ISSN: 1692-7257 - Volumen 1 – Número 45 - 2025

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Digital Object Identifier: 10.24054/rcta.v1i45.2966

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

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

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.*

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

Recibido: *16 junio 2024.* ***Aceptado:*** *20 diciembre 2024.* ***Publicado:*** *01 enero 2025.*

Cómo citar: *I. S. Escobar Martínez, K. Marceles Villalba, y S. Amador Donado, «Fortalecimiento de infraestructuras educativas críticas: un enfoque de Red Team y metodologías avanzadas para la evaluación de vulnerabilidades», RCTA, vol. 1, n.º 45, pp. 159–169, jan.2025. Recuperado de 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. INTRODUCCIÓN

Las infraestructuras críticas desempeñan un papel esencial en todas las regiones, proporcionando servicios vitales a sus usuarios. Estos sistemas manejan datos altamente sensibles, que varían según el sector, y están sujetos a amenazas crecientes de ciberataques en nuestra era digital [1]. La constante evolución de la tecnología ha hecho que los sistemas de información sean cada vez más indispensables para cualquier entidad, sin importar su campo. Sin embargo, esta dependencia también ha expuesto a estas infraestructuras a numerosos riesgos, ya que ningún sistema de información es completamente seguro [2].

En este contexto, el sector educativo se destaca como una de las áreas más críticas. La seguridad de los sistemas de información no solo es vital para la integridad de los datos, sino también para la reputación y la confianza de los usuarios en los servicios proporcionados. La constante amenaza de los cibercriminales que buscan explotar vulnerabilidades en estas infraestructuras agrava la situación. Según la Cámara Colombiana de Informática y Telecomunicaciones, Colombia ha experimentado un aumento del 18% en incidentes de ciberataques, lo que resalta la urgencia de abordar este problema [3].

El sector educativo es particularmente vulnerable debido a la diversidad de áreas y la abundancia de información sensible, con la posibilidad de amenazas internas por parte de estudiantes que buscan beneficios ilícitos [4]. La necesidad de una respuesta proactiva y efectiva es evidente en el enfoque "Red Team". Este enfoque implica simular posibles ataques y detectar brechas de seguridad en la red, permitiendo corregir las vulnerabilidades antes de que los delitos cibernéticos se materialicen [5].

Se adopta un enfoque metodológico comparativo con elementos de investigación descriptiva. Esta metodología permite una evaluación exhaustiva de las técnicas de seguridad y facilita la detección efectiva de vulnerabilidades en la red, lo que a su vez posibilita la implementación de medidas preventivas adecuadas.

Los siguientes trabajos relacionados proporcionaron soporte y antecedentes para el proyecto:

El proyecto titulado "Análisis de Vulnerabilidades de la Infraestructura Tecnológica a través de Pruebas de Caja Blanca bajo ISO 27005 en Caracol Radio, Nodo Principal Bogotá" por [6] se centró en evaluar y analizar los riesgos del sistema de información en Caracol Radio. Utilizando la metodología de pruebas de caja blanca, se examinaron grandes volúmenes de datos para identificar debilidades, a pesar de que esta técnica requiere un tiempo considerable. Después de la evaluación, se proporcionaron recomendaciones basadas en las vulnerabilidades identificadas para minimizar los riesgos. Este proyecto se basó en el marco de trabajo de la ISO 27005 y sirvió como guía para diagnosticar vulnerabilidades, evaluar sus efectos en la empresa y facilitar la implementación de una nueva metodología de pentesting.

Otro proyecto titulado "Desarrollo de Metodología para Encontrar Vulnerabilidades en Redes Corporativas e Intrusiones Controladas" presentado por [7], desarrolló varias metodologías de pentesting para identificar vulnerabilidades en un escenario propuesto de red corporativa. Este proyecto comparó y analizó tres metodologías: Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), Marco de Evaluación de la Seguridad de los Sistemas de Información (ISSAF) y OWASP. La comparación cuantitativa de estas metodologías fue crucial para elegir una y sirvió como referencia valiosa para el trabajo actual.

