ISSN: 1692-7257 - Volume 1 – Number 45 - 2025

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Digital Object Identifier: 10.24054/rcta.v1i45.2966

Strengthening critical educational infrastructures: a Red Team approach and advanced vulnerability assessment methodologies

Fortalecimiento de infraestructuras educativas críticas: un enfoque de Red Team y metodologías avanzadas para la evaluación de vulnerabilidades

Isabel del Socorro Escobar Martínez[1], Msc. Katerine Márceles Villalba[2]
PhD. (c) Siler Amador Donado[3]

[1] ***Institución Universitaria Colegio Mayor del Cauca,*** *Facultad de Ingeniería, Grupo de investigación I+D en Informática, Popayán, Cauca, Colombia.*
[2] ***Universidad de Antioquia,*** *Facultad de Ingeniería, Grupo de Investigación In2Lab, Medellín, Antioquia, Colombia.*
[3] ***Universidad del Cauca,*** *Facultad de Ingeniería Electrónica y Telecomunicaciones, Grupo de Investigación GTI, Popayán, Cauca, Colombia.*

Correspondence: *katerine.marceles@udea.edu.co*

Received: *june 16, 2024.* ***Accepted:*** *december 20, 2024.* ***Published:*** *january 01, 2025.*

How to cite: *I. S. Escobar Martínez, K. Marceles Villalba, and S. Amador Donado, "Strengthening critical educational infrastructures: a Red Team approach and advanced vulnerability assessment methodologies", RCTA, vol. 1, no. 45, pp. 159–169, jan.2025. Recovered from https://ojs.unipamplona.edu.co/index.php/rcta/article/view/2966*

Abstract: This article delves into strengthening security in critical educational infrastructures using a Red Team approach for thorough vulnerability assessments. Applying methodologies like the Penetration Testing Execution Standard (PTES) and the Open Web Application Security Project (OWASP), the study identifies subtle vulnerabilities, emphasizing the need for a proactive approach. The Red Team perspective, mimicking attacker tactics, uncovers system weaknesses, allowing for preventive measures. The analysis highlights crucial concerns, particularly in Apache server configurations, stressing the need for continuous reviews and compatibility checks. Recommendations include adopting OWASP for preventive audits, regular server configuration updates, and strengthening firewalls for rapid anomaly response. Insights on Denial of Service attacks underscore the urgency of immediate action and a quick, effective response. The findings emphasize the importance of vigilant protection, paving the way for a resilient educational sector against evolving cyber threats.

Keywords: critical infrastructures, denial of service, educational security, red team, owasp.

Resumen: Este artículo profundiza en el fortalecimiento de la seguridad en infraestructuras educativas críticas, utilizando un enfoque de Red Team para evaluaciones exhaustivas de vulnerabilidades. Aplicando metodologías como Penetration Testing Execution Standard (PTES) y Open Web Application Security Project (OWASP), el estudio identifica vulnerabilidades sutiles, subrayando la necesidad de un enfoque proactivo. La perspectiva del Red Team, que imita tácticas de atacantes, descubre debilidades del sistema,

permitiendo implementar medidas preventivas. El análisis destaca preocupaciones cruciales, especialmente en configuraciones del servidor Apache, enfatizando la necesidad de revisiones continuas y verificaciones de compatibilidad. Las recomendaciones incluyen la adopción de OWASP para auditorías preventivas, actualizaciones regulares de configuraciones del servidor y fortalecimiento de firewalls para una respuesta rápida ante anomalías. Las percepciones sobre ataques de Denegación de Servicio resaltan la urgencia de acciones inmediatas y una respuesta rápida y efectiva. Los hallazgos destacan la importancia de una protección vigilante, allanando el camino para un sector educativo resiliente ante amenazas cibernéticas.

Palabras clave: denegación de servicios, infraestructuras críticas, red team, seguridad educativa, owasp.

1. INTRODUCTION

E Critical infrastructures play an essential role in all regions, providing vital services to their users. These systems handle highly sensitive data, which varies by sector, and are subject to increasing threats of cyberattacks in our digital age [1]. The constant evolution of technology has made information systems increasingly indispensable for any entity, regardless of its field. However, this dependence has also exposed these infrastructures to numerous risks, as no information system is completely secure [2].

