Análisis de vulnerabilidades en redes inalámbricas: métodos y soluciones

Eugenio Rafael Mora Zambrano [1]

[1] *Instituto Superior Universitario Japón, Quito, Ecuador. gmora@itsjapon.edu.ec.*
https://orcid.org/0000-0002-5654-8695

Resumen: El análisis de vulnerabilidades en redes inalámbricas presenta desafíos críticos para la seguridad, a pesar de ofrecer flexibilidad y movilidad. Métodos como el análisis de protocolos, pruebas de penetración, auditorías de seguridad y monitoreo continuo son esenciales para identificar posibles amenazas. Estas vulnerabilidades pueden incluir fallos en la seguridad del protocolo, configuraciones incorrectas y debilidades en dispositivos. Para mitigar estos riesgos, se recomienda implementar protocolos de seguridad robustos, actualizar regularmente el firmware y realizar configuraciones personalizadas. Además, la educación del usuario y el monitoreo en tiempo real son aspectos clave en la defensa contra ataques. En compendio, al emplear estrategias integrales de análisis y soluciones proactivas, las organizaciones pueden salvaguardar la integridad de sus datos y la seguridad de sus redes inalámbricas.

Palabras clave: Vulnerabilidades; redes inalámbricas; seguridad; métodos de identificación.

Wireless network vulnerability analysis: methods and solutions

Abstract: Wireless network vulnerability analysis presents critical security challenges, despite offering flexibility and mobility. Methods such as protocol analysis, penetration testing, security audits and continuous monitoring are essential to identify potential threats. These vulnerabilities can include protocol security failures, incorrect configurations, and device weaknesses. To mitigate these risks, it is recommended to implement robust security protocols, regularly update firmware, and make custom configurations. In addition, user education and real-time monitoring are key aspects in defense against attacks. In Compendium, by employing comprehensive analytics strategies and proactive solutions, organizations can safeguard the integrity of their data and the security of their wireless networks.

Keywords: Vulnerabilities; wireless networks; security; identification methods.

1. INTRODUCCIÓN

La evolución de las redes inalámbricas ha revolucionado la conectividad y la movilidad en la era digital actual [1]. Estas redes ofrecen una conectividad sin restricciones geográficas, lo que ha permitido un acceso instantáneo a la información en cualquier momento y lugar [2]. Sin embargo, esta conveniencia también ha introducido una serie de desafíos en términos de seguridad cibernética, lo que ha generado preocupaciones significativas en la comunidad investigadora y empresarial [3].

Debido a su naturaleza inalámbrica, las redes inalámbricas son inherentemente más vulnerables a una variedad de amenazas [4]. Los ciberdelincuentes aprovechan estas vulnerabilidades para comprometer la integridad y confidencialidad de la información transmitida a través de estas redes, lo que representa un riesgo para individuos, empresas e instituciones en todo el mundo [5]. Por ejemplo, la proliferación de redes Wi-Fi públicas ha aumentado el riesgo de ataques de hombre en el medio, donde los atacantes pueden interceptar comunicaciones sensibles entre usuarios y puntos de acceso [6].

En respuesta a estos desafíos, es fundamental abordar de manera efectiva las vulnerabilidades en las redes inalámbricas y proponer soluciones adecuadas [7]. El objetivo de este estudio es precisamente explorar métodos para identificar vulnerabilidades y proponer medidas efectivas para mitigar los riesgos asociados en estas redes [8]. Al comprender mejor los riesgos y adoptar un enfoque proactivo para abordarlos, las organizaciones pueden fortalecer su postura de seguridad cibernética y garantizar la protección adecuada de su infraestructura de red y los datos críticos que fluyen a través de ella [9].

Colocar el correo electrónico del primer autor

Recibido: *21 Junio 2024 /**Aceptado:** 12 de Julio 2024* ***ISSN Electrónico:*** 2697-3308

En las secciones siguientes, se profundizará en los métodos de identificación de vulnerabilidades y las soluciones disponibles para mejorar la seguridad de las redes inalámbricas en el entorno digital actual [10].

