593 Digital Publisher
CEIT
ISSN 2588-0705

Análisis de Vulnerabilidades en la Infraestructura de Red: Una Revisión Sistemática de Literatura

Vulnerability Analysis in Network Infrastructure: A Systematic Literature Review

Edison Mauricio Cornejo-Jiménez [1]
Pontificia Universidad Católica del Ecuador Sede Ambato - Ecuador
edisoncornejo21@hotmail.com

David Omar Guevara-Aulestia [2]
Pontificia Universidad Católica del Ecuador Sede Ambato - Ecuador
dguevara@pucesa.edu.ec

doi.org/10.33386/593dp.2024.5.2620

V9-N5 (sep-oct) 2024, pp 527-542 | Recibido: 28 de junio del 2024 - Aceptado: 29 de julio del 2024 (2 ronda rev.)

1 ORCID: http://orcid.org/0009-0000-8735-3420
2 ORCID: http://orcid.org/0000-0002-0410-4398

Cómo citar este artículo en norma APA:

Cornejo-Jiménez, E., Guevara-Aulestia, D., (2024). Análisis de Vulnerabilidades en la Infraestructura de Red: Una Revisión Sistemática de Literatura. 593 Digital Publisher CEIT, 9(5), 527-542, https://doi.org/10.33386/593dp.2024.5.2620

Descargar para Mendeley y Zotero

RESUMEN

Con el avance de la era digital, las organizaciones han experimentado una creciente dependencia de las tecnologías de la información y comunicación. Este aumento en la conectividad ha llevado consigo un incremento en los ataques cibernéticos a las infraestructuras de red, poniendo en peligro activos y datos críticos. En el presente artículo se desarrolla una revisión sistemática de literatura sobre el análisis de vulnerabilidades de infraestructura de red en los últimos 10 años, empleado las bases de datos IEEE, SCOPUS y Redalyc para el proceso de revisión. Se determinó que el método más utilizado fue el análisis de tráfico, y la técnica más empleada el fuzzing de protocolos de red. Predominó el análisis de vulnerabilidades sobre protocolos de red y, por tanto, el análisis del componente de servicio. El análisis de vulnerabilidades en infraestructuras de red es un ámbito de investigación que posee escasa documentación científica publicada en los últimos 10 años, requiriendo especial atención en el ámbito industrial, así como una mayor investigación en áreas emergentes como el Internet de las cosas, la inteligencia artificial y la computación en la nube.

Palabras claves: análisis de redes, seguridad, vulnerabilidades de red, métodos, técnicas.

ABSTRACT

With the advancement of the digital era, organizations have experienced an increasing dependence on information and communication technologies. This increase in connectivity has led to an increase in cyber attacks on network infrastructures, putting critical assets and data at risk. This article develops a systematic literature review on the analysis of network infrastructure vulnerabilities in the last 10 years, using the IEEE, SCOPUS and Redalyc databases for the review process. It was determined that the most widely used method was traffic analysis, and the most widely used technique was network protocol fuzzing. The analysis of vulnerabilities on network protocols predominated and, therefore, the analysis of the service component. The analysis of vulnerabilities in network infrastructures is a research area that has little scientific documentation published in the last 10 years, requiring special attention in the industrial field, as well as further research in emerging areas such as the Internet of Things, artificial intelligence and cloud computing.

Keywords: network analysis, security, network vulnerabilities, methods, techniques.

Digital Publisher CEIT ISSN 2588-0705

Introducción

Con la llegada de la era digital, las organizaciones han experimentado una creciente dependencia de las tecnologías de la información y comunicación. Paralelamente, se han incrementado los ataques cibernéticos a las infraestructuras de red, amenazando los activos y datos críticos de las organizaciones y de la sociedad, respecto a sus intereses colectivos e individuales (Sánchez et al., 2022). Una muestra de ello, fueron los eventos WannaCry Ransomware (Deola, 2023) y Krack (Pastorino, 2017) ocurridos en el año 2017, los cuales ocasionaron interrupciones en los servicios informáticos de agencias gubernamentales, así como importantes pérdidas económicas a las empresas y sus usuarios. En ambos eventos, los atacantes aprovecharon las vulnerabilidades existentes en las redes corporativas y de internet.

Las vulnerabilidades de seguridad se originan en fallos o errores en el diseño, configuración, o programación del hardware o software, los cuales posibilitan que un atacante ponga en riesgo la integridad y confidencialidad de los datos procesados por un sistema (Limones, 2022). Dentro de su clasificación se encuentran las vulnerabilidades de red, que afectan al software y a los componentes de interconexión red, las vulnerabilidades de bajo nivel y software malicioso que impactan al sistema operativo y aplicaciones, las vulnerabilidades en aplicaciones web, y finalmente las de ingeniería social, las cuales se propician por las acciones de los usuarios de sistemas (Navarro, 2011).

La infraestructura de red comprenden todos los componentes físicos y lógicos que permiten la conectividad y comunicación entre dispositivos de red, y que son esenciales para el funcionamiento de los sistemas de información (Rouse, 2023) (CISCO, 2023). Varios autores limitan su definición a componentes hardware como enrutadores y repetidores, componentes software como sistemas operativos, firewall y herramientas de gestión de red, y componentes de servicios como los protocolos de red (Rouse, 2023)(SolarWinds, 2023), excluyendo los componentes de hardware y software relacionados con aplicaciones o software que se ejecutan en la red, como computadoras personales, discos duros, o **páginas web**. El análisis de vulnerabilidades en infraestructuras de red, por lo tanto, restringe su ámbito de acción a la revisión de vulnerabilidades de red y de sistema operativo.

El análisis de vulnerabilidades es una práctica fundamental para mantener la operatividad de las redes, así como proteger los sistemas informáticos que a través de estas infraestructuras se ejecutan. Mediante técnicas y herramientas especializadas se identifican y evalúan sus debilidades potenciales, a fin de diseñar y aplicar medidas efectivas que reduzcan el riesgo de posibles ataques (Molina & Orozco, 2020) (Marcillo et al., 2021). Dicho análisis juega un rol fundamental para la seguridad de las infraestructuras de red, más aún cuando las estadísticas indican que, entre 2022 y 2023, las organizaciones tardaron un promedio de 206 días en identificar una violación de seguridad y 72 días en contenerlas (IBM Security, 2023).

Varias vulnerabilidades en infraestructuras de red podrían evitarse, por ejemplo, a partir de la actualización periódica de sistemas operativos, aplicaciones y dispositivos de red, así como su correcta configuración (Peng, 2023). Además de estas medidas, existen diversas prácticas de análisis de vulnerabilidades, como métodos y técnicas, que facilitan la identificación y mitigación de riesgos tales como los test de penetración y auditorías de seguridad (Ramírez, 2023). Los métodos son enfoques o estrategias generales utilizados para identificar y evaluar vulnerabilidades, mientras que las técnicas son procedimientos específicos, herramientas o pasos que se aplican en el proceso de análisis (Pando, 2023) (Fortra, 2022). Desde la perspectiva de la investigación documental, el amplio conocimiento que puede alcanzarse a través de la revisión de la literatura científica, puede ser especialmente útil en el ámbito de la ciberseguridad.