In this context, the educational sector stands out as one of the most critical areas. The security of information systems is not only vital for data integrity but also for the reputation and trust of users in the provided services. The constant threat from cybercriminals seeking to exploit vulnerabilities in these infrastructures exacerbates the situation. According to the Colombian Chamber of Informatics and Telecommunications, Colombia has seen an 18% increase in cyberattack incidents, highlighting the urgency of addressing this problem [3].

The educational sector is particularly vulnerable due to the diversity of areas and the abundance of sensitive information, with the possibility of internal threats from students seeking illicit benefits [4]. The need for a proactive and effective response is evident in the "Red Team" approach. This approach involves simulating potential attacks and detecting security gaps in the network, allowing vulnerabilities to be corrected before cybercrimes materialize [5].

A comparative methodological approach with elements of descriptive research is adopted. This methodology allows for thorough evaluation of security techniques and facilitates effective detection of network vulnerabilities, thereby enabling the implementation of appropriate preventive measures.

The following related works provided support and background for the project:
The project titled "Analysis of Technological Infrastructure Vulnerabilities through White-Box Testing under ISO 27005 at Caracol Radio, Main Node Bogotá" by [6] focused on evaluating and analyzing the information system risks at Caracol Radio. Using the white-box testing methodology, large volumes of data were examined to identify weaknesses, despite this technique requiring considerable time. After the evaluation, recommendations based on the identified vulnerabilities were provided to minimize risks. This project was based on the ISO 27005 framework and served as a guide for diagnosing vulnerabilities, assessing their effects on the company, and facilitating the implementation of a new pentesting methodology.

Another project titled "Development of Methodology for Finding Vulnerabilities in Corporate Networks and Controlled Intrusions" presented by [7], developed various pentesting methodologies to identify vulnerabilities in a proposed corporate network scenario. This project compared and analyzed three methodologies: Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), and OWASP. The quantitative comparison of these methodologies was crucial for choosing one and served as a valuable reference for the current work.

Additionally, the "Proposal of a Risk-Oriented Penetration Testing Methodology" developed by [8], focused on comparing five widely used

pentesting methodologies, considering criteria such as usability and risk assessment. This proposal provided a comparative structure that was adapted with more criteria to select the appropriate methodology, offering theoretical support to the current project.

Finally, the study "A Study of Security Awareness in Dhaka City Using a Portable WiFi Pentesting Device" by [9] focused on the vulnerabilities of wireless networks and associated risks, particularly through the Evil-Twin attack. This technique stands out for tricking users into falling victim to Man-in-the-Middle (MITM) attacks. The study provided significant insights into wireless network security and highlighted the need to raise user awareness, especially in public areas.

In light of the above, these investigations provide a comparative basis for selecting methodologies, a detailed evaluation of available options, and an awareness of specific vulnerabilities in wireless networks. These contributions will enable effective decision-making and strategy development for vulnerability assessment and mitigation.

2. METHODOLOGY

The methodological process employed in this study was based on a comparative methodology with elements of descriptive research. The comparative methodology was crucial for analyzing various pentesting methodologies and assessing their effectiveness in the education sector [10]. This detailed comparison allowed for the identification of similarities and differences, providing valuable information to determine the most suitable methodology for educational infrastructures.

Simultaneously, the descriptive methodology was applied to gain a detailed understanding of each methodology's particularities, including their components, steps, and objectives. This approach provided a clear view of how these methodologies operate and how they can be applied in the context of critical educational infrastructures.

The combination of both methodologies ensured a comprehensive analysis of vulnerabilities [7], providing a solid foundation for decision-making and the implementation of security improvements in the educational sector. This rigorous and complete approach not only offered a deep understanding of pentesting methodologies but also laid the groundwork for future research and practical applications in the security of educational infrastructures.