2. METODOLOGÍA

El análisis de vulnerabilidades en redes inalámbricas se basa en un enfoque multifacético que comprende diversas etapas esenciales [1]:

1. Análisis de Protocolos. -Se emplean herramientas como Nmap y Wireshark para realizar un escaneo exhaustivo de la red y detectar dispositivos conectados, así como identificar los protocolos de comunicación utilizados. Este análisis proporciona una visión detallada de la topología de la red, identificando posibles puntos de vulnerabilidad. Además, se pueden utilizar herramientas de análisis de paquetes como Tcpdump para examinar el tráfico de red y detectar posibles anomalías [11]:

Figura 1. Análisis de vulnerabilidades. (Usado, con permiso, de [1].)

La Figura 1 resume el proceso de análisis de vulnerabilidades en redes inalámbricas, destacando la importancia del análisis de protocolos.

2. Pruebas de Penetración. -Se llevan a cabo simulaciones de ataques para identificar puntos débiles y vulnerabilidades en la seguridad de la red. Estas pruebas implican intentos controlados de explotar fallos de seguridad y vulnerabilidades conocidas, evaluando así la resistencia de la red ante posibles ataques externos. Por ejemplo, se pueden realizar ataques de fuerza bruta a contraseñas para evaluar la solidez de las medidas de autenticación [12].
3. Auditorías de Seguridad. - Se realiza una evaluación exhaustiva de las configuraciones y políticas de seguridad implementadas en la red. Esto implica revisar la configuración de dispositivos inalámbricos, como enrutadores y puntos de acceso, para asegurar el cumplimiento de las mejores prácticas de seguridad y evitar configuraciones inseguras que puedan ser explotadas por ciberdelincuentes. Además, se pueden utilizar herramientas de escaneo de vulnerabilidades como Nessus para identificar posibles fallos de seguridad en los dispositivos de red [13].
4. Monitoreo Continuo. - Se implementan sistemas de detección de intrusiones (IDS) para monitorear la red en busca de actividades sospechosas en tiempo real. Además, se realiza un análisis regular de los registros de eventos para identificar patrones o actividades anómalas que puedan indicar una brecha de seguridad. Este monitoreo continuo es esencial para detectar y responder rápidamente a posibles amenazas cibernéticas. Por ejemplo, se pueden implementar IDS basados en firmas y en comportamiento para detectar y bloquear ataques conocidos y actividades anómalas en la red [14].

3. RESULTADOS Y DISCUSIÓN

Durante el análisis de vulnerabilidades en redes inalámbricas, se identificaron distintas deficiencias en la seguridad que plantean riesgos considerables para la integridad y confidencialidad de la información. Entre las principales vulnerabilidades identificadas se encuentran las siguientes:

1. Fallos en la Seguridad del Protocolo. - Se detectaron debilidades en los protocolos de cifrado, como WEP (Wired Equivalent Privacy) y WPA (Wi-Fi Protected Access), los cuales son susceptibles a ataques de fuerza bruta y descifrado de claves. Por ejemplo, se registraron instancias de ataques de reinyección de paquetes que comprometen la seguridad de las redes WEP [15].

Figura 2. Vulnerabilidades Identificadas. (Usado, con permiso, de [3].)

La Figura 2 proporciona una síntesis visual de las vulnerabilidades detectadas durante el proceso de análisis de seguridad en redes inalámbricas.

2. Configuraciones Incorrectas. - Se hallaron configuraciones inseguras, como la transmisión del SSID (Service Set Identifier) de manera broadcast, lo que facilita la identificación de la red, así como el uso de contraseñas débiles o predeterminadas, las cuales pueden ser fácilmente comprometidas por atacantes. Por ejemplo, se identificaron casos de redes con contraseñas por defecto que no fueron modificadas por los administradores [16].
3. Vulnerabilidades de Dispositivos. - Se observaron dispositivos con firmware desactualizado, lo que los

Recibido: *21 Junio 2024 /**Aceptado:** 12 de Julio 2024* ***ISSN Electrónico:*** 2697-3308

expone a ataques conocidos que han sido corregidos en versiones más recientes del firmware. Además, algunas configuraciones predeterminadas de fábrica dejaban puertas traseras abiertas para posibles intrusiones. Por ejemplo, se encontraron casos de routers con vulnerabilidades conocidas que no habían sido corregidas por los fabricantes.