Además, la "Propuesta de una Metodología de Pruebas de Penetración Orientada al Riesgo" desarrollada por [8], se centró en comparar cinco metodologías de pentesting ampliamente utilizadas, considerando criterios como la usabilidad y la evaluación de riesgos. Esta propuesta proporcionó una estructura comparativa que fue adaptada con más criterios para seleccionar la metodología adecuada, ofreciendo soporte teórico al proyecto actual.

Finalmente, el estudio "Un Estudio de Concienciación sobre la Seguridad en la Ciudad de Dhaka Utilizando un Dispositivo Portátil de Pentesting WiFi" realizado por [9] se centró en las vulnerabilidades de las redes inalámbricas y los riesgos asociados, particularmente a través del ataque de Evil-Twin. Esta técnica se destaca por engañar a los usuarios para que caigan víctimas de ataques Man-in-the-Middle (MITM). El estudio proporcionó información significativa sobre la seguridad de las redes inalámbricas y destacó la necesidad de aumentar la concienciación de los usuarios, especialmente en áreas públicas.
A la luz de lo anterior, estas investigaciones proporcionan una base comparativa para la selección de metodologías, una evaluación detallada de las opciones disponibles y una comprensión de las vulnerabilidades específicas en las redes inalámbricas. Estas contribuciones permitirán una toma de decisiones efectiva y el desarrollo de estrategias para la evaluación y mitigación de vulnerabilidades.

2. METODOLOGÍA

El proceso metodológico empleado en este estudio se basó en una metodología comparativa con elementos de investigación descriptiva. La metodología comparativa fue crucial para analizar varias metodologías de pentesting y evaluar su efectividad en el sector educativo [10]. Esta comparación detallada permitió identificar similitudes y diferencias, proporcionando información valiosa para determinar la metodología más adecuada para las infraestructuras educativas.

Simultáneamente, se aplicó la metodología descriptiva para obtener una comprensión detallada de las particularidades de cada metodología, incluidos sus componentes, pasos y objetivos. Este enfoque proporcionó una visión clara de cómo operan estas metodologías y cómo pueden aplicarse en el contexto de infraestructuras educativas críticas.

La combinación de ambas metodologías aseguró un análisis exhaustivo de las vulnerabilidades [7], proporcionando una base sólida para la toma de decisiones y la implementación de mejoras de seguridad en el sector educativo. Este enfoque riguroso y completo no solo ofreció una comprensión profunda de las metodologías de pentesting, sino que también sentó las bases para futuras investigaciones y aplicaciones prácticas en la seguridad de las infraestructuras educativas.

Este artículo presenta un sólido enfoque metodológico basado en una metodología comparativa con elementos de investigación descriptiva para llevar a cabo pruebas de penetración (pentesting) en infraestructuras críticas [11]. La selección y aplicación de metodologías de pentesting son esenciales para detectar vulnerabilidades en entornos específicos. Desde la perspectiva de un equipo rojo [12], se determinaron las siguientes fases:

2.1. Fase 1: Selección de Metodología de Pentesting

Se analizaron y compararon varias metodologías clave para elegir la más adecuada para el proyecto. La metodología OSSTMM (Open Source Security Testing Methodology Manual) se destaca por su enfoque cuantitativo y actualizaciones constantes, permitiendo una evaluación de seguridad exhaustiva [8]. La metodología OWASP (Open Web Application Security Project) se centra en aplicaciones web y proporciona un modelo estándar para la evaluación de riesgos, incluyendo auditorías web y pruebas automatizadas. ISSAF (Information System Security Assessment Framework) se enfoca en áreas específicas como la seguridad de redes y aplicaciones, ofreciendo un marco de evaluación integral [13], [14]. Mientras tanto, PTES (Penetration Testing Execution Standard) combina elementos de OSSTMM y OWASP [15], permitiendo un enfoque cualitativo y adaptativo, enfatizando la configuración de redes y servicios [8].

Estas metodologías proporcionan un marco sólido para realizar pruebas de penetración en infraestructuras críticas, asegurando una evaluación detallada y un enfoque sistemático. La combinación de estas metodologías garantiza un análisis exhaustivo de las vulnerabilidades, proporcionando una base para las tomas de decisiones de seguridad y las mejoras en infraestructuras críticas.