This article presents a solid methodological approach based on a comparative methodology with elements of descriptive research to conduct penetration testing (pentesting) in critical infrastructures [11]. The selection and application of pentesting methodologies are essential for detecting vulnerabilities in specific environments. From the perspective of a red team [12], the following phases were determined:

2.1. Phase 1: Selection of Pentesting Methodology

Several key methodologies were analyzed and compared to choose the most suitable one for the project. The OSSTMM (Open Source Security Testing Methodology Manual) methodology stands out for its quantitative approach and constant updates, allowing for a thorough security evaluation [8]. The OWASP (Open Web Application Security Project) methodology focuses on web applications and provides a standard model for risk assessment, including web audits and automated testing. ISSAF (Information System Security Assessment Framework) focuses on specific areas like network and application security, offering a comprehensive evaluation framework [13], [14]. Meanwhile, PTES (Penetration Testing Execution Standard) combines elements of OSSTMM and OWASP [15], allowing for a qualitative and adaptive approach, emphasizing network configuration and services [8].

These methodologies provide a solid framework for conducting penetration tests on critical infrastructures, ensuring a detailed evaluation and a systematic approach. The combination of these methodologies guarantees a comprehensive analysis of vulnerabilities, providing a solid basis for security decisions and improvements in critical infrastructures.

2.1.1. Quality Evaluation Criteria for Pentesting Methodologies

Based on the above, quality evaluation criteria were established [16] to ensure an appropriate evaluation of the pentesting methodologies considered. The established evaluation criteria were:

1. **CEC 1**: Does the methodology focus on and apply to data networks?

2. **CEC 2**: Does the methodology have a technical focus to provide helpful recommendations based on the detected vulnerabilities?
3. **CEC 3**: Does the methodology have a detailed analysis depth when searching for vulnerabilities?
4. **CEC 4**: Does the methodology have high usability to be considered acceptable in the quality evaluation criteria?
5. **CEC 5**: Does the methodology include metrics for measuring risks and properly evaluating the impact of detected vulnerabilities on critical infrastructure?
6. **CEC 6**: Does the methodology have detailed phases covering all necessary activities for a complete analysis according to the initial objective?

For each quality evaluation criterion, the following rating was applied:

- **S (yes) = 1**
- **P (partially) = 0.5**
- **N (no) = 0**

Thus, the total score for evaluating each methodology (CEC1 + CEC2 + CEC3 + CEC4 + CEC5 + CEC6) could result in: 0 (incomplete), 0.5-2.0 (regular), 2.5-3.0 (good), 3.5-4.5 (very good), and 5.0 (excellent).

To evaluate each pentesting methodology, specific rules were established for each evaluation criterion, complementing the qualitative assessment:

- **CEC 1**: Specific focus on data networks.
- **CEC 2**: Adequate technical scope.
- **CEC 3**: Depth in vulnerability analysis.
- **CEC 4**: Level of usability.
- **CEC 5**: Clear metrics for risk evaluation.
- **CEC 6**: Detailed development phases.

2.1.2. Quality Evaluation Study for Pentesting Methodologies

In the following table, a qualitative quality evaluation was conducted for the different pentesting methodologies investigated, aiming to select the most suitable for the research, considering various characteristics such as area, use, analysis, evaluation, and results. Four important methodologies in the field of pentesting were considered, which have good practices and support guides for detailed results.

The following Comparison of Security Evaluation Methodologies is the result of an adaptation of Álvarez Intriago, Vilma (2018), from her work "Propuesta de una Metodología de Pruebas de Penetración Orientada a Riesgos":

.

Scope and Focus

- **OSSTMM**: Operational focus for any company wanting to assess information security.
- **OWASP**: Focused on web applications.
- **PTES**: Applicable to any application environment.
- **ISSAF**: Focused on organizational security assessment requirements.

Range

- **OSSTMM**: Covers equipment and systems associated with the network.
- **OWASP**: Audits for web applications.
- **PTES**: Focused on specific technical levels.
- **ISSAF**: Evaluates the network and application control systems.

Depth

- **OSSTMM**: Detailed analysis.
- **OWASP**: Detailed analysis.
- **PTES**: Unifies OSSTMM and OWASP methodologies.
- **ISSAF**: Detailed procedures for testing.

Usability

- **OSSTMM**: Medium level of usability.
- **OWASP**: High usability for web applications.
- **PTES**: Medium usability due to process updates.
- **ISSAF**: Medium usability.

Metrics

- **OSSTMM**: Uses RAV (risk assessment values) for security.
- **OWASP**: Has metrics for risk assessment.

- **PTES**: Uses qualitative risk levels for effective client communication.
- **ISSAF**: No established metrics.

