP Timestamps	permite intercambiar entre ambos extremos los valores del reloj del sistema	Media	Baja exposición, ya que el atacante deberá adivinar un timestamp válido.	Si se llega insertar el segmento con un tiempo valido, los futuros segmentos se congelarán.
ICMP Timestamp Reply Information Disclosure	Se puede determinar la hora exacta establecida en el host remoto. Responde solicitud de marca de tiempo ICMP.	Media	Se puede obtener el tiempo de paquetes que se envía, para posterior realizar un ataque.	Esto permite al atacante sepa la fecha de configuración y esto ayude a vencer los protocolos de autenticación

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

En la figura 10, se muestran estadísticas en base a la afección e impacto de las amenazas y vulnerabilidades.

Figura 10

Afección triada CID e Impacto Potencial



La figura 10, se representa el nivel de afección a la triada CID presente en base al análisis de la cámara web y aplicación móvil, así mismo el impacto potencial que se presentaría en estas amenazas.

Resultados

Plan de mitigación de riesgos

Se basa en las vulnerabilidades y amenazas encontradas en la cámara web.

La tabla 8, se describe a detalle las medidas de mitigación.

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023
www.concienciadigital.org

Tabla 8

Plan de mitigación de riesgos

Amenaza/ Vulnerabilidades	Probabilidad que ocurra	Impacto potencial	Medidas de mitigación sugeridas
TCP Timestamps	Baja	Prescindible	Aleatorizar los timestamp, con el objetivo de mitigar los vectores anteriormente descritos.
ICMP Timestamp Reply Information Disclosure	Baja	Prescindible	Filtrar solicitudes de marca de tiempo.
Los datos de la aplicación se pueden respaldar	Medio	Grave	Se recomienda establecer el valor de "android:allowBackup" en "false" en el archivo de manifiesto de la aplicación, a menos que exista una necesidad específica de respaldar y restaurar los datos de la aplicación. Esto ayuda a proteger la privacidad y seguridad de los datos de la aplicación en caso de acceso no autorizado al dispositivo.
Acceso no autorizado	Medio	Importante	Configuración de contraseñas fuertes Desactivar cámaras que no se usen. Registros de acceso, para posibles accesos no autorizados por terceros .
Malware	Alto	Grave	Descarga de software solo en sitios confiables. Limitación de permisos en la cámara.
Interceptación de datos (MiTM)	Bajo	Importante	Utilizar conexiones seguras Encriptación de información para la transmisión de datos. Configurar la red para puertos abiertos.
Configuración no adecuada	Alta	Prescindible	Configurar el factor de doble autenticación. Restricciones de conexión de redes externas.
Espionaje corporativo	Alta	Prescindible	Creación de políticas de privacidad de los empleados, en el área que sea necesario. Protección de redes de la empresa. Segregación de redes.
Ataques de fuerza bruta	Bajo (factor doble autenticación)	Importante	Configuración de contraseñas seguras. Limitación del número de intentos de ingreso. Utilizar el software de autenticación de dos factores.

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

Tabla 8

Plan de mitigación de riesgos (continuación)

Amenaza/ Vulnerabilidades	Probabilidad que ocurra	Impacto potencial	Medidas de mitigación sugeridas
Ataque de denegación de servicios	Medio	Importante	Configuración del firewall para no permitir acceso de malintencionados. Monitoreo del tráfico de red (Wireshark).
Vulnerabilidades físicas	Medio	Importante	Protección de cubierta física. Configuración de sensores de movimiento, para el ingreso no autorizado.
Compartir datos con terceros	Alta	Importante	Selección cuidadosa de personas que tendrán acceso a la cámara web.

Conclusiones

- El análisis realizado de vulnerabilidades y amenazas proporcionó un mayor entendimiento de los riesgos a los que los usuarios se enfrentan al utilizar este tipo de tecnología. En el desarrollo de la metodología OWASP, los resultados obtenidos desempeñaron un papel fundamental en la creación del plan de mitigación.
- La versatilidad de la metodología OWASP permite llevar a cabo tanto análisis automatizados como manuales, lo que se traduce en un mejor control de calidad de los resultados obtenidos. El análisis y la creación de un plan de mitigación de riesgos para estos dispositivos contribuyen a mejorar la seguridad no solo de este módulo en particular, sino también del uso más amplio de los mismos. Estas acciones buscan brindar medidas de protección a los usuarios contra posibles ataques y reducir su exposición a vulnerabilidades.
- Gracias al análisis con herramientas automatizadas, se facilita la comprensión de los resultados, lo que conduce a un desarrollo efectivo del plan de mitigación de riesgos frente a las vulnerabilidades y amenazas identificadas. El plan de mitigación contempla varios escenarios en los cuales un ciberdelincuente podría atacar este dispositivo IoT. Sin embargo, gran parte de estos escenarios ya han sido mitigados gracias a la configuración proporcionada por el fabricante. Los puntos débiles se encuentran en la configuración del usuario, lo cual refuerza la importancia de proteger la privacidad de los datos en un mundo cada vez más interconectado, y contribuye a fortalecer la confianza de los beneficiarios de estos dispositivos.

