Análisis de seguridad en las redes Wi-Fi de acceso público gratuito: caso Barranquilla.

Security analysis in free public access Wi-Fi networks: Barranquilla case

DOI: https://doi.org/10.17981/cesta.05.01.2024.02

Research Article. Received: March 15, 2024; Accepted: May 15, 2024.

Diana Suárez-López
Corporación Universitaria Americana, Escuela de Postgrado de ingeniería
Barranquilla, Colombia
dsuarez@americana.edu.co

Karen Pinto-Mejia
Corporación Universitaria Americana, Escuela de Postgrado de ingeniería
Barranquilla, Colombia
pintokaren@americana.edu.co

Arquimedes Rios
Corporación Universitaria Americana, Escuela de Postgrado de ingeniería
Barranquilla, Colombia
arquimedesrios@gmail.com

Luis Villa
Corporación Universitaria Americana, Escuela de Postgrado de ingeniería
Barranquilla, Colombia
luisvilla0075@gmail.com

Wilber Hurtado
Corporación Universitaria Americana, Escuela de Postgrado de ingeniería
Barranquilla, Colombia
hurtadowalter@americana.edu.co

How to cite:
D. Suárez-López, K. Pinto Mejia, A. Rios, L. Villa, W. Hurtado "Security analysis in free public access Wi-Fi networks: Barranquilla case", *J. Comput. Electron. Sci.: Theory Appl., vol. 5 no. 1*, pp. 17-24, 2024. DOI: https://doi.org/10.17981/cesta.05.01.2024.02

Resumen

Este trabajo analiza las redes Wi-Fi públicas distribuidas en Barranquilla. Para ello, se identificaron y evaluaron métricas que permiten medir el desempeño de estas redes en términos de disponibilidad del servicio, confidencialidad y seguridad física. Adicionalmente, se consideraron varios aspectos, desde la cobertura y velocidad de conexión hasta la seguridad de autenticación e integridad de los datos transmitidos. Para ello se aplicaron herramientas de software libre como x, y, y z para facilitar la conservación de los datos. Los resultados muestran los puntos fuertes y débiles encontrados en cada red evaluada en términos de vulnerabilidades y algunas deficiencias.

Este estudio contribuye significativamente a este campo al proporcionar un marco para evaluar y mejorar las redes Wi-Fi públicas, promoviendo así su adopción segura y eficiente en entornos públicos.

Palabras Clave – seguridad informática; zonas Wi-Fi gratis estilo; títulos.

Abstract

This paper analyzes public Wi-Fi networks distributed throughout Barranquilla. For this purpose, metrics that allow measuring the performance of these networks in terms of service availability, confidentiality, and physical security were identified and evaluated. Additionally, several aspects were considered, from coverage and connection speed to the security of authentication and integrity of the transmitted data. For which free software tools such as x, y, and z were applied to facilitate data retention. The results show the strengths and weaknesses found in each network evaluated regarding vulnerabilities and some deficiencies.

This study contributes significantly to the field by providing a framework for evaluating and improving public Wi-Fi networks, thus promoting their safe and efficient adoption in public environments.

Keywords–Wi-Fi; physical security; service availability; reliability.

I. INTRODUCTION

In Colombia, the Ministry of Information and Communication Technologies (MINTIC), to provide free Internet to Colombians who do not have this service, considered essential today, created the strategy of free public Wi-Fi zones, which are a free service that in these times of digital economy, provide significant support to different users. Thanks to the joint work of MINTIC and the ICT Management District of Barranquilla, 150 free Wi-Fi zones are installed in parks and squares (Fig. 1), allowing users to do different tasks, entrepreneurship, and marketing work in digital channels.