Risk Assessment

- **OSSTMM**: Applies RAV quantifiably.
- **OWASP**: Uses metrics for risk assessment.
- **PTES**: Does not have its own risk assessment; relies on OSSTMM methodology.
- **ISSAF**: Uses established calculations and formulas for evaluation.

Duration of Application

- **OSSTMM**: 4 development phases.
- **OWASP**: 2 phases (active and passive).
- **PTES**: 7 development phases.
- **ISSAF**: 3 development phases.

Advantages

- **OSSTMM**: Depth in vulnerability scanning and best practices for risk detection and analysis.
- **OWASP**: Methodology based on the software lifecycle.
- **PTES**: The unification of methodologies provides a comprehensive approach.
- **ISSAF**: Project-focused environment.

Disadvantages

- **OSSTMM**: Requires training for effective implementation and results.
- **OWASP**: Limited to web devices; risk analysis not complex.
- **PTES**: Seldom used.
- **ISSAF**: Lacks metrics for optimal risk assessment.

The following table presents a quality evaluation of various pentesting methodologies based on specific evaluation criteria. Each methodology is identified by an ID and its name, with quantitative and qualitative ratings obtained from the Quality Evaluation Criteria (CEC).

Table 1. *Evaluation of criteria.*

ID	Metodology	CEC 1	CEC 2	CEC 3	CEC 4	CEC 5	CEC 6	Cuantitative	Cualitative
1	OSSTMM	P	P	S	P	S	S	4.5	MB
2	OWASP	P	N	S	S	S	S	4.5	MB
3	PTES	P	S	S	P	S	S	5.0	E
4	ISSAF	S	P	P	P	N	N	2.5	R

Note: *S (yes) = 1, P (partially) = 0.5, N (no) = 0. Qualitative and Quantitative Notation: 2.5 = R (Regular), 4.5 = MB (Very Good), 5.0 = E (Excellent).*
Source: *Own elaboration.*

According to the project's objectives and focus on network security, the OSSTMM and OWASP methodologies are highlighted.

- **OSSTMM**: Stands out for its broad scope and detailed analysis, suitable for critical infrastructures. Its risk assessment is quantifiable, allowing for precise impact evaluation.
- **OWASP**: Ideal for detailed analysis of web applications, with high compatibility for web environments.

The PTES methodology is chosen for its ability to unify the previous methodologies and offer flexibility. It is adaptable to any environment, especially networks. Although it does not have its own risk assessment, it relies on OSSTMM, providing comprehensive vulnerability reports. Its seven phases allow for an in-depth and detailed analysis, from prior knowledge to the final detection and vulnerability report, ensuring that no detail is overlooked.

For the practical evaluation of internet threats, the OWASP methodology is used, suitable for web applications and servers. The structure of the PTES methodology is employed as a general guide for the project's phases, ensuring comprehensive and detailed coverage of the critical infrastructure.

2.2. Phase 2: Deployment of the selected pentesting methodology

It is important to mention that an educational institution was taken as a case study, which allowed for the proper deployment of the methodology to evaluate and identify vulnerabilities using the selected methodology. This was conducted under the principles of ethical hacking, employing a red team approach and framed within the legal

guidelines of Colombian Law 1279 of 2009 on computer crimes [17].

2.3. Stage I – Pre-Engagement

In this initial stage of the pentesting process, the education sector was identified as a particularly vulnerable critical area, especially highlighted due to the COVID-19 pandemic and previous incidents of attacks that compromised data integrity. These situations revealed a clear lack of attention by institutions towards the security of their systems, emphasizing the urgent need to improve security and trust measures. After considering various factors such as location, documentation, and permissions, the focus was on scanning the web server as the starting point for the vulnerability analysis.

2.4. Stage II – Information Gathering

In this stage, the white-box technique was implemented, which involves a deep knowledge of the infrastructure, including confidential details such as the internal network structure, security properties, server IP addresses, and interconnection diagrams. For the web server area, a thorough inventory of the devices and equipment was conducted, evaluating aspects such as cabling, firewall, and connections on the campus and critical infrastructure. Additionally, the Footprinting technique, or reconnaissance, was applied, which consisted of an exhaustive search of the website to obtain seemingly insignificant but valuable information. This information provided essential data to recognize vulnerabilities and facilitate server access. Using tools such as the Kali Linux terminal and nslookup commands, the web server IP addresses were validated, ensuring the accuracy and reliability of the data collected during this phase.