2.1.1 Criterios de Evaluación de Calidad para Metodologías de Pentesting

Con base en lo anterior, se establecieron criterios de evaluación de calidad [16] para asegurar una evaluación adecuada de las metodologías de pentesting consideradas. Los criterios de evaluación establecidos fueron:

- **CEC 1**: ¿La metodología se enfoca y aplica a redes de datos?
- **CEC 2**: ¿La metodología tiene un enfoque técnico para proporcionar recomendaciones útiles basadas en las vulnerabilidades detectadas?
- **CEC 3**: ¿La metodología tiene un análisis detallado al buscar vulnerabilidades?
- **CEC 4**: ¿La metodología tiene una alta usabilidad para ser considerada aceptable en los criterios de evaluación de calidad?
- **CEC 5**: ¿La metodología incluye métricas para medir riesgos y evaluar adecuadamente el impacto de las vulnerabilidades detectadas en infraestructuras críticas?
- **CEC 6**: ¿La metodología tiene fases detalladas que cubren todas las actividades necesarias para un análisis completo según el objetivo inicial?

Para cada criterio de evaluación de calidad, se aplicó la siguiente calificación:
S (sí) = 1
P (parcialmente) = 0.5
N (no) = 0

Así, la puntuación total para evaluar cada metodología (CEC1 + CEC2 + CEC3 + CEC4 + CEC5 + CEC6) podría resultar en: 0 (incompleto), 0.5-2.0 (regular), 2.5-3.0 (bueno), 3.5-4.5 (muy bueno) y 5.0 (excelente).
Para evaluar cada metodología de pentesting, se establecieron reglas específicas para cada criterio de evaluación, complementando la evaluación cualitativa:

- **CEC 1**: Enfoque específico en redes de datos.
- **CEC 2**: Alcance técnico adecuado.
- **CEC 3**: Profundidad en el análisis de vulnerabilidades.
- **CEC 4**: Nivel de usabilidad.
- **CEC 5**: Métricas claras para la evaluación de riesgos.
- **CEC 6**: Fases de desarrollo detalladas.

2.1.2. Estudio de Evaluación de Calidad para Metodologías de Pentesting

En la siguiente tabla 1, se realizó una evaluación cualitativa de la calidad para las diferentes metodologías de pentesting investigadas, con el objetivo de seleccionar la más adecuada para la investigación, considerando varias características como área, uso, análisis, evaluación y resultados. Se consideraron cuatro metodologías importantes en el campo del pentesting, que tienen buenas prácticas y guías de soporte para resultados detallados.

La siguiente Comparación de Metodologías de Evaluación de Seguridad es el resultado de una adaptación de Álvarez Intriago, Vilma (2018), de su trabajo "Propuesta de una Metodología de Pruebas de Penetración Orientada a Riesgos":

Alcance y Enfoque
- **OSSTMM:** Enfoque operativo para cualquier empresa que desee evaluar la seguridad de la información.
- **OWASP:** Enfocado en aplicaciones web.
- **PTES:** Aplicable a cualquier entorno de aplicación.
- **ISSAF:** Enfocado en los requisitos de evaluación de seguridad organizacional.

Rango
- **OSSTMM:** Cubre equipos y sistemas asociados con la red.
- **OWASP:** Realiza auditorías para aplicaciones web.
- **PTES:** Enfocado en niveles técnicos específicos.
- **ISSAF:** Evalúa los sistemas de control de red y de aplicaciones.

Profundidad
- **OSSTMM**: Análisis detallado.
- **OWASP**: Análisis detallado.
- **PTES**: Unifica las metodologías de OSSTMM y OWASP.
- **ISSAF**: Procedimientos detallados para pruebas.

Usabilidad
- **OSSTMM:** Nivel medio de usabilidad.
- **OWASP:** Alta usabilidad para aplicaciones web.
- **PTES:** Usabilidad media debido a las actualizaciones de procesos.
- **ISSAF:** Usabilidad media.

Métricas

- **OSSTMM**: Utiliza RAV (valores de evaluación de riesgos) para la seguridad.
- **OWASP**: Tiene métricas para la evaluación de riesgos.
- **PTES**: Utiliza niveles de riesgo cualitativos para una comunicación efectiva con el cliente.
- **ISSAF**: No tiene métricas establecidas.