Conocer los métodos y técnicas más utilizados en el análisis de vulnerabilidades de infraestructuras de red, proporcionaría una base

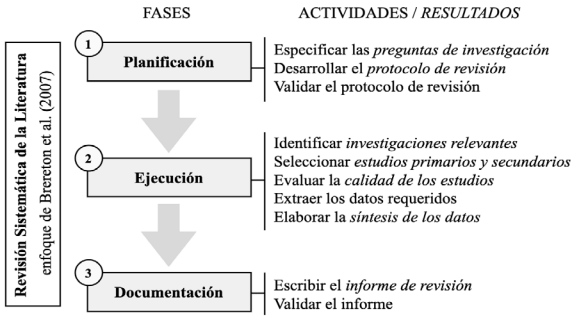
sólida para la toma de decisiones y el desarrollo continuo de mejores prácticas de seguridad informática, en su ámbito específico. Por su parte, identificar las vulnerabilidades analizadas en distintas infraestructuras de red, permitiría a los profesionales de seguridad anticiparse a posibles brechas de seguridad y desarrollar estrategias de mitigación efectivas, mejorando así la resiliencia de las organizaciones frente a posibles ataques. Explorar las tendencias de investigación, respecto a los componentes sobre los cuales se han centrado estos estudios, facilitaría la identificación de los **ámbitos en los que se carece de conocimiento documentado científicamente, o en los cuales es insuficiente.**

En la presente investigación, se ha propuesto obtener una visión general de los diferentes métodos y técnicas utilizados en el análisis de vulnerabilidades en la infraestructura de red, así como identificar las vulnerabilidades y los componentes de infraestructura de red analizados, a partir de una Revisión Sistemática de la Literatura (RSL) de los últimos 10 años. El presente estudio se encuentra organizado en cinco secciones principales: la descripción de los métodos empleados en el estudio, el desarrollo o ejecución de la revisión sistemática, la presentación de resultados, su discusión técnica, y conclusiones generales.

Método

La investigación se diseñó como un estudio cualitativo, de naturaleza aplicativa y alcance descriptivo, y en el cual se aplicaron los métodos analítico-sintético y deductivo para el análisis y la discusión de resultados. En cuanto a la RSL, se aplicó el enfoque sistemático de Brereton et al. (2007), mismo que se sostiene su ejecución en tres fases: planificación, ejecución y documentación de la revisión. Sus actividades, a detalle, se describen en la Figura 1.

Figura 1
Proceso de Revisión Sistemática de la Literatura



Nota. Basado en *Systematic literature review process* (p.572), de Brereton et al. (2007). La figura muestra los resultados de cada fase del proceso con letra cursiva (7 resultados en total).

A continuación, se describen los resultados de la fase de planificación de la RSL.

Preguntas de investigación

Las preguntas de investigación parten de la determinación clara de la necesidad de información (Brereton et al., 2007). En este caso, la necesidad de conocimiento documentado sobre los métodos y técnicas empleados en el análisis de vulnerabilidades de infraestructuras red en los últimos 10 años, las vulnerabilidades identificadas recurrentemente, y los componentes de la infraestructura de red en los cuales se ha centrado la investigación científica. Esta información es requerida en el ámbito de la gestión de redes, para la toma de decisiones informada y el desarrollo de planes de mitigación.

P1: ¿Qué métodos han sido utilizados en el análisis de vulnerabilidades en infraestructuras de red, en los últimos 10 años?

P2: ¿Qué técnicas han sido utilizadas en el análisis de vulnerabilidades en infraestructuras de red, en los últimos 10 años?

P3: ¿Qué vulnerabilidades han sido analizadas en infraestructuras de red, en los últimos 10 años?

593 Digital Publisher CEIT ISSN 2588-0705

P4: ¿Qué componentes de la infraestructura de red han sido analizados en sus vulnerabilidades, en los últimos 10 años?

Protocolos de revisión

Para la revisión sistemática de la literatura se han seleccionado las bases de datos SCOPUS, IEEE y Redalyc, mismas que promueven la divulgación de información científica de alto impacto en el ámbito específico de las tecnologías de la información (Ierardi et al., 2017) (Codina, 2019). Las bases de datos proporcionaron una visión amplia y complementaria de la información requerida.

En la determinación de la cadena de búsqueda, se seleccionaron los términos clave de las preguntas de investigación, siendo estos: análisis, vulnerabilidades, protocolo, red, métodos, y técnicas. Las cadenas de búsqueda, con base en los protocolos de revisión, se configuraron de la siguiente forma:

IEEE: ("All Metadata":analysis) AND ("All Metadata":vulnerabilities) AND ("All Metadata":network) AND ("All Metadata":method) AND ("All Metadata":technique) - Filtros: Rango (2014-2023) y OpenAccess = true

SCOPUS: TITLE-ABS-KEY (analysis AND vulnerabilities AND network AND method AND technique) AND PUBYEAR > 2013 AND PUBYEAR < 2024 AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (SUBJAREA , "COMP"))

REDALYC: (analysis AND vulnerabilities AND network AND method AND technique) – Filtros: Rango (2014-2023), Disciplina (Ingeniería, Computación, Comunicación, Ciencias de la Información)

Se consideran varios criterios de inclusión y exclusión de información científica. Entre los criterios de inclusión, se encuentran: investigaciones de los últimos 10 años (publicados entre el 2014 al 2023), divulgadas a través de revistas científicas o actas de congresos, y escritas en idiomas español e inglés. Por otra parte, los criterios de exclusión son: poster científico, contenido de acceso pagado y enfoque distinto al de ciberseguridad.

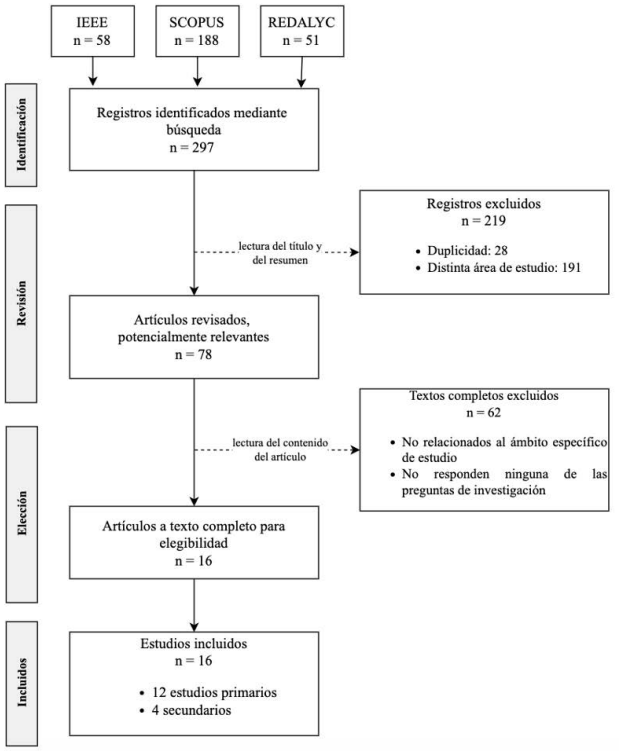
La validación del protocolo de revisión consistió en un rápido análisis de los resultados obtenidos en la ejecución de las cadenas de búsqueda en SCOPUS, IEEE y Redalcy, dentro del cual se realizó una prueba de extracción de datos en torno a las preguntas de investigación. Como resultado, se identificó un primer artículo científico elegible en cada base de datos cuyo contenido respondía a las preguntas establecidas. Se concluyó, por lo tanto, que el protocolo respondía adecuadamente al objetivo del estudio.