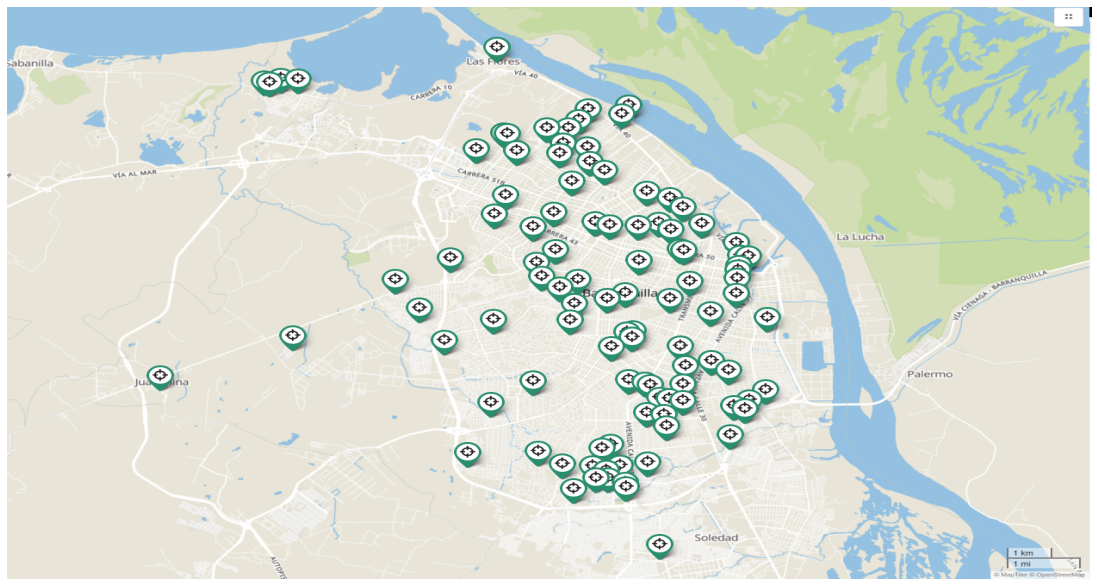

Fig. 1. Barranquilla Wi-Fi zones distribution map

MINTIC emphasizes that these networks have navigability restrictions to mitigate the misuse of the Internet to sites that may affect the good use of the area, such as pornography pages, recognized sites of terrorist groups, for banking transactions, fraud, or phishing [1]. In this sense, some cybersecurity entities do not consider making payments or other banking transactions advisable. Despite the risks, 5 million users throughout the country connect through these free connection points; in the case of Barranquilla, around 150 thousand users connect monthly.

These same particularities make free Wi-Fi hotspots interesting for users who must register their personal data (bank accounts, social network passwords, even personal photos, and videos) to browse, which are then exposed to all users connected to the same network, making them vulnerable. Being left defenseless makes them more palatable to black-hat hackers [2]; especially since they do not require authentication to establish a network connection. This allows hackers to access unprotected devices on the same network easily.

Daniel Frívidad, an expert at the National Institute of Cybersecurity (INCIBE) [3] for companies and professionals, explains that using open networks is dangerous regardless of your access system.

II. LITERATURE REVIEW

Computer security is defined as a set of policies and technological mechanisms that aim to ensure the confidentiality, integrity, and availability [4], [5] of the resources of a computer system. These elements are latent under circumstances or events that can cause damage or compromise them, translating into a threat. This takes advantage of a vulnerability in a system due to a failure in design, construction, or implementation to carry out a computer attack [6]. This is intended to execute any offensive maneuver of deliberate exploitation to gain unauthorized access, take control, destabilize, or damage a system.

Security in Wi-Fi networks is addressed by implementing specific security measures and protocols to protect the integrity, confidentiality, and availability [7] of data transmitted over the wireless network. Some of the common ways in which security in Wi-Fi networks is studied include [8]:

- Data encryption [9].
- Authentication [10].
- Access control [11].
- Network monitoring [12].
- Awareness [13] and education [14].

This paper [15] evaluates Wi-Fi network performance in five health centers in Marikina City, Philippines, as part of the "Free Wi-Fi for All" project. A smartphone system was implemented to collect Wi-Fi network information from the end-user's perspective. Smartphones collect information from access points, such as service set identifier (SSID) and received signal strength indicator (RSSI). This data was sent to a cloud server, where it was processed to visualize the quality and coverage of the Wi-Fi network using a Radio Signal Strength (RSS) map. The results obtained can be viewed at www.ph-Wi-Fi-map.com, which provides information on the Wi-Fi network quality of the FW4A program. The study also included bandwidth tests to determine if download speeds met the minimum requirements of the FW4A sites.