Conflicto de intereses

No existe conflicto de intereses entre los autores

Referencias Bibliográficas

Abdullah, R. M., Abualkishik, A. Z., Isaacc, N. M., Alwan, A. A., & Gulzar, Y. (2022). An investigation study for risk calculation of security vulnerabilities on android applications. *Indonesian Journal of Electrical Engineering and Computer Science*, *25*(3), 1736–1748. https://doi.org/10.11591/ijeecs.v25.i3.pp1736-1748

Álvarez Pezo, A. M. (2023). *Diseño de una propuesta de Ciberseguridad para la detección de fuga de información a través de dispositivos IoT en el área de TI de una empresa embotelladora y distribuidora de bebidas en Arequipa- 2021*.

Arnau Muñoz, L. (2023). *Sistema de detección de anomalías para infraestructuras IoT*. 35–39. https://rua.ua.es/dspace/handle/10045/135258

Bellasmil, A. I., & Zúñiga, J. L. (2018). *Diseño e implementación de un timbre inteligente basado en el Internet de las Cosas (IoT) para fortalecer la seguridad contra robos en viviendas sociales*. 101. http://www.academia.edu/9523397/COLUMNAS_UNIVERSIDAD_NACIONAL_PEDRO_RUIZ_GALLO_COLUMNAS

Bozzini, D., & Bozzini, P. D. (2023). *How Vulnerabilities Became Commodities. The Political Economy of Ethical Hacking (1990-2020). To cite this version: HAL Id: hal-04068476 How Vulnerabilities Became Commodities the Political Economy of Ethical Hacking (1990 – 2020).*

Castro García, Á. de. (2023). *Herramienta para el despliegue de laboratorios virtuales mediante Docker*.

Cerasela Pana, A. (2021). La seguridad cibernética y los derechos humanos. Los límites de la restricción de derechos humanos para la protección del espacio cibernético. *La Seguridad Cibernética y Los Derechos Humanos. Los Límites de La Restricción de Derechos Humanos Para La Protección Del Espacio Cibernético*. https://doi.org/10.5682/9786062813604

Chiluiza, L., & Enciso, L. (2023). Detección y solución de vulnerabilidades con Greenbone Security Assistant. *Revista Ibérica de Sistemas e Tecnologías de Informação*, *E57*, 560–570.

Cruz Vega Mario, Oliete Vivas Pablo, Morales Ríos Christian, & González Carlos. (2015). *Las tecnologías IoT dentro de la industria conectada 4.0*. Fundación EOI.

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

https://www.eoi.es/es/savia/publicaciones/21125/las-tecnologias-iot-dentro-de-la-industria-conectada-40

Díaz, R. M. (2022). Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe. *Cepal*. https://repositorio.cepal.org/bitstream/handle/11362/48065/1/S2200203_es.pdf

Li, Y., & Mogos, G. (2023). Digital forensics on Tencent QQ-instant messaging service in China. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(1), 412–420. https://doi.org/10.11591/ijeecs.v29.i1.pp412-420

Lluís, L. A., & Robles, A. (2022). *Estudio de los ataques y su defensa en la ingeniería social*. Pág. 1-132. http://e-spacio.uned.es/fez/eserv/bibliuned:master-ETSInformatica-II-Lagil/Gil_Lluis_Luis_TFM.pdf

Lyon, G. F. (2008). *Nmap network scanning: official Nmap project guide to network discovery and security scanning*. Insecure. https://nmap.org/book/

Millán-Rojas, E. E., Gallego-Torres, A. P., & Chico-Vargas, D. C. (2016). Simulación de una red Grid con máquinas virtuales para crear un entorno de aprendizaje de la computación de alto desempeño. *Revista Facultad de Ingeniería*, *25*(41), 85–92. https://doi.org/10.19053/01211129.4140

Ortiz Padilla, G. A., Flores Urgilés, C. H., Padilla Cruz, I. N., & Carrillo Zenteno, J. A. (2022). Análisis de técnicas para pruebas de Ethical Hacking-Pentesting en sitios web. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *6*(42), 421–444. https://doi.org/10.29018/issn.2588-1000vol6iss42.2022pp421-444

Tp-link. (2023). *Comparison of Wireless Technologies (Bluetooth, WiFi, BLE, Zigbee, Z-Wave, 6LoWPAN, NFC, WiFi… - Hackster.io*. https://www.hackster.io/news/comparison-of-wireless-technologies-bluetooth-wifi-ble-zigbee-z-wave-6lowpan-nfc-wifi-eece5593d80f

Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 141 – 160, noviembre 2023

www.concienciadigital.org

El artículo que se publica es de exclusiva responsabilidad de los autores y no necesariamente reflejan el pensamiento de la **Revista Conciencia Digital.**

Ciencia Digital Editorial

latindex catálogo

Conciencia Digital

Indexaciones