Desarrollo

Dentro de la fase de ejecución de la RSL se llevaron a cabo varios procesos, como la identificación de investigaciones relevantes, la selección de estudios primarios y secundarios, la evaluación de la calidad de los estudios, la extracción de los datos requeridos, y la síntesis de los mismos (Brereton et al., 2007). La Figura 2 ilustra el proceso de selección de estudios.

Figura 2

Flujograma de selección de estudios



Investigaciones relevantes

Al 13 de diciembre de 2023, la aplicación de las cadenas de búsqueda en IEEE, SCOPUS y Redalyc dio como resultado un total de 297 investigaciones identificadas. Luego de analizar los títulos y resúmenes, se filtraron 78 investigaciones como potencialmente relevantes, excluyendo 219 registros por duplicidad (28) y enfoque en otras áreas (191). De aquellos que se enfocan en otras áreas, 67 investigaciones tratan específicamente sobre ataques de red, a nivel experimental o descriptivo.

Estudios primarios y secundarios

Para la selección de estudios primarios y secundarios, se efectuó una revisión completa del contenido de cada una las 78 investigaciones potencialmente relevantes, a fin de identificar su relación con el ámbito específico del estudio (análisis de vulnerabilidades en infraestructuras de red), y la contestación de al menos a una de las cuatro preguntas de investigación. De su lectura completa se descartaron 62 artículos, de los cuales 60 presentaban un enfoque hacia las vulnerabilidades en aplicaciones (software y aplicaciones web). Finalmente, 16 fueron considerados para su análisis: 12 son estudios primarios y 4 estudios secundarios.

Calidad de los estudios

Con base en el rigor académico y los estrictos criterios de publicación manejados por SCOPUS, IEEE y Redalyc, no se evaluó la calidad de los estudios primarios y secundarios seleccionados.

Síntesis de los datos

A lo largo de la fase de ejecución se emplearon instrumentos que aportarían al proceso de síntesis de datos de los estudios seleccionados. Se utilizó Zotero para la organización bibliográfica de los artículos, así como una hoja de cálculo de MS Excel para la descripción de cada estudio mediante el **año, autor, título del artículo, resumen,** URL y respuestas a las cuatro preguntas de investigación. La información de la matriz se fue complementando en cada actividad del proceso de selección, garantizando un tratamiento consistente y verificable de toda la información.

Resultados

Esta sección se describen los resultados del proceso de RSL, en relación a cada pregunta de investigación. En la Tabla 1 se resumen los datos principales de los artículos seleccionados.

Ver tabla 1.

Se han identificado artículos de valor para la RSL en cada una de las bases de datos elegidas, los cuales han sido principalmente publicados en los años 2018 y 2023. Se tratan mayormente de estudio primarios publicados como artículos de revistas académicas. A continuación, se describen, sintetizan y analizan las respuestas a cada una de las preguntas de investigación:

P1: ¿Qué métodos han sido utilizados en el análisis de vulnerabilidades en infraestructuras de red, en los últimos 10 años?

Tabla 2
Detalle de resultados por artículo – pregunta de investigación 1

ID Artículo	Pregunta 1
E1	-
E2	Análisis de árbol de ataque (Grafos de Ataque Bayesiano - BAG)
E3	Análisis de tráfico Análisis de protocolos
E4	Análisis de árbol de ataque
E5	Marco metodológico para evaluaciones de seguridad asistidas por inteligencia artificial (propuesta)
E6	-
E7	Análisis de tráfico Análisis de protocolos
E8	-
E9	-
E10	Método Dinámico de Hexágonos Difusos (propuesta)
E11	-
E12	-
E13	Análisis de tráfico
E14	-
E15	Análisis y explotación de vulnerabilidades
E16	Análisis y explotación de vulnerabilidades