Similarly, using the Shodan tool, we searched for open ports and related information for an address, which in this case is the server of the entity. This tool allowed us to find vulnerabilities within a timeframe and investigate the most recent exploitation methods to inform critical infrastructure.

2.4.1. Results Obtained from the Shodan Tool

General Information of the Server The use of this tool allowed obtaining the IP address assigned to the server. The additional information provided by the tool included: host name, provider name, location, and ASN (Autonomous System Number, which refers to IP networks with their own and independent routes).

2.4.2. Port Evaluation

Ports 80, 110, 143, and 443 were found to be open, all associated with the TCP (Transmission Control Protocol).

The following table presents the vulnerabilities detected by the SHODAN tool in 2022 associated with the web server.

Table 2: *Information collected from the Shodan tool on vulnerability*

Vulnerability	Description
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier versions, a malicious request to a Lua script calling r:parsebody(0) can cause a denial-of-service due to no default limit on possible input size.
CVE-2022-22721	If LimitXMLRequestBody is configured to allow request bodies larger than 350 MB (the default value is 1 MB) on 32-bit systems, an integer overflow occurs leading to out-of-bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier versions.
CVE-2022-22720	Apache HTTP Server 2.4.53 and earlier versions may not send X-Forwarded-* headers to the origin server according to the client-side connection header hop-by-hop mechanism. This can be used to bypass IP-based authentication on the origin server/application.
CVE-2022-23943	A carefully crafted request body can cause a read into a random memory area, potentially causing the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier versions.

Source: *Own elaboration*.

Based on the findings, the Nikto tool was employed to complement the information previously gathered with Shodan. Through Nikto, an additional scan was conducted to obtain further relevant details for vulnerability analysis.

The process began with a general scan of the website using the command:

nikto -h (host) or nikto -h (IP Address)

The results of this command revealed information about the server and its version, as well as some header issues, such as:

- Lack of protection against clickjacking: This indicates a lack of protection against the technique that deceives users to obtain confidential information or credentials by making them believe they are interacting with the original page. This is achieved through an invisible interface that deceives the user to extract login information or other data according to the attacker's objectives.

- Absence of definition of X-XSS Protection: This security header is designed to protect against XSS (Cross-Site Scripting) attacks, which occur when malicious scripts are injected into the website. This absence can be exploited when user input is not properly validated or encoded before being displayed in the output.

2.5. Stage III - Threat Modeling

In this stage of the process, the previously collected information was carefully analyzed to identify threats to the infrastructure. Factors such as the asset at risk, potential threats, attack consequences, and exploited vulnerabilities were assessed.

For this evaluation, the OWASP methodology was used, specialized in auditing web applications and discovering vulnerabilities, including the well-known "Top 10 vulnerabilities". These vulnerabilities, often unnoticed, can be exploited to cause a negative impact on the organization.

Among the main identified vulnerabilities are:

- Access control failures in OWASP.
- Cryptographic failures.
- Injection.
- Unsafe design.
- Incorrect security configuration.
- Vulnerable and outdated components.
- Identification and authentication failures.
- Software and data integrity failures.
- Security logging and monitoring failures.

These findings were organized into a descriptive risk matrix using the OWASP methodology as a guide. This matrix effectively considered specific vulnerabilities associated with web servers and applied appropriate measures to mitigate these risks.

To systematically address vulnerabilities, an assessment matrix was developed that considers qualitative and quantitative aspects. This matrix provides a detailed understanding of the impact, probability, and frequency associated with each vulnerability, allowing for an accurate assessment of its potential risk, show the table 2.