4. Fallos en la Seguridad del Protocolo. - Se detectaron debilidades en protocolos de cifrado como WEP (Wired Equivalent Privacy) y WPA (Wi-Fi Protected Access), que son susceptibles a ataques de fuerza bruta y de descifrado de claves. Por ejemplo, se observaron casos de ataques de reinyección de paquetes para vulnerar la seguridad de redes WEP [15].
5. Configuraciones Incorrectas. - Se encontraron configuraciones inseguras, como la transmisión del SSID (Service Set Identifier) de forma broadcast, lo que facilita la identificación de la red, y el uso de contraseñas débiles o predeterminadas, que pueden ser fácilmente comprometidas por atacantes. Por ejemplo, se identificaron casos de redes con contraseñas por defecto que no habían sido cambiadas por los administradores [16].
6. Vulnerabilidades de Dispositivos. - Se observaron dispositivos con firmware desactualizado, lo que los hace vulnerables a ataques conocidos que han sido corregidos en versiones más recientes del firmware. Además, algunas configuraciones predeterminadas de fábrica dejaban puertas traseras abiertas para posibles intrusiones. Por ejemplo, se encontraron casos de routers con vulnerabilidades conocidas que no habían sido parcheadas por los fabricantes.

Para abordar las vulnerabilidades identificadas y fortalecer la seguridad de las redes inalámbricas, se proponen diversas soluciones, como se detalla en la Figura 3, basada en la fuente proporcionada [2]. En primer lugar, se recomienda la implementación de protocolos de cifrado más robustos, como WPA2 o WPA3, en lugar de WEP, con el fin de garantizar una mayor seguridad [17].

Figura 3. Soluciones Propuestas. (Usado, con permiso, de [2].)

Además, se sugiere desactivar la transmisión del SSID para dificultar su detección por parte de posibles atacantes. Es fundamental aplicar parches de seguridad y actualizaciones de firmware proporcionadas por los fabricantes de dispositivos para corregir vulnerabilidades conocidas y mejorar la resistencia frente a ataques [18]. Por ejemplo, se puede implementar un proceso automatizado de actualización de firmware para garantizar que los dispositivos estén siempre protegidos contra las últimas amenazas. Se insta también a implementar configuraciones de seguridad personalizadas, como el uso de contraseñas fuertes y únicas, así como políticas de seguridad adecuadas para restringir el acceso no autorizado a la red y proteger la integridad de los datos. Se puede considerar la implementación de un sistema de gestión de contraseñas para generar y almacenar contraseñas seguras de forma segura.

Asimismo, se pueden sugerir medidas adicionales como la implementación de sistemas de detección y prevención de intrusiones, la realización de auditorías de seguridad regulares y la capacitación del personal en mejores prácticas de seguridad cibernética [19].

4. CONCLUSIONES

El análisis exhaustivo de vulnerabilidades en redes inalámbricas emerge como una tarea crucial en la era digital, donde la seguridad de la información se convierte en un aspecto crítico para cualquier organización. Este estudio resalta la importancia vital de esta práctica y cómo la adopción de enfoques proactivos puede fortalecer la seguridad cibernética de una entidad.

Las redes inalámbricas, si bien proporcionan flexibilidad y conveniencia, también están expuestas a diversas amenazas cibernéticas que ponen en riesgo la integridad de los datos. Por ello, el análisis de vulnerabilidades se revela como una herramienta esencial para proteger la integridad de los datos y prevenir la exposición a posibles ataques maliciosos que podrían comprometer la información sensible.

En la implementación de soluciones efectivas, se destaca la importancia de adoptar medidas que mitiguen los riesgos identificados durante el análisis de vulnerabilidades. Esto incluye la adopción de protocolos de seguridad robustos, la actualización regular de firmware y software, así como la configuración personalizada de dispositivos y políticas de seguridad.

El compromiso con la seguridad cibernética continua se posiciona como un proceso dinámico y en constante evolución. Es crucial que las organizaciones mantengan un compromiso continuo con la seguridad, estando al tanto de las últimas tendencias y amenazas en el panorama cibernético. Esto implica no solo implementar medidas de seguridad, sino también realizar evaluaciones periódicas de riesgos y ajustar las estrategias de seguridad según sea necesario.