Digital Publisher CEIT ISSN 2588-0705

Tabla 1

Artículos seleccionados mediante la RSL

ID	BD	Autor/Año	Título	Tipo
E1	IEEE SCOPUS	(Zolanvari et al., 2019)these techniques can help improve the security of the IIoT systems as well. In this paper, we first present common IIoT protocols and their associated vulnerabilities. Then, we run a cyber-vulnerability assessment and discuss the utilization of ML in countering these susceptibilities. Following that, a literature review of the available intrusion detection solutions using ML models is presented. Finally, we discuss our case study, which includes details of a real-world testbed that we have built to conduct cyber-attacks and to design an intrusion detection system (IDS	Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things	SEC AREV
E2	IEEE SCOPUS	(Kim et al., 2023)	Time-Based Moving Target Defense Using Bayesian Attack Graph Analysis	PRI AREV
E3	IEEE	(Alarood et al., 2023)	Attacks Notification of Differentiated Services Code Point (DSCP) Values Modifications	PRI AREV
E4	IEEE SCOPUS	(Alhaidary et al., 2018)	Vulnerability Analysis for the Authentication Protocols in Trusted Computing Platforms and a Proposed Enhancement of the OffPAD Protocol	SEC AREV
E5	SCOPUS	(Nebbione & Calzarossa, 2023)misconfigurations and operational weaknesses. In this scenario, a timely assessment and mitigation of the security risks affecting technological environments are of paramount importance. To cope with these compelling issues, we propose an AI-assisted methodological framework aimed at evaluating whether the target environment is vulnerable or safe. The framework is based on the combined application of graph-based and machine learning techniques. More precisely, the components of the target together with their vulnerabilities are represented by graphs whose analysis identifies the attack paths associated with potential security threats. Machine learning techniques classify these paths and provide the security assessment of the target. The experimental evaluation of the proposed framework was performed on 220 artificially generated Active Directory environments, half of which injected with vulnerabilities. The results of the classification process were generally good. For example, the F1-score obtained by the Random Forest classifier for the assessment of vulnerable networks was equal to 0.91. These results suggest that our approach could be applied for automating the security assessment procedures of complex networked environments. © 2013 IEEE.","archive":"Scopus","container-title":"IEEE Access","DOI":"10.1109/ACCESS.2023.3244490","ISSN":"21693536 (ISSN	A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments	PRI AREV
E6	SCOPUS	(Zhang et al., 2023)as the communication rules among computer network devices, are the foundation for the normal operation of networks. However, security issues arising from design flaws and implementation vulnerabilities in network protocols pose significant risks to network operations and security. Network protocol fuzzing is an effective technique for discovering and mitigating security flaws in network protocols. It offers unparalleled advantages compared to other security analysis techniques thanks to the minimal requirement for prior knowledge of the target and low deployment complexity. Nevertheless, the randomness in test case generation, uncontrollable test coverage, and unstable testing efficiency introduce challenges in ensuring the controllability of the testing process and results. In order to comprehensively survey the development of network protocol fuzzing techniques and analyze their advantages and existing issues, in this paper, we categorized and summarized the protocol fuzzing and its related techniques based on the generation methods of test cases and testing conditions. Specifically, we overviewed the development trajectory and patterns of these techniques over the past two decades according to chronological order. Based on this analysis, we further predict the future directions of fuzzing techniques. © 2023 by the authors.","archive":"Scopus","container-title":"Electronics (Switzerland	A Survey on the Development of Network Protocol Fuzzing Techniques	SEC AREV
E7	SCOPUS	(Milani & Chatzigiannakis, 2021)developed by the LoRa (Long Range	Design, analysis, and experimental evaluation of a new secure rejoin mechanism for lorawan using elliptic-curve cryptography	PRI AREV
E8	SCOPUS	(Shastry et al., 2017)contemporary fuzzers fall short of thoroughly testing applications with a high degree of control-flow diversity, such as firewalls and network packet analyzers. In this paper, we demonstrate how static program analysis can guide fuzzing by augmenting existing program models maintained by the fuzzer. Based on the insight that code patterns reflect the data format of inputs processed by a program, we automatically construct an input dictionary by statically analyzing program control and data flow. Our analysis is performed before fuzzing commences, and the input dictionary is supplied to an off-the-shelf fuzzer to influence input generation. Evaluations show that our technique not only increases test coverage by 10–15% over baseline fuzzers such as afl but also reduces the time required to expose vulnerabilities by up, to an order of magnitude. As a case study, we have evaluated our approach on two classes of network applications: nDPI, a deep packet inspection library, and tcpdump, a network packet analyzer. Using our approach, we have uncovered 15 zero-day vulnerabilities in the evaluated software that were not found by stand-alone fuzzers. Our work not only provides a practical method to conduct security evaluations more effectively but also demonstrates that the synergy between program analysis and testing can be exploited for a better outcome. © 2017, Springer International Publishing AG.","archive":"Scopus","container-title":"Lect. Notes Comput. Sci.","DOI":"10.1007/978-3-319-66332-6_2","event-title":"Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics	Static Program Analysis as a Fuzzing Aid	PRI ACON

ID	BD	Autor/Año	Título	Tipo
E9	SCOPUS	(Luo et al., 2018)one fatal drawback of existing fuzzing methods is that a huge number of test files are required to maintain a high test coverage. In this paper, a novel method based on protocol reverse engineering is proposed to reduce the amount of test files for fuzzing. The proposed method uses techniques in the field of protocol reverse engineering to identify message formats of IoT application-layer protocol and create test files by generating messages with error fields according to message formats. The protocol message treated as a sequence of bytes is assumed to obey a statistic process with change-points indicating the boundaries of message fields. Then, a multi-change-point detection procedure is introduced to identify change-points of byte sequences according to their statistic properties and divide them into segments according to their change-points. The message segments are further processed via a position-based occurrence probability test analysis to identify keyword fields, data fields and uncertain fields. Finally, a message generation procedure with mutation operation on message fields is applied to construct test files for fuzzing test. The results show that the proposed method can effectively find out the message fields and significantly reduce the amount of test files for fuzzing test. © 2018 by the authors.","archive":" Scopus","container-title":"Symmetry","DOI":"10.3390/sym10110561","ISSN":"20738994 (ISSN	IoT application-layer protocol vulnerability detection using reverse engineering	PRI AREV
E10	SCOPUS	(Kholidy, 2022)5G networks are expected to become the backbone of many critical IT applications. With 5G, new tech advancements and innovation are expected; 5G currently operates on software-defined networking. This enables 5G to implement network slicing to meet the unique requirements of every application. As a result, 5G is more flexible and scalable than 4G LTE and previous generations. To avoid the growing risks of hacking, 5G cybersecurity needs some significant improvements. Some security concerns involve the network itself, while others focus on the devices connected to 5G. Both aspects present a risk to consumers, governments, and businesses alike. There is currently no real-time vulnerability assessment framework that specifically addresses 5G Edge networks, with regard to their real-time scalability and dynamic nature. This paper studies the vulnerability assessment in the 5G networks and develops an optimized dynamic method that integrates the Technique for Order of Preference by Similarity to Ideal Solution (TOP- SIS	Multi-layer attack graph analysis in the 5g edge network using a dynamic hexagonal fuzzy method	PRI AREV
E11	SCOPUS	(Alabady et al., 2020)	A Novel Security Model for Cooperative Virtual Networks in the IoT Era	PRI AREV
E12	SCOPUS	(Kumar et al., 2019)	Fixing network security vulnerabilities in local area network	PRI ACON
E13	Redalyc	(Gábor & Sándor, 2014)	Improving the Performance and Security of the TOTD DNS64 Implementation	PRI AREV
E14	Redalyc	(Álvarez et al., 2021)	Risks and security solutions existing in the Internet of things (IoT) in relation to Big Data	SEC AREV
E15	Redalyc	(Astudillo et al., 2018)es más alta aun cuando se vincula a plataformas financieras donde existe información sensible. Este artículo resume las técnicas utilizadas en el pentesting realizado al software ERP desarrollado en APEX 5 por la Universidad del Azuay; para ello se han contemplado seis etapas que sugieren una prueba de penetración: i	Acometer contra un ERP con Software Libre	PRI AREV
E16	Redalyc	(Cueva & Alvarado, 2017)	Análisis de Certificados SSL/ TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación.	PRI AREV

Nota. ID: identificador, BD: base de datos, PRI: primaria, SEC: secundaria, AREV: artículo de revista académica, ACON: artículo de conferencia

Digital Publisher CEIT ISSN 2588-0705

En términos generales, los artículos seleccionados emplearon los términos método y técnica de manera indistinta dentro de su contenido. Sin embargo, tras un análisis exhaustivo, se ha identificado que los métodos empleados durante la última década para el análisis de vulnerabilidades en infraestructuras de red, fueron: el análisis de tr**áfico** (E3, E7, E13), el análisis de protocolos (E3, E7), el análisis de árbol de ataque (E2, E4), y el análisis y explotación de vulnerabilidades (E15, E16). Adicionalmente, existen dos propuestas de autor: una metodología para evaluaciones de seguridad asistidas por inteligencia artificial (E5), y un método dinámico de hexágonos difusos (E10).