Similarly, in [16], a study is conducted to determine trust and security in public Wi-Fi networks. The perceived security of the network can influence users' decision to use or not use Wi-Fi. Likewise, distrust in the security of these networks, especially due to concerns about online fraud and data privacy, may lead to lower adoption of public Wi-Fi for certain transactions or to provide personal information.

In [17] proposes an innovative model of Wi-Fi zones with self-sustainable free connectivity as a critical factor to guarantee the connection's quality and the infrastructure's maintenance. This is to promote social development, focusing on using mobile devices for academic activities, information queries, procedures, and entertainment. In addition, there is a need to supply energy, perform monitoring based on a tracking system, and generate operation and attention reports.

III. METHODOLOGY

This research used quantitative methodology to collect and analyze safety-related data. For this purpose, the following measurement indicators were defined:

Service availability (AS): measures timely access during a given period. This indicator is given as a percentage

$$DS = (TA - \frac{IS}{TA})*100 \qquad (1)$$

Where,

TA: Activity time is given in minutes.

IS: Interruption of service is given in minutes.

Physical Safety: A checklist was designed with the following items: protection against fire, floods, earthquakes, explosions, and social manifestations, with a rating of 1 or 0 as appropriate, classified as low, medium, and high.

Confidentiality: A checklist was designed with the following items: implementation of security policies and captive portals, application of WAP encryption [18], WAP2 [19], WEP [20], encrypted passwords, and closed access to the web, with a rating of 1 or 0 as appropriate, classified as low, medium and high.

The following free software was used to measure the above metrics:

Wireshark: is packet analyzer software that captures incoming and outgoing network traffic [21]. Its versatility is worth highlighting because it supports hundreds of protocols, performs complete VoIP analysis, and helps monitor file metadata saved on disk. This information is analyzed and saved using the metadata of each packet. Also, it has filtering tools to present reconstructed streams of a TCP session.

Advanced IP Scanner: a free network scanning program [22]. It allows scanning, analyzing, and retrieving the required information from local network computers and private IP addressing, viewing shared folders after authentication and connecting to web servers, FTP [23], SSH [24], and incorporating other basic network tools.

Nmap: an open-source tool that allows scanning of the ports of the nodes of a network. Nmap helps to obtain information to monitor and manage security issues [16].

Kali Linux: is a Linux distribution based on Debian [25]. It has been designed for various security topics, such as network analysis, wireless attacks, and forensic analysis. It contains tools to perform all these security tests and analyses.

IV. RESULTS

Fig. 2 shows the location of the network's physical equipment. Some Wi-Fi zones were solar, and others were interconnected. We also observed that they all had the free Wi-Fi identification sign (TOTEM), and the height was 3 meters.

The evaluations were conducted in five random parks distributed throughout the city, yielding the following results.

According to Table I, it can be observed that the degree of service availability, on average, is high. However, the data show that availability varies among the different wind farms, with some experiencing service interruptions

and others operating without interruptions during the observed period. This indicates that, on average availability overall, most of the wind farms maintained an acceptable level of reliability during the period analyzed.

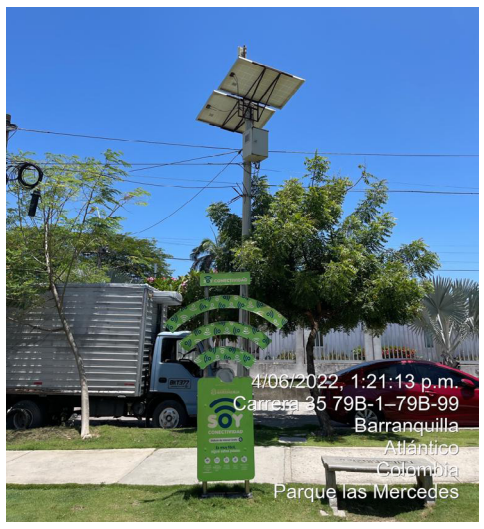

Fig. 2. Wi-Fi zones location

Table II shows that the parks have low protection in all aspects evaluated, except for protection against floods and social manifestations, where they have moderate protection (value 1). The fact that three items are in low protection implies that the parks may be exposed to significant risks in those areas.

