



UNIVERSIDAD DEL AZUAY
DEPARTAMENTO DE POSGRADOS
MAESTRÍA EN TELECOMUNICACIONES

**“Demostración y Análisis de Vulnerabilidades Existentes en
Redes Wi-Fi y Recomendaciones de Seguridad”**

Trabajo de graduación previo a la obtención del título de:

MAGÍSTER EN TELECOMUNICACIONES

Autor:

LUIS MIGUEL SERRANO VÁZQUEZ

Director:

DANIEL ESTEBAN ITURRALDE PIEDRA

CUENCA, ECUADOR

2022

Demostración y Análisis de Vulnerabilidades Existentes en Redes Wi-Fi y Recomendaciones de Seguridad

RESUMEN

Wi-Fi es una de las tecnologías más utilizadas en el mercado. Se implementa en hogares, universidades, negocios, empresas, entre otros. Al ser una tecnología de comunicación inalámbrica, brinda facilidad y comodidad a los usuarios, pero también expone la información que se está transmitiendo. Esta puede ser capturada por un tercero, con un receptor, dentro del área de cobertura, por lo que se debe garantizar la confidencialidad, integridad y disponibilidad en la comunicación. En este trabajo se realiza una descripción y análisis de los protocolos de seguridad de Wi-Fi, desde los más antiguos e inseguros como WEP y WPA hasta los más modernos y recomendados como WPA2 y WPA3. Se realiza una descripción y demostración práctica, en una red de pruebas, de las vulnerabilidades que se pueden encontrar en cada protocolo para, finalmente, detallar las medidas y recomendaciones que permiten mitigar estos problemas de seguridad. Las recomendaciones consisten en técnicas y protocolos seguros que se pueden utilizar, configuraciones que se pueden hacer en los equipos y descripciones de las mejoras que se pueden obtener con actualizaciones en los dispositivos.

Palabras clave: Wi-Fi, seguridad, WPA2, WPA3.



Ing. Daniel Iturralde Piedra. Ph.D
Coordinador de Carrera



Ing. Daniel Iturralde Piedra. Ph.D
Director de Trabajo de Titulación



Ing. Luis Miguel Serrano Vázquez
Autor

Demonstration and Analysis of Existing Vulnerabilities in Wi-Fi Networks and Security Recommendations

ABSTRACT

Wi-Fi is one of the most widely used technologies on the market. It is implemented in homes, universities, businesses, and companies. Being a wireless communication technology, it brings ease and comfort to users and exposes the information that is being transmitted. This can be captured by a third party, with a receiver, within the coverage area, so confidentiality, integrity, and availability in communication must be guaranteed. This paper described and analyzed Wi-Fi security protocols, from the oldest and most insecure ones, such as WEP and WPA, to the most modern and recommended ones, such as WPA2 and WPA3. A description and practical demonstration were made, in a lab network, of the vulnerabilities that could be found in each protocol to finally detail the measures and recommendations to mitigate these security problems. The proposals consisted of techniques and security protocols that can be used, configurations that can be made on the equipment, and descriptions of the improvements obtained with updates on the devices.

Keywords: Wi-Fi, security, WPA2, WPA3.



Ing. Daniel Iturralde Piedra. Ph.D
Career Coordinator



Ing. Daniel Iturralde Piedra. Ph.D
Thesis Director

Translated by:



Ing. Luis Miguel Serrano Vázquez
Author