El análisis de tráfico permite detectar patrones o actividades inusuales en tiempo real, el análisis de protocolos puede revelar debilidades específicas en torno a las reglas de comunicación, y el análisis de árbol de ataque proporciona una visión holística de las posibles secuencias de eventos adversos. El uso combinado del análisis de tráfico, de protocolos, y del árbol de ataque facilitaría, por lo tanto, un enfoque integral que aborda diversas facetas de la seguridad de la red. Son lo suficientemente flexibles para adaptarse a los cambios en la infraestructura de red y a las nuevas amenazas que puedan surgir a futuro, lo que es esencial en un entorno cibernético en constante evolución. Además, permiten adoptar un enfoque proactivo para la gestión de vulnerabilidades, mediante la identificación de posibles riesgos antes de que se conviertan en problemas reales.

Mediante el análisis y explotación de vulnerabilidades se identifican debilidades y se simulan ataques para evaluar el impacto real en la infraestructura de red. Esto permite entender cómo podrían ser explotadas las vulnerabilidades, lo cual facilita a su vez el desarrollo contramedidas específicas y robustas. Herramientas como Metasploit y técnicas de fuzzing han automatizado y mejorado estos procesos (Kubecka, 2020, p.92).

El método dinámico de hexágonos difusos emplea la teoría de conjuntos difusos para manejar la incertidumbre y la imprecisión en la información de seguridad. A través de la construcción de hexágonos difusos, se pueden modelar diversas métricas de seguridad de manera dinámica, permitiendo una evaluación más flexible y adaptativa a los cambios en el entorno de red. A nivel experimental, se destaca la inclusión de la inteligencia artificial (IA) dentro de marcos propositivos para la evaluación de seguridad asistida por IA, lo cual responde a la evolución tecnológica actual.

P2: ¿Qué técnicas han sido utilizadas en el análisis de vulnerabilidades en infraestructuras de red, en los últimos 10 años?

Tabla 3

Detalle de resultados por artículo – pregunta de investigación 2

ID Artículo	Pregunta 2
E1	-
E2	-
E3	-
E4	-
E5	Técnicas basadas en grafos Técnicas de aprendizaje automático
E6	Fuzzing de protocolos de red
E7	-
E8	Fuzzing de protocolos de red
E9	Fuzzing de protocolos de red Ingeniería inversa de protocolos
E10	Número difuso hexagonal (Hexagonal fuzzy number) Orden de Preferencia por Similitud a la Solución Ideal (TOPSIS)
E11	Utilización de escáner de vulnerabilidades (Nessus)
E12	Utilización de distribución de Linux especializada en seguridad informática y pruebas de penetración (Kali Linux v2.0) Utilización de escáner de vulnerabilidades (FNSV - Desarrollada) Utilización de herramientas para pruebas de penetración y auditoría de seguridad (NMAP Nbtscan)
E13	Utilización de herramientas para capturar y analizar el tráfico de red (tshark).
E14	-
E15	Utilización de herramientas para pruebas de penetración y auditoría de seguridad (NMAP y Sparta)
E16	Utilización de distribución de Linux especializada en seguridad informática y pruebas de penetración (Kali Linux v2.0)

Las técnicas empleadas para el análisis de vulnerabilidades en infraestructuras de red en los últimos 10 años fueron: las técnicas basadas en grafos (E5), las técnicas de aprendizaje

automático (E5), el fuzzing de protocolos de red (E6, E8, E9), la ingeniería inversa de protocolos (E9), el uso del número difuso hexagonal o hexagonal fuzzy number (E10), y la Orden de Preferencia por Similitud a la Solución Ideal – TOPSIS (E10). En cuanto al uso de aplicativos o herramientas, se emplearon técnicas basadas en la utilización de escáneres de vulnerabilidades (E11, E12), distribuciones de Linux especializadas en seguridad informática y pruebas de penetración (E12, E16), herramientas para capturar y analizar el tráfico de red (E13), y herramientas para pruebas de penetración y auditoría de seguridad (E12, E15).

En el ámbito de protocolos de red se identificó el empleo de las técnicas de fuzzing e ingeniería inversa. El fuzzing de protocolos de red implica enviar datos de entrada aleatorios o manipulados para identificar vulnerabilidades. Esta técnica es efectiva para descubrir fallos y debilidades en la implementación de protocolos, al exponer posibles puntos débiles que podrían ser explotados por atacantes. La ingeniería inversa de protocolos permite alcanzar una comprensión profunda de los mismos, identificando posibles fallos en la implementación y debilidades en el diseño que podrían ser explotadas. Ambas técnicas pueden complementarse para mejorar los resultados.

Se observaron también técnicas relacionadas con procesos de representación y priorización. Las técnicas basadas en grafos son eficaces para visualizar y representar las relaciones entre los componentes de una red, analizar las interacciones entre nodos, identificar posibles rutas de ataque, dependencias y conexiones críticas, y comprender las vulnerabilidades que pueden surgir de la configuración y la conexión de los componentes de la red. El número difuso hexagonal permite representar y manejar la incertidumbre en los datos de ciberseguridad, al aplicarse en el modelado de riesgos y la evaluación de amenazas. En cuanto a la priorización, la técnica TOPSIS facilita la toma de decisiones basadas en datos, al considerar múltiples factores y criterios en el proceso de selección y priorización de medidas de seguridad.

Las técnicas de aprendizaje automático, como subdisciplina de la inteligencia artificial, se relacionan con procesos de predicción de vulnerabilidades, análisis de tráfico y detección de anomalías. Mediante el an**álisis de** datos históricos y patrones de ataques anteriores, el aprendizaje automático puede prever posibles vulnerabilidades emergentes y ayudar en la priorización de parches y medidas de seguridad. También puede analizar patrones de tráfico de red para identificar comportamientos sospechosos. Puede emplearse para modelar el comportamiento normal de la red para identificar cualquier desviación significativa o anomalía.

El empleo de técnicas basadas en herramientas es fundamental para un análisis exhaustivo y efectivo de las vulnerabilidades en infraestructuras de red, permitiendo a los profesionales de seguridad identificar, evaluar y mitigar riesgos de manera proactiva. A más de Nessus, Nmap, Nbtscan, Tshark, ampliamente utilizadas en la gestión de redes, destaca el uso de Kali Linux v2.0 y el desarrollo de una herramienta complementaria programada en Python denominada FNSV (Fixing Network Security Vulnerability), la cual escanea y reporta varias vulnerabilidades en una red, incluyendo seguridad de puertos, escaneo de sitios web y detección de parches faltantes. El uso combinado de las capacidades de las herramientas mencionadas juego un papel importante en la evaluación exhaustiva de la seguridad de la red.

P3: ¿Qué vulnerabilidades han sido analizadas en infraestructuras de red, en los últimos 10 años?