Table I. Service Availability

Park	Activity time (minutes)	Service interruption (minutes)	Availability %
1	60	10	83.3
2	70	0	100
3	80	30	62.5
4	50	0	100
5	60	5	91.6
Total	320	45	85.9

Table II. Physical Security

Item	P1	P2	P3	P4	P5	Level
Fire protection	0	0	0	0	0	Low
Flood protection	1	1	1	1	1	Low
Earthquake protection	0	0	0	0	0	Low
Explosion protection	0	0	0	0	0	Low
Protection against social protests	1	1	1	1	1	Low
Overall score	2					Low

Table III shows that the overall score is low, indicating that the parks have deficiencies in the security measures implemented in all the aspects evaluated. This shows a high risk of security vulnerabilities and threats to network integrity and user privacy. This is a consequence of the non-implementation of security policies and encryption in Wi-Fi networks.

Table III. Confidentiality

Item	P1	P2	P3	P4	P5	Level
Security policies implementation	0	0	0	0	0	Low
Captive portals implementation.	1	1	1	1	1	Low
Application of WAP, WAP2, WEP encryption.	0	0	0	0	0	Low
Encrypted passwords	0	0	0	0	0	Low
Web access closed	1	1	1	1	1	Low
Overall score	2					Baja

On the other hand, the following vulnerabilities were detected in the evaluations carried out in the different parts:

- ICPM protocol enabled.
- Different open ports.
- Capture of network traffic.
- Network IP scanning.
- Network equipment manufacturer display.

Regarding the ports enabled, ports 53, 80, 443, 3128, and 8080 were enabled in parks 1, 2, and 3. As for Park 4, only protocol 445 was opened, and Park 5 was open to protocols 135, 139, and 445. These tests were made from different IPs.

The above data reflects that:

Port 53 is used by the Domain Name System (DNS) service. When found open, it could mean that the network allows DNS queries, which is necessary for web browsing and other network functions.

Port 80 is used for non-secure HTTP web browsing. Open indicates that unencrypted web traffic is allowed on the network.

Port 443 is also used for web browsing, but in this case, it implements the secure HTTPS protocol and uses the TLS protocol underneath. It acts as a virtual and secure endpoint through which all data transmissions are sent and received.

The presence of ports 3128 and 8080 could indicate the presence of a proxy server that may have various implications for the control and management of network traffic. It is important to note that security and privacy can be compromised if proper precautions are not taken when using a public Wi-Fi network.

Ports 135, 139, and 445 are associated with the Microsoft Windows network protocol called “Server Message Block” (SMB). Being open means that devices on that network may be using the SMB protocol for file sharing and printing, among other functions. However, having these ports open can also present security risks, as SMB has historically been a target for malware attacks due to vulnerabilities; additionally, it allows remote code execution and unauthorized access to shared resources. In this way, the network is exposed to ransomware attacks, exploiting vulnerabilities, and other forms of intrusion.

Finally, the controls implemented in the Wi-Fi zones of the selected parks were evaluated using a checklist, as shown in Table IV, to determine compliance with them.

Table IV. Checklist Application Results

Control	No. of Questions	Yes	Not
Network access control	5	1	4
Data protection and privacy control	1	1	0
Compliance Control	3	3	0
Physical and environmental security control	4	1	3
Total	13	6	7

According to the results obtained, the public Wi-Fi networks in the city of Barranquilla comply with the regulations the Colombian state requires to implement these types of networks and the data protection policy. However, most do not comply with the applicable controls regarding network access, information, and physical and environmental security.

Additionally, network traffic analysis was carried out using the free software tool Wireshark, which captured user and password credentials from a website, as shown in Fig. 3.