***Table 3**: Qualitative and Quantitative Risk Matrix*

Vulnerability	Impact	Probability	Frequency
Open IDS	Very High (10)	Very High (10)	Very frequent (9)
Cross Site Scripting	High (8)	Very High (10)	Very frequent (9)
Data Validation	High (8)	Media(7)	Media(7)
Robots.txt	Very High (10)	Media(7)	Very frequent (9)
Request Flooding	Very High (10)	Very High (10)	Very frequent (9)
Open headers	Medium (7)	Medium (7)	Medium(7)
Security Breach	High (8)	Low (4)	Medium(7)
Deseralización insegura	High (8)	Low (4)	Low (4)

***Source:** Own elaboration.*

2.6. Stage IV - Vulnerability Analysis

In the previous project phase, a variety of tools were employed, yielding detailed results during the scanning process, varying based on the specific area and focus presented. These tools not only aided in the analysis of vulnerabilities identified in the collection phase but also served to validate and discover additional vulnerabilities. This was achieved through the utilization of specific commands, based on threat modeling and prior studies to comprehend the impact on the evaluated critical infrastructure.

Among the tools utilized, Nmap stood out as a comprehensive option, providing information on vulnerabilities, port states, and services on each port, as well as update flaws, among other detections. A specific command, such as "-v -O -oscan-guess (IP Address)," enabled an aggressive process to detect the operating system, identifying devices like cameras and phones, and indicating the presence of ports in closed and filtered states.

Furthermore, Nmap offered the capability to perform an activity trace, analyzing versions and services. A packet capture filter and the MassDNS tool were used to identify the attack surface of a web

application. Through this process, IP addresses were obtained and a ping was sent to the server's IP, revealing information about open and closed ports along with their respective services. This information was crucial for assessing potential vulnerabilities in critical infrastructure, especially those related to the TCP protocol.

Additionally, the "vulners" script of Nmap was explored, as seen in the following figure, which allowed for external queries to identify vulnerabilities based on the CVE list, enumerating existing vulnerabilities. This function played a crucial role in providing specific details about the detected vulnerabilities, offering a deeper understanding of potential risks to the evaluated infrastructure. Together, these tools and techniques significantly contributed to the comprehensive analysis of vulnerabilities in the project.

This agile and detailed command provides references to CVE and evaluates the severity level of vulnerabilities, even offering exploit suggestions for exploitation. This tool, crucial in validating Shodan used previously in the collection phase, showed similarities in vulnerability detection. The most recent vulnerabilities detected, validated both by Shodan during information gathering and by Nmap through commands combined with specific vulnerability analysis scripts, were taken into account. This thorough comparison ensured a comprehensive and accurate assessment of identified threats.

2.7. Stage V - Exploitation

In this stage, vulnerabilities were assessed and exploited to understand their nature and measure their risk, focusing particularly on CVE-2022-29404, which enables a denial-of-service (DoS) attack. This type of attack aims to overwhelm a specific web server with an overwhelming flow of traffic or requests, causing the server to crash and interrupting service for users.

To exploit this vulnerability, the specialized tool LOIC was used, which sends multiple requests in TCP protocol. Despite a 4-hour attack that generated over 431 million requests, it was not sufficient due to the scale of the target server and the speed limitations imposed by the nature of the DoS attack.

After a previous pause, the continuous sending of requests resumed for approximately 24 hours, totaling 2,067,940,318 requests until the application ceased traffic, confirming the complete execution of the denial-of-service attack.

To verify the proper functioning of the traffic, Wireshark, a traffic control tool, was utilized, displaying details such as source and destination addresses, ports, and protocols used, along with ACK communication between source and destination machines.

When a potential denial-of-service was suspected, the website was accessed from various devices (laptop and cellphone) to validate the situation. This confirmed the server's downtime for a brief period, approximately 8 minutes, during which the denial-of-service was evident, preventing user access to the website.

2.8. Stage VI - Post-Exploitation

In this phase, considered optional within the OWASP methodology for web server pentesting, the response of the UTM (Unified Threat Management) security system to the denial-of-service attack was evaluated. Following the successful denial-of-service attack, the security system blocked the originating IP address for approximately one hour as a countermeasure. This action limited the complete execution of the post-exploitation phase, including functions such as privilege escalation, evasion of authentication mechanisms, and acquisition of information not visible to general users.

2.9. Stage VII - Report

The report details the entire process, from confirmation to evaluation and results obtained. A specific analysis was conducted on vulnerabilities found during the year, 2023, considering the types of attacks to which they are prone, their consequences, impacts, and corresponding mitigations. It specifies which attack from OWASP's Top 10 each vulnerability belongs to.