Digital Publisher CEIT ISSN 2588-0705

Tabla 4

Detalle de resultados por artículo – pregunta de investigación 3

ID Artículo	Pregunta 3
E1	Vulnerabilidades en protocolos de sistemas SCADA (Falta de confidencialidad y autenticación, falta de integridad de los datos, falta de cifrado)
E2	Vulnerabilidades de Windows 10 y Ubuntu (CVSS)
E3	Vulnerabilidad del protocolo IP (alteración de valores DSCP - clasificación y priorización del tráfico de red)
E4	Vulnerabilidades de protocolos de autenticación de uno y múltiples factores (configuración de seguridad en RFC 2617) Vulnerabilidades del protocolo HTTP DAA con OffPAD (autenticación vulnerable a ataques, específicamente ataques de repetición y de intermediario)
E5	-
E6	-
E7	Vulnerabilidades en protocolo LoRaWAN (susceptibilidad de la red a interferencia interferencia de radiofrecuencia RF jamming)
E8	Vulnerabilidades de día cero (10 vulnerabilidades de día cero en tcpdump y 5 vulnerabilidades de día cero en nDPI)
E9	-
E10	Vulnerabilidades en el Kernel de Linux (CVE2002-0392)
E11	Vulnerabilidades del Protocolo de Árbol de Expansión – STP (falta de autenticación y verificación en el proceso de selección del puente raíz en la red)
E12	Vulnerabilidades de Gestión y Configuración de Red (parches faltantes y exploits en servidor, puertos abiertos - lógicos y físicos-)
E13	Vulnerabilidad de cache poisoning
E14	Vulnerabilidades de Suplantación de Identidad, Interceptación y Manipulación de Tráfico (falta de cifrado en el transporte, falsificación de perfiles, manipulación de la red)
E15	Vulnerabilidades de Gestión y Configuración de Red (errores del administrador, errores de configuración, puertos abiertos, certificados digitales incoherentes)
E16	Vulnerabilidades de Suplantación de identidad, Interceptación y Manipulación de Tráfico (lectura de paquetes enviados por el cliente y servidor, suplantación de servidor o cliente, alteración de paquetes)

Las vulnerabilidades analizadas en infraestructuras de red, en los últimos 10 años, fueron: las vulnerabilidades en protocolos de sistemas SCADA (E1), las vulnerabilidades de los sistemas operativos Windows 10 y Ubuntu (E2), la vulnerabilidad del protocolo IP por alteración de valores DSCP (Differentiated Services Code Point) (E3), las vulnerabilidades de protocolos de autenticación de uno y múltiples factores (E4), las vulnerabilidades del protocolo HTTP DAA (Digest Access Authentication) con OffPAD (E4), las vulnerabilidades en protocolo LoRaWAN (E7), las vulnerabilidades de día cero en herramientas de administración y monitoreo de redes (E8), las vulnerabilidades en el Kernel de Linux CVE2002-0392 (E10), las vulnerabilidades del protocolo STP (Spanning-Tree Protocolo) (E11), las vulnerabilidades de gestión y configuración de red (E12, E15), las vulnerabilidad de cache poisoning (E13), y las vulnerabilidades de suplantación de identidad, interceptación y manipulación de tráfico (E14,E16).

Los sistemas de control y adquisición de datos (SCADA) son esenciales para operaciones críticas a nivel industrial. Estos sistemas, diseñados para monitorear y controlar procesos físicos y operaciones industriales, están intrínsecamente interconectados con otras redes y a menudo se conectan a Internet para permitir la supervisión remota y el acceso a los datos en tiempo real. Sin embargo, su complejidad inherente y su conexión a redes externas también los hace vulnerables a una variedad de amenazas cibernéticas. La falta de medidas de seguridad adecuadas puede exponer a estos sistemas a riesgos como la intrusión, la manipulación de datos, el acceso no autorizado y el sabotaje. Además, debido a la naturaleza crítica de muchas de sus operaciones, cualquier vulnerabilidad o brecha de seguridad podría tener consecuencias graves, incluyendo daños materiales, interrupciones en la producción, riesgos para la seguridad de los trabajadores y riesgos para el medio ambiente.

Las vulnerabilidades en los protocolos HTTP, IP, LoRaWAN y STP destacan la importancia de la integridad y seguridad de la comunicación en las redes. El análisis de vulnerabilidades en los protocolos de autenticación de uno y múltiples factores, revela la constante lucha por mejorar la seguridad en el acceso a sistemas y redes, pues la autenticación débil o mal implementada puede ser explotada por atacantes para comprometer la seguridad.

Dado que Windows 10 y Ubuntu son sistemas operativos ampliamente utilizados en entornos empresariales y de consumidores, se convierten en objetivos

atractivos para los atacantes. La popularidad de estos sistemas operativos los convierte en objetivos primarios para la investigación y explotación de vulnerabilidades. La presencia de vulnerabilidades en el Kernel de Linux desde hace más de una década, destaca la necesidad continua de evaluar y abordar cuestiones históricas en la seguridad. Los sistemas heredados o mal mantenidos pueden representar riesgos significativos.

La vulnerabilidad de cache poisoning (envenenamiento de caché) representa una amenaza significativa para la integridad del sistema de nombres de dominio (DNS), permitiendo a los atacantes corromper la información almacenada en la caché de los servidores DNS. Esto puede resultar en la redirección de tráfico legítimo a destinos maliciosos, lo que potencialmente expone a los usuarios a ataques de phishing y otras formas de explotación.

Las vulnerabilidades de gestión y configuración de red reflejan graves errores en la administración de los dispositivos de red. Desde contraseñas débiles hasta políticas de seguridad inadecuadas, estas debilidades dejan expuesta a la infraestructura de red a riesgos como el acceso no autorizado, el robo de datos y la interrupción del servicio. Las vulnerabilidades de suplantación de identidad, interceptación y manipulación de tráfico, por su parte, pueden permitir a los adversarios interceptar y alterar comunicaciones sensibles, comprometiendo la confidencialidad y la integridad de los datos transmitidos a través de la red.

Las herramientas de administración y monitoreo son esenciales para mantener la salud y el rendimiento de las redes. Sin embargo, su propia complejidad y la constante evolución de las amenazas pueden dar lugar a vulnerabilidades de día cero que aún no han sido abordadas por los desarrolladores. Al ser defectos de seguridad en software, hardware o protocolos que son desconocidos para el desarrollador o el proveedor del producto, no existe parche o actualización para corregirlas antes de que se exploten, lo cual resalta la importancia de implementar estrategias proactivas de detección y respuesta.

P4: ¿Qué componentes de la infraestructura de red han sido analizados en sus vulnerabilidades, en los últimos 10 años?