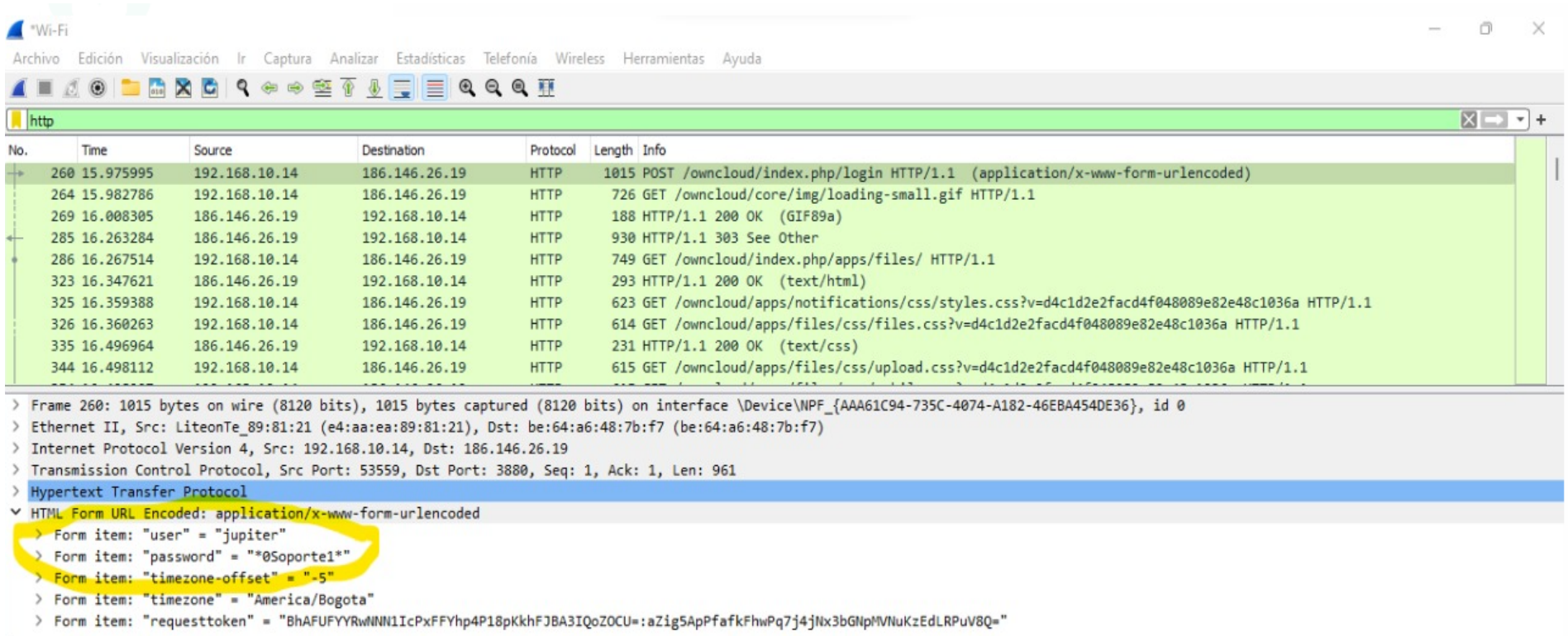

Fig 3. Wireshark analysis results.

V. CONCLUSIONS

The overall goal of port scanning is usually to find open ports, which is a victory for the cybercriminal looking for an avenue of attack. Still, it certainly increases the risk if proper security measures are not implemented.

opening ports on a public network increases the risk of cyber-attacks and data theft if adequate security measures are not implemented. Security depends on the configuration of the services operating on those ports and the overall network management and security policies implemented.

Regarding protocols, SMB (Server Message Block) if enabled on a Wi-Fi network, can introduce significant security risks, especially if security patches are not applied, secure configurations are implemented, and the network is actively monitored for malicious activity. Therefore, it is important to ensure that devices with open ports are properly protected with firewalls, security updates, and other security measures to prevent potential unauthorized intrusions.

It is recommended that SMB protocols be disabled if they are not necessary for network operation and that security best practices be applied to protect devices and data on the network.

Enabling the ICMP Protocol can provide benefits in terms of diagnostics, troubleshooting, and network monitoring, but it can also expose the network to certain security risks, especially in relation to denial-of-service attacks. Network administrators must balance the benefits and risks when making decisions about enabling ICMP on a network.