Evaluación de riesgos

- **OSSTMM:** Aplica RAV de manera cuantificable.
- **OWASP:** Utiliza métricas para la evaluación de riesgos.
- **PTES:** No tiene su propia evaluación de riesgos; se basa en la metodología OSSTMM.
- **ISSAF:** Utiliza cálculos y fórmulas establecidas para la evaluación.

Duración de la aplicación

- **OSSTMM**: 4 fases de desarrollo.
- **OWASP**: 2 fases (activa y pasiva).
- **PTES**: 7 fases de desarrollo.
- **ISSAF**: 3 fases de desarrollo.

Ventajas

- **OSSTMM**: Profundidad en el escaneo de vulnerabilidades y mejores prácticas para la detección y análisis de riesgos.
- **OWASP**: Metodología basada en el ciclo de vida del software.
- **PTES**: La unificación de metodologías proporciona un enfoque integral.
- **ISSAF**: Entorno enfocado en proyectos.

Desventajas

- **OSSTMM**: Requiere capacitación para una implementación y resultados efectivos.
- **OWASP**: Limitado a dispositivos web; análisis de riesgos no complejo.
- **PTES**: Rara vez utilizado.
- **ISSAF**: Carece de métricas para una evaluación óptima de riesgos.

La siguiente tabla presenta una evaluación de calidad de varias metodologías de pentesting basada en criterios de evaluación específicos. Cada metodología está identificada por un ID y su nombre, con calificaciones cuantitativas y cualitativas obtenidas de los Criterios de Evaluación de Calidad (CEC).

Tabla 1. *Evaluación de criterios.*

ID	Metodología	CEC 1	CEC 2	CEC 3	CEC 4	CEC 5	CEC 6	Cuantitativa	Cualitativa
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

Nota: *S (sí) = 1, P (parcialmente) = 0.5, N (no) = 0. Notación Cualitativa y Cuantitativa: 2.5 = R (Regular), 4.5 = MB (Muy Bueno), 5.0 = E (Excelente).*
Fuente: *Elaboración propia.*

De acuerdo con los objetivos del proyecto y el enfoque en la seguridad de redes, se destacan las metodologías OSSTMM y OWASP.

- **OSSTMM**: Se destaca por su amplio alcance y análisis detallado, adecuado para infraestructuras críticas. Su evaluación de riesgos es cuantificable, lo que permite una evaluación precisa del impacto.
- **OWASP**: Ideal para un análisis detallado de aplicaciones web, con alta compatibilidad para entornos web.

La metodología PTES se elige por su capacidad para unificar las metodologías anteriores y ofrecer flexibilidad. Es adaptable a cualquier entorno, especialmente redes. Aunque no tiene su propia evaluación de riesgos, se basa en OSSTMM, proporcionando informes de vulnerabilidad integrales. Sus siete fases permiten un análisis profundo y detallado, desde el conocimiento previo hasta la detección final y el informe de vulnerabilidades, asegurando que no se pase por alto ningún detalle.

Para la evaluación práctica de amenazas en internet, se utiliza la metodología OWASP, adecuada para aplicaciones web y servidores. La estructura de la metodología PTES se emplea como guía general para las fases del proyecto, asegurando una cobertura integral y detallada de la infraestructura crítica.

2.2. Fase 2: Implementación de la metodología de pentesting seleccionada

Es importante mencionar que se tomó una institución educativa como caso de estudio, lo que permitió la adecuada implementación de la metodología para evaluar e identificar vulnerabilidades utilizando la metodología seleccionada. Esto se llevó a cabo bajo los principios

del hacking ético, empleando un enfoque de equipo rojo y enmarcado dentro de las pautas legales de la Ley colombiana 1279 de 2009 sobre delitos informáticos [17].

2.3. Etapa I – Pre-compromiso

En esta etapa inicial del proceso de pentesting, se identificó al sector educativo como un área crítica particularmente vulnerable, especialmente destacada, debido a la pandemia de COVID-19 y a incidentes previos de ataques que comprometieron la integridad de los datos. Estas situaciones revelaron una clara falta de atención por parte de las instituciones hacia la seguridad de sus sistemas, enfatizando la necesidad urgente de mejorar las medidas de seguridad y confianza. Tras considerar varios factores como la ubicación, la documentación y los permisos, el enfoque se centró en escanear el servidor web como punto de partida para el análisis de vulnerabilidades.