Tabla 5

Detalle de resultados por artículo – pregunta de investigación 4

ID Pregunta	Pregunta 4
E1	Protocolos de red
E2	Sistemas Operativos
E3	Protocolos de red
E4	Protocolos de red
E5	Sistemas Operativos
E6	Protocolos de red
E7	Protocolos de red
E8	Protocolos de red Herramientas de administración y monitoreo de redes
E9	Protocolos de red
E10	Sistemas Operativos
E11	Protocolos de red
E12	Servidores Sistemas Operativos
E13	Servidores (DNS)
E14	Firewalls Herramientas de administración y monitoreo de redes
E15	Protocolos de red Servidores (Web)
E16	Servidores (Web)

Los componentes de la infraestructura de red analizados en sus vulnerabilidades durante la última década fueron: los sistemas operativos (E2, E5, E10, E12), herramientas de administración y monitoreo de redes (E8, E14), protocolos de red (E1, E3, E4, E6 – E9, E11, E15), servidores (E12, E13, E15, E16) y firewalls (E14), siento predominante el análisis del componente de servicio.

Tal como se ha plasmado en las preguntas previas, existe un predominio de los estudios revisados sobre el análisis de vulnerabilidades en protocolos de red, debido a la importancia crítica de los protocolos de red para el funcionamiento y la seguridad de la infraestructura de red en su conjunto. Los protocolos de red actúan como la base para la comunicación y el intercambio de datos en la red, lo que los convierte en un

Digital Publisher CEIT ISSN 2588-0705

objetivo principal para los atacantes en busca de vulnerabilidades que puedan explotar para acceder, manipular o interrumpir el tráfico de red.

Discusión

Durante la ejecución de la RSL se observó una clara tendencia de los investigadores por el análisis de vulnerabilidades de aplicaciones. Se evidenci**ó además** que el análisis de vulnerabilidades en infraestructuras de red es un ámbito de investigación que posee escasa documentación científica publicada en los últimos 10 años. Un importante número de investigaciones refiere el término "vulnerabilidades" en su **título** o resumen, sin embargo, su contenido se orienta al análisis descriptivo o experimental de ataques de red.

Una mayor investigación en cuanto a vulnerabilidades de software y ataques de red puede atribuirse en parte a la importancia crítica de estos aspectos en la seguridad de la información. El software es la base de la mayoría de los sistemas y servicios digitales, y las vulnerabilidades en el software pueden tener consecuencias graves, desde la exposición de datos sensibles hasta el compromiso de sistemas críticos de infraestructura. Del mismo modo, los ataques de red representan una preocupación fundamental debido a su capacidad para comprometer la integridad y disponibilidad de los datos, así como para interrumpir las operaciones comerciales normales.

Los resultados obtenidos en la RSL indican que, en la última década, los protocolos de red han sido el componente de la infraestructura más analizado en cuanto a vulnerabilidades. En consecuencia, los métodos y técnicas más utilizados han sido el análisis de tráfico y el fuzzing de protocolos de red, respectivamente. Esto se debe a la función crítica que desempeñan los protocolos de red en la comunicación y operación de sistemas informáticos. Los protocolos de red, como TCP/IP, HTTP, DNS y otros, son fundamentales para el intercambio de datos y la conectividad en las redes. Sin embargo, su omnipresencia y complejidad los convierten en objetivos atractivos para los atacantes. Además, la transformación de aplicaciones locales en servicios de red ha resaltado la importancia de realizar pruebas de seguridad en los protocolos de comunicación utilizados entre los clientes y servidores (Li et al., 2018).

Los protocolos de red, en el ámbito industrial, han sido desarrollados en torno a requisitos de rendimiento, más que de seguridad (Akpinar & Ozcelik, 2019). Históricamente, estos ambientes permanecían aislados de la red global de internet, siendo menos susceptibles a ataques. Hoy en día, el avance tecnológico de las redes industriales y su inherente conectividad a internet promueven la aplicación de un enfoque integral de ciberseguridad que incluya el análisis de los distintos componentes de la infraestructura de red, a más del análisis de vulnerabilidades de software o aplicaciones.

Mientras que se han realizado avances significativos en la identificación y mitigación de vulnerabilidades en protocolos de red, sistemas operativos y herramientas de administración, aún quedan áreas pendientes que requieren atención. Una de las áreas pendientes en el análisis de vulnerabilidades es la evaluación de riesgos emergentes asociados con tecnologías disruptivas como el Internet de las cosas (IoT), la inteligencia artificial (IA) y la computación en la nube. Estas tecnologías introducen nuevos vectores de ataque y desafíos de seguridad que requieren enfoques innovadores para su detección y mitigación (Jacklin, 2024). Además, la rápida evolución de las amenazas cibernéticas y las tácticas de los adversarios plantea desafíos constantes para los investigadores y profesionales de seguridad, que deben mantenerse al día con las últimas tendencias, **técnicas de ataque**, así como los métodos y técnicas para identificar y mitigar vulnerabilidades.

Conclusiones

El análisis de vulnerabilidades en la infraestructura de red ha sido un área de investigación relativamente poco documentada en la última década, a pesar de su importancia crítica para la seguridad de la información. La

RSL realizada evidenció que los investigadores han mostrado una mayor inclinación hacia el análisis de vulnerabilidades en aplicaciones y los ataques de red. En cuanto a sus resultados, los protocolos de red han sido el componente de infraestructura más analizado en cuanto a vulnerabilidades en la última década, mientras que los métodos y técnicas predominantes han sido el análisis de tráfico y el fuzzing de protocolos de red. Si bien se ha progresado en el análisis y mitigación de vulnerabilidades en componentes críticos de la infraestructura de red, es imperativo que la investigación continúe expandiéndose hacia áreas emergentes.

Referencias bibliográficas

Akpinar, K. O., & Ozcelik, I. (2019). Analysis of Machine Learning Methods in EtherCAT-Based Anomaly Detection. *IEEE Access*, *7*, 184365-184374. Scopus. https://doi.org/10.1109/ACCESS.2019.2960497

Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A Novel Security Model for Cooperative Virtual Networks in the IoT Era. *International Journal of Parallel Programming*, *48*(2), 280-295. Scopus. https://doi.org/10.1007/s10766-018-0580-z

Alarood, A., Ibrahim, A., & Alsubaei, F. (2023). Attacks Notification of Differentiated Services Code Point (DSCP) Values Modifications. *IEEE Access*, *11*, 126950-126966. https://doi.org/10.1109/ACCESS.2023.3332119

Alhaidary, M., Rahman, S. M. M., Zakariah, M., Shamim Hossain, M., Alamri, A., Haque, M. S. M., & Gupta, B. B. (2018). Vulnerability Analysis for the Authentication Protocols in Trusted Computing Platforms and a Proposed Enhancement of the OffPAD Protocol. *IEEE Access*, *6*, 6071-6081. Scopus. https://doi.org/10.1109/ACCESS.2017.2789301

Álvarez, Y., Leguizamón, M., & Londoño, T. (2021). Risks and security solutions existing in the Internet of things (IoT) in relation to Big Data. *Ingeniería y Competitividad*, *23*, 1-13.