FUNDING

This research was developed with its resources.

AUTHORS' CONTRIBUTION

The authors confirm their contribution to the article as follows:
Research Arquimedes Rios, Karen Pinto-Mejia, Wilber Hurtado, Luis Villa; Manuscript preparation.
Diana Suárez-López; review, and editing.
Diana Suárez-López; methodology, data processing and manuscript preparation.
Diana Suárez-López, Arquimedes Rios, Wilber Hurtado, Karen Pinto-Mejia, Luis Villa; Methodology, research, visualization, and supervision.
All authors reviewed the results and approved the final version of the manuscript.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest to report regarding the present study.

REFERENCES

[1] MinTic, «MinTIC y Tigo inauguraron Wi-Fi gratuito en el Gran Malecón, en Barraquilla», https://www.mintic.gov.co/portal/inicio/Sala-de-prensa. [En línea]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/179064:MinTIC-y-Tigo-inauguraron-Wi-Fi-gratuito-en-el-Gran-Malecon-en-Barraquilla

[2] G. S. Rao, P. N. Kumar, P. Swetha, y G. BhanuKiran, «Security assessment of computer networks -an ethical hacker's perspective», en International Conference on Computing and Communication Technologies, Hyderabad, India: IEEE, dic. 2014, pp. 1-5. doi: 10.1109/ICCCT2.2014.7066756.

[3] «El Wi-Fi gratis puede salir muy caro». [En línea]. Disponible en: https://elpais.com/tecnologia/2019/09/02/actualidad/1567419913_441362.html

[4] I. D. Yakubdjanovna y X. I. Ubaydullayevna, «Analysis of Information Security Problems in Electronic Management with Possible Solutions», en 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan: IEEE, nov. 2021, pp. 1-5. doi: 10.1109/ICISCT52966.2021.9670265.

[5] E. A. Kirillova, U. M. Yakhutlov, X. Wenqi, G. Huiting, y W. Suyu, «Information Security in the Management of Personnel in a Modern Organization», en 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia: IEEE, sep. 2020, pp. 107-109. doi: 10.1109/ITQMIS51053.2020.9322884.

[6] T. Xie et al., «The Untold Secrets of Wi-Fi -Calling Services: Vulnerabilities, Attacks, and Countermeasures», IEEE Trans. Mob. Comput., vol. 20, n.o 11, pp. 3131-3147, nov. 2021, doi: 10.1109/TMC.2020.2995509.

[7] Y. Wang, J. Yao, y X. Yu, «Information Security Protection in Software Testing», en 2018 14th International Conference on Computational Intelligence and Security (CIS), Hangzhou, China: IEEE, nov. 2018, pp. 449-452. doi: 10.1109/CIS2018.2018.00106.

[8] Y. Wen y T. Liu, «WI-FI Security Certification through Device Information», en 2018 International Conference on Sensor Networks and Signal Processing (SNSP), Xi'an, China: IEEE, oct. 2018, pp. 302-305. doi: 10.1109/SNSP.2018.00065.

[9] Y. Liu, Q. Liao, J. Zhao, y Z. Han, «Deep Learning Based Encryption Policy Intrusion Detection Using Commodity Wi-Fi », en 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China: IEEE, dic. 2019, pp. 2129-2135. doi: 10.1109/ICCC47050.2019.9064215.

[10] R. Latha y B. R.M., «Detection of Deauthentication Threats in Wi-Fi Channels Using Machine Learning Strategies», en 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI), Chennai, India: IEEE, dic. 2022, pp. 1-6. doi: 10.1109/ICDSAAI55433.2022.10028874.

[11] G. Carrión-Barco, K. I. C. Quiroz, V. Alexandra, P. Fernández, D. J. F. Adrianzén, y A. C. Coloma, «Protocolos de autenticación de usuarios en el control de acceso a redes inalámbricas: Estudio comparativo».

[12] F. Xu, Q. Chen, Q. Liu, y N. Li, «Intelligent Analysis Algorithm for Hidden Danger Identification of Intelligent Network Monitoring System from the Perspective of Big Data», Procedia Comput. Sci., vol. 228, pp. 57-63, 2023, doi: 10.1016/j.procs.2023.11.008.