Comparing results by impact and origin, it is concluded that vulnerabilities found in the web server are primarily related to versioning and compatibility issues in its Apache code. These issues must be addressed during updates to prevent attackers from exploiting these vulnerabilities. Each of these vulnerabilities is classified with a high severity level, which is cause for concern, as they require review and solutions before a real attack occurs and compromises the integrity of user data or

the infrastructure itself. Vulnerabilities have been categorized based on severity, classified as critical, high, medium, and low, show the table 3.

Table 4: *Risk Analysis of Detected Vulnerabilities*

	CVE-23943	CVE-29404	CVE-22721	CVE-22720
Value	7.5	5.0	5.0	5.0
Attack	Buffer Overflow	Denial of Service	Integer Overflow	HTTP Request Smuggling
Consequence	Allows the attacker to overwrite memory with attacker-generated data	No limit on input size	Causes out-of-bounds writes	Does not discard the request body
Top 10 OWASP	Software and Data Integrity Failures	Software and Data Integrity Failures	Vulnerable and Outdated Components	Broken Access Control
Impact	Remote control of a host and privilege escalation	Temporary loss of the provided service	Causes buffer overflow	Allows bypassing security controls and accessing confidential data
Mitigation	Update	Update	Update	Update

Source: *Own elaboration.*

3. DISCUSSION

This work was based on rigorous penetration testing conducted on the web server of an educational institution. Utilizing PTES and OWASP methodologies, vulnerabilities and security measures were thoroughly explored and evaluated. Based on this meticulous analysis, the following recommendations emerged, highlighting the importance of proactively adopting measures to protect the integrity of the institution's data and services.

- Implementation of OWASP: It is urged to adopt the OWASP methodology for preventive audits. This methodology provides detailed analyses, detecting even seemingly simple but impactful vulnerabilities.
- Continuous Configuration Review: It is crucial to regularly review server configurations and ensure compatibility to avoid conflicts that could open doors to attacks. Frequent updates are essential.
- Strengthening the Firewall: Improve the firewall security system for a quick response to unusual traffic. Blocking IP addresses should be done proactively, anticipating potential exploitations of vulnerabilities.

4. CONCLUSION

Finally, it is important to present the processes and results obtained from the critical and reflective analysis regarding the exploration and identification of vulnerabilities through the following items:

- Strategic Selection of Methodologies: The combination of PTES and OWASP methodologies proved effective for evaluating the server. This specific approach provides a comprehensive assessment and allows for the proactive identification of vulnerabilities.
- Importance of the Red Team: The Red Team approach was crucial. By adopting the attacker's perspective, deficiencies were identified before they could be exploited. This enabled preventive actions and proactive protection of data and services.
- Detailed Report for Immediate Action: Alarming results, such as denial-of-service attacks, underscore the need for immediate measures. The detailed report provides specific recommendations to strengthen the system and protect the integrity of the entity's data and services.

ACKNOWLEDGMENT

Thanks to the University of Cauca, especially the GTI research group, the Colegio Mayor del Cauca University Institution, and the University of Antioquia and its In2lab group for providing the resources and support for the development of this proposal.

REFERENCES

[1] C. N. Baralt Blanco, ERD, “Infraestructuras críticas y ciberseguridad en las fuerzas armadas dominicanas”, Segur., Cienc. & Def., vol. 5, n.º 5, pp. 13–21, marzo de 2021. Accedido el 29 de mayo de 2024. [En línea]. Disponible: https://doi.org/10.59794/rscd.2019.v5i5.57

[2] J. L. González Quirós, “Las Instituciones Críticas En La Era Digital”, Nat. Lib. Rev. Estud. Interdiscip., vol. 1, n.º 11, febrero de 2019. Accedido el 29 de mayo de 2024. [En línea]. Disponible: https://doi.org/10.24310/natylib.2019.v1i11.5577

[3] J. A. Rincón Arteaga, A. Quijano Díaz, S. A. Castiblanco Hernández, J. D. Urquijo Vanegas y Y. K. P. L. Pregonero León,

"Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos?", Rev. Crim., vol. 64, n.º 3, pp. 95–116, 2022. Accedido el 29 de mayo de 2024. [En línea]. Disponible: https://doi.org/10.47741/17943108.368