Astudillo, C., Carvajal, F., Carvallo, J., Crespo, E., Orellana, M., & Vintimilla, R. (2018). Acometer contra un ERP con Software Libre. *Enfoque UTE*, *9*, 138-148.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571-583. https://doi.org/10.1016/j.jss.2006.07.009

CISCO. (2023). *What Is Network Infrastructure?* Cisco. https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-infrastructure.html

Codina, L. (2019, octubre 30). *Scopus: Caracterización y guía de uso avanzado · Preparación, búsqueda y exportación de resultados*. Lluís Codina. https://www.lluiscodina.com/scopus-analisis-guia-utilizacion/

Cueva, M., & Alvarado, D. (2017). Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación. *Enfoque UTE*, *8*, 273-286.

Deola, E. (2023, febrero 4). Ataque Wanna Cry: La importancia de disponer de sistemas de seguridad actualizados. *FlashStart*. https://flashstart.com/es/el-ataque-wannacry-de-2017/

Fortra. (2022). *Qué es el escaneo de vulnerabilidades y cómo funciona | Fortra Blog*. https://www.fortra.com/es/blog/escaneo-vulnerabilidades

Gábor, L., & Sándor, R. (2014). Improving the Performance and Security of the TOTD DNS64 Implementation. *Journal of Computer Science and Technology*, *14*, 9-15.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/downloads/cas/E3G5JMBP

Ierardi, C., Orihuela, D. L., Jurado, I., Rodríguez, Á., & Tapia, A. (2017). Revisión sistemática de la literatura en ingeniería de sistemas. Caso práctico: Técnicas de estimación distribuida

Digital Publisher CEIT ISSN 2588-0705

de sistemas ciberfísicos. *Actas de las XXXVIII Jornadas de Automática, 2017, ISBN 978-84-16664-74-0, págs. 84-91*, 84-91. https://dialnet.unirioja.es/servlet/articulo?codigo=6591559

Jacklin, B. (2024, febrero 21). *AI Technology is Invaluable for Cybersecurity*. Https://Www.Smartdatacollective.Com/. https://www.smartdatacollective.com/ai-technology-is-invaluable-for-cybersecurity/

Kholidy, H. (2022). Multi-layer attack graph analysis in the 5g edge network using a dynamic hexagonal fuzzy method. *Sensors*, *22*(1). Scopus. https://doi.org/10.3390/s22010009

Kim, H., Hwang, E., Kim, D., Cho, J., Moore, T. J., Nelson, F. F., & Lim, H. (2023). Time-Based Moving Target Defense Using Bayesian Attack Graph Analysis. *IEEE Access*, 1-1. Scopus. https://doi.org/10.1109/ACCESS.2023.3269018

Kubecka, M. (2020). *Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects* (Packt Publishing).

Kumar, B. K., Raj, N., Dhivvya, J., & Muralidharan, D. (2019). Fixing Network Security Vulnerabilities in Local Area Network. *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 1349-1354. https://doi.org/10.1109/ICOEI.2019.8862634

Li, J., Zhao, B., & Zhang, C. (2018). Fuzzing: A survey. *Cybersecurity*, *1*(1), 6. https://doi.org/10.1186/s42400-018-0002-y

Limones, E. (2022, septiembre 23). *Análisis de vulnerabilidades informáticas* [Blog]. OpenWebinars.net. https://openwebinars.net/blog/analisis-de-vulnerabilidades-informaticas/

Luo, J., Shan, C., Cai, J., & Liu, Y. (2018). IoT application-layer protocol vulnerability detection using reverse engineering. *Symmetry*, *10*(11). Scopus. https://doi.org/10.3390/sym10110561

Marcillo, M. P., Marcillo, J. C., Ortiz, M. M., & Mero, E. A. (2021). Análisis de las Herramientas y Técnicas utilizadas en prueba de penetración para la detección de vulnerabilidades en aplicaciones web. *UNESUM - Ciencias. Revista Científica Multidisciplinaria*, *5*(1), Article 1. https://doi.org/10.47230/unesum-ciencias.v5.n3.2021.316

Milani, S., & Chatzigiannakis, I. (2021). Design, analysis, and experimental evaluation of a new secure rejoin mechanism for lorawan using elliptic-curve cryptography. *Journal of Sensor and Actuator Networks*, *10*(2). Scopus. https://doi.org/10.3390/JSAN10020036

Molina, Y., & Orozco, L. G. (2020). *Vulnerabilidades de los Sistemas de Información: Una revisión*. https://dspace.tdea.edu.co/handle/tdea/1398

Navarro, G. (2011). *Introducción a las vulnerabilidades*. Universitat Oberta de Catalunya.

Nebbione, G., & Calzarossa, M. (2023). A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments. *IEEE Access*, *11*, 15119-15130. Scopus. https://doi.org/10.1109/ACCESS.2023.3244490

Pando, F. (2023, junio 22). Haz un análisis de vulnerabilidades para tu empresa; cajas blanca y negra. *IT Masters Mag*. https://www.itmastersmag.com/noticias-analisis/analisis-de-vulnerabilidades-cual-es-su-importancia/

Pastorino, C. (2017). *Aclarando KRACK Attack, la vulnerabilidad descubierta en WPA2*. Welivesecurity. https://www.welivesecurity.com/la-es/2017/10/27/aclarando-krack-attack-wpa2/

Peng, Y. (2023). Research on the Technology of Computer Network Security Protection. *Journal of Applied Data Sciences*, *4*(1), Article 1. https://doi.org/10.47738/jads.v4i1.80

Ramírez, G. A. (2023). Seguridad en desarrollo web: Mejores prácticas para proteger aplicaciones y datos. *Dominio de las Ciencias*, *9*(3), Article 3. https://doi.org/10.23857/dc.v9i3.3552

Rouse, M. (2023, octubre 30). Network Infrastructure. *Techopedia*. https://www.

techopedia.com/definition/16955/network-infrastructure

Sánchez, F., Martínez, J. E., & Téllez, A. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *methaodos.revista de ciencias sociales*, *10*(2), Article 2. https://doi.org/10.17502/mrcs.v10i2.577

Shastry, B., Leutner, M., Fiebig, T., Thimmaraju, K., Yamaguchi, F., Rieck, K., Schmid, S., Seifert, J., & Feldmann, A. (2017). Static Program Analysis as a Fuzzing Aid. En M. Polychronakis, M. Antonakakis, M. Dacier, & M. Bailey (Eds.), *Lect. Notes Comput. Sci.: Vol. 10453 LNCS* (pp. 26-47). Springer Verlag; Scopus. https://doi.org/10.1007/978-3-319-66332-6_2

SolarWinds. (2023). *What Is Network Infrastructure? All About Network Infrastructure - IT Glossary*. https://www.solarwinds.com/resources/it-glossary/network-infrastructure

Zhang, Z., Zhang, H., Zhao, J., & Yin, Y. (2023). A Survey on the Development of Network Protocol Fuzzing Techniques. *Electronics (Switzerland)*, *12*(13). Scopus. https://doi.org/10.3390/electronics12132904

Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2019). Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), 6822-6834. Scopus. https://doi.org/10.1109/JIOT.2019.2912022