[13] A. B. Muñoz y M. G. Jiménez-Torres, «Análisis de expertos sobre la educación en ciberseguridad dirigida a población no-técnica».

[14] A. Beltran, M. G. Jiménez-Torres, y S. Sampayo, «Métodos y efectos de la educación en ciberseguridad: una revisión sistemática».

[15] R. S. Guion y W. M. Tan, «Characterization of Wi-Fi Signal Range and Bandwidth of the Philippines' "Free Wi-Fi For All" Project», en 2021 IEEE 13th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), Manila, Philippines: IEEE, nov. 2021, pp. 1-6. doi: 10.1109/HNICEM54116.2021.9731943.

[16] S. Liao et al., «A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments», en 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Chongqing, China: IEEE, oct. 2020, pp. 64-71. doi: 10.1109/CyberC49757.2020.00020.

[17] L. Fortich Tulena, «Propuesta para implementar un modelo innovador de zonas Wi-Fi con conectividad gratuita autosostenible en Sincelejo», en Innovación en la Región Caribe de Colombia: aportes teóricos y buenas prácticas, 1.a ed., Editorial CECAR, 2020. doi: 10.21892/9789585547858.5.

[18] Y. Z. Jian, N. Ismail, y M. S. Nabi, «Wireless Access Point Mapper (WAP-MAP): An Automated Wireless Access Point Plotting Web Application», en 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India: IEEE, nov. 2022, pp. 1-7. doi: 10.1109/ASSIC55218.2022.10088395.

[19] Z. Ya, «Research on The Design of Japanese Mobile Learning System Based on WAP», en 2020 5th International Conference on Smart Grid and Electrical Automation (ICSGEA), Zhangjiajie, China: IEEE, jun. 2020, pp. 450-453. doi: 10.1109/ICSGEA51094.2020.00103.

[20] A. Badholia, V. Verma, y S. K. Kashyap, «Wep, Wap and Wap2 Wireless Network Security Protocol: A Compact Algorithm : (Wireless Network Security Protocol)», en 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India: IEEE, oct. 2019, pp. 239-243. doi: 10.1109/ICCCIS48478.2019.8974517.

[21] H. Kim, H. Lee, y H. Lim, «Performance of Packet Analysis between Observer and WireShark», en 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang,, Korea (South): IEEE, feb. 2020, pp. 268-271. doi: 10.23919/ICACT48636.2020.9061452.

[22] N. X. Arreaga, G. M. Enriquez, S. Blanc, y R. Estrada, «Security Vulnerability Analysis for IoT Devices Raspberry Pi using PENTEST», Procedia Comput. Sci., vol. 224, pp. 223-230, 2023, doi: 10.1016/j.procs.2023.09.031.

[23] A. S. Reddy, A. Mahendra, S. Krishna, y N. Neelima, «Creating a Private Cloud using FTP Server», en 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India: IEEE, may 2021, pp. 159-161. doi: 10.1109/ICICCS51141.2021.9432320.

[24] M. Ariano. Kristyanto et al., «SSH Bruteforce Attack Classification using Machine Learning», en 2022 10th International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia: IEEE, ago. 2022, pp. 116-119. doi: 10.1109/ICoICT55009.2022.9914864.

[25] R. Karayat, M. Jadhav, L. S. Kondaka, y A. Nambiar, «Web Application Penetration Testing & Patch Development Using Kali Linux», en 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India: IEEE, mar. 2022, pp. 1392-1397. doi: 10.1109/ICACCS54159.2022.9785232.

Diana Suárez-López, holds a PhD in Computer Science and Technology from Universidad Carlos III de Madrid (UC3M) and is a Systems Engineer by profession, with an academic and research career framed by innovation and technological development and recognized as an Associate Researcher by the Ministry of Science, Technology, and Innovation.

Karen Pinto-Mejia, Arquimedes Rios, Luis Villa y Wilber Hurtado, are systems engineers specializing in computer security from the Graduate School of Engineering, American University Corporation.