[4] "Ciberseguridad en la Educación - Bejob". Bejob. Accedido el 29 de mayo de 2024. [En línea]. Disponible: https://bejob.com/ciberseguridad-en-la-educacion/

[5] J. Masís Solís, "La protección de las infraestructuras críticas en la era digital en el contexto de Costa Rica", Rev. Fac. Derecho Mex., vol. 69, n.º 274-1, p. 463, junio de 2019. Accedido el 29 de mayo de 2024. [En línea]. Disponible: https://doi.org/10.22201/fder.24488933e.2019.274-1.69957

[6] M. D. Lozano Alvarez, M. A. Correa Mesa, "Análisis de las vulnerabilidades de la infraestructura tecnológica mediante testing de caja blanca, bajo la norma ISO 27005 en la compañía Caracol Radio, nodo principal Bogotá", Trabajos de grado - Pregrado, Universidad Cooperativa de Colombia, Facultada de Ingeniería, Ingeniería de Sist., Bogotá, Bogotá, 2020. Accedido el 10 de mayo de 2023. [En línea]. Disponible: https://hdl.handle.net/20.500.12494/16502

[7] D. F. Ortiz Aristizábal, C. Caycedo, "Desarrollo de metodología para hallazgos de vulnerabilidades en redes corporativas e intrusiones controladas", Pregrado, Fund. Univ. Lib., Bogotá, 2015. Accedido el 3 de mayo de 2023. [En línea]. Disponible: http://hdl.handle.net/11371/342

[8] V. K. Alvarez Intriago, "Propuesta de una metodología de pruebas de penetración orientada a riesgos", Postgrado, Univ. Espiritu St., Guayaquil, 2018. Accedido el 12 de abril de 2023. [En línea]. Disponible: http://repositorio.uees.edu.ec/bitstream/123456789/2525/1/ALVAREZ%20INTRIAGO%20VILMA%20KARINA.pdf

[9] I. Hossain, M. M. Hasan, S. F. Hasan y M. R. Karim, "A study of security awareness in Dhaka city using a portable WiFi pentesting device", 2019 2nd Int. Conf. Innov. Eng. Technol. (ICIET). Accedido el 3 de mayo de 2023. [En línea]. Disponible: https://ieeexplore.ieee.org/document/9290589/authors#authors

[10] I. Vásquez Hidalgo. "Tipos de estudio y métodos de investigación". gestiopolis. Accedido el 1 de marzo de 2023. [En línea]. Disponible: https://www.gestiopolis.com/tipos-estudio-metodos-investigacion/

[11] "Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación". LISA Institute. Accedido el 11 de enero de 2023. [En línea]. Disponible: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

[12] M. Alba. "Análisis de metodologías de pentesting, red team y simulación de adversarios". B-SECURE | Pasión por la Seguridad. Accedido el 2 de febrero de 2023. [En línea]. Disponible: https://www.b-secure.co/blog/pentesting-red-team-y-simulacion-de-adversarios

[13] "Information Systems Security Assessment Framework". Pymesec.org. Accedido el 18 de enero de 2023. [En línea]. Disponible: https://pymesec.org/issaf/

[14] "Information System Security Assessment Framework (ISSAF)". FutureLearn. Accedido el 12 de julio de 2023. [En línea]. Disponible: https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521

[15] "Pentesting con OWASP: fases y metodología - Blog de hiberus". Blog de hiberus. Accedido el 18 de mayo de 2023. [En línea]. Disponible: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

[16] H. Ausecha, K. Márceles Villalba y S. Amador Donado, "Análisis de los frameworks de ciberseguridad en IIoT existentes", Rev. Iber. Tecnol. Informacion, n.º 49, pp. 436–448, 2022. Accedido el 9 de agosto de 2023. [En línea]. Disponible: https://www.risti.xyz/issues/ristie49.pdf

[17] L. Mayer Lux y J. Vera Vega, "El delito de espionaje informático: concepto y delimitación", Rev. Chil. Derecho Tecnol., vol. 9, n.º 2, p. 221, diciembre de 2020. Accedido el 29 de mayo de 2024. [En línea]. Disponible:

https://doi.org/10.5354/0719-2584.2020.59236