Además de las soluciones técnicas, la concienciación y la capacitación del personal emergen como aspectos

Recibido: *21 Junio 2024 /****Aceptado:*** *12 de Julio 2024* ***ISSN Electrónico:*** 2697-3308

fundamentales en la defensa contra ciberataques. Educar a los usuarios sobre las mejores prácticas de seguridad, como el uso de contraseñas seguras y la identificación de posibles amenazas, puede contribuir significativamente a fortalecer la postura de seguridad de una organización. Se recomienda ofrecer programas de capacitación en seguridad cibernética para empleados y usuarios finales, así como realizar campañas de concienciación sobre los riesgos asociados con el uso de redes inalámbricas.

5. REFERENCIAS BIBLIOGRÁFICAS

1. F. U. Los Libertadores, "Revista Ciber-Sistemas," Julio-diciembre de 2022, vol. 3, 2023.
2. O. T. Rodriguez, Aspectos jurídicos de la ciberseguridad. Madrid, España: Ra-Ma Editorial, 2020.
3. M. Chakra, "Desarrollo de una Técnica de Seudonimización de Datos Personales basada en criptografía," 2021.
4. C. A. Román Carrión, "El uso del celular y su influencia en las actividades académicas y familiares de los estudiantes de primer año de bachillerato de la Unidad Educativa Sagrados Corazones de Rumipamba de la ciudad de Quito," Master's thesis, Universidad Andina Simón Bolívar, Sede Ecuador, 2017.
5. P. Ramos, E. Jefferson, y D. F. Andaluz Espinosa, "Elaboración de un plan de contingencia para los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Pastocallle caso de estudio Junta administradora de agua 'Miño San Antonio'," 2023.
6. G. Toaza Moran, "Análisis de diferencias y mejoras entre ssl y tls en términos de seguridad y protección," Bachelor's thesis, Babahoyo: UTB-FAFI, 2023.
7. Dávila Angeles and B. J. Dextre Alarcón, "Propuesta de una implementación de un programa de gestión de vulnerabilidades de seguridad informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001: 2014 en la ciudad de Lima-2021," 2021.
8. L. L. Vargas Santana, "Análisis de vulnerabilidades críticas del sistema operativo móvil Android mediante Pentesting," Doctoral dissertation, PUCESE–Escuela de ingeniería en tecnologías de la información, 2023.
9. S. D. L. A. Núñez López, "Hacking ético para la detección de vulnerabilidades mediante la utilización de herramientas Open Source en la red inalámbrica de la Unidad Educativa Pelileo," Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Tecnologías de la Información, 2024.
10. E. M. Guevara Betanco, E. R. Hernández León, and G. M. López Pérez, "Evaluación del nivel de seguridad de la red informática de la Universidad de Ciencias Comerciales UCC-Campus León, para la identificación y mitigación de riesgos en un periodo comprendido de enero a junio 2023," Doctoral dissertation, Universidad de Ciencias Comerciales, 2023.
11. T. Lara and M. Johanna, "Análisis de la seguridad de la red del Ministerio de Inclusión Económica y Social mediante técnicas de hacking ético para identificar vulnerabilidades y amenazas," Bachelor's thesis, La Libertad: Universidad Estatal Península de Santa Elena, 2024.
12. P. A. Polanco Villarreal, "Capacidades técnicas, legales y de gestión para equipos blue team y red team," 2023.
13. O. D. Arango Gomez, "El ABC de la seguridad informática: guía práctica para entender la seguridad digital," 2023. [Online]. Available: https://www.autoreseditores.com/libro/22997/oscar-dario-arango-gomez/el-abc-de-la-seguridad-informatica-guia-practica-para-entender.html.
14. E. Leal Contreras, "Viabilidad Tecnológica y Económica para Implementar un Sistema de Detección de Intrusos en PYMES," 2003.
15. J. A. Cieza Celis and A. J. Ojeda Romero, "Evaluación del desempeño de protocolos de seguridad para combatir ataques en redes inalámbricas wi-fi," 2022.
16. J. Gomez, J. González, and C. Vicario, "Instituto Politécnico Nacional," 2016.
17. J. A. Cieza Celis and A. J. Ojeda Romero, "Evaluación del desempeño de protocolos de seguridad para combatir ataques en redes inalámbricas wi-fi," 2022.
18. S. Mulero Palencia, "Vulnerabilidades en edificios inteligentes," 2021.
19. J. Tiebas, "Carrera de Especialización en Seguridad Informática," 2017.

Recibido: *21 Junio 2024 /**Aceptado:** 12 de Julio 2024* ***ISSN Electrónico:*** 2697-3308