2.4. Etapa II – Recolección de información

En esta etapa, se implementó la técnica de caja blanca, que implica un profundo conocimiento de la infraestructura, incluyendo detalles confidenciales como la estructura de la red interna, propiedades de seguridad, direcciones IP de los servidores y diagramas de interconexión. Para el área del servidor web, se realizó un inventario exhaustivo de los dispositivos y equipos, evaluando aspectos como el cableado, el cortafuegos y las conexiones en el campus y la infraestructura crítica.

Además, se aplicó la técnica de Footprinting, o reconocimiento, que consistió en una búsqueda exhaustiva del sitio web para obtener información aparentemente insignificante pero valiosa. Esta información proporcionó datos esenciales para reconocer vulnerabilidades y facilitar el acceso al servidor. Utilizando herramientas como la terminal de Kali Linux y comandos nslookup, se validaron las direcciones IP del servidor web, asegurando la precisión y confiabilidad de los datos recopilados durante esta fase.

De manera similar, utilizando la herramienta Shodan, se buscaron los puertos abiertos e información relacionada para una dirección, que en este caso es el servidor de la entidad. Esta herramienta permitió encontrar vulnerabilidades dentro de un marco temporal e investigar los métodos de explotación más recientes para informar sobre la infraestructura crítica.

2.4.1. Resultados obtenidos con la herramienta Shodan

Información general del servidor. El uso de esta herramienta permitió obtener la dirección IP asignada al servidor. La información adicional proporcionada por la herramienta incluyó: nombre del host, nombre del proveedor, ubicación y ASN (Número de Sistema Autónomo, que se refiere a redes IP con sus propias rutas independientes).

2.4.2. Puertos de evaluación

Se encontraron abiertos los puertos 80, 110, 143 y 443, todos asociados con el TCP (Protocolo de Control de Transmisión).

La siguiente tabla presenta las vulnerabilidades detectadas por la herramienta SHODAN en 2022 asociadas con el servidor web.

Tabla 2: *Información recopilada de la herramienta Shodan sobre vulnerabilidades*

Vulnerabilidades	Descripción
CVE-2022-29404	En el servidor Apache HTTP v.2.4.53 y versiones anteriores, presenta una vulnerabilidad a través de una solicitud maliciosa de un Lua script que llama a r: parsebody (0) puede causar una denegación de servicio debido a la falta de un límite predeterminado en el tamaño posible de la entrada.
CVE-2022-22721	Si LimitXMLRequestBody está configurado para permitir cuerpos de solicitud mayores de 350 MB (el valor predeterminado es 1 MB) en sistemas de 32 bits, ocurre un desbordamiento de enteros que lleva a escrituras fuera de límites. Este problema afecta a un servidor Apache HTTP v.2.4.52 y versiones anteriores.
CVE-2022-22720	Servidor Apache HTTP v.2.4.53 y versiones anteriores pueden no enviar los encabezados X-Forwarded-* al servidor de origen según el mecanismo de salto a salto del encabezado de conexión del lado del cliente. Esto puede usarse para eludir la autenticación basada en IP en el servidor o la aplicación de origen.
CVE-2022-23943	Un cuerpo de solicitud cuidadosamente elaborado puede causar una lectura en

	un área de memoria aleatoria, lo que podría provocar el bloqueo del proceso. Este problema afecta a el servidor Apache HTTP v.2.4.52 y versiones anteriores.

Fuente: *Elaboración propia.*

Basado en los hallazgos, se empleó la herramienta Nikto para complementar la información previamente recopilada con Shodan. A través de Nikto, se realizó un escaneo adicional para obtener más detalles relevantes para el análisis de vulnerabilidades.

El proceso comenzó con un escaneo general del sitio web utilizando el comando:

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

Los resultados de este comando revelaron información sobre el servidor y su versión, así como algunos problemas de encabezados, tales como:

Falta de protección contra clickjacking: Esto indica la falta de protección contra la técnica que engaña a los usuarios para obtener información confidencial o credenciales haciéndoles creer que están interactuando con la página original. Esto se logra a través de una interfaz invisible que engaña al usuario para extraer información de inicio de sesión u otros datos según los objetivos del atacante.

Ausencia de definición de X-XSS-Protection: Este encabezado de seguridad está diseñado para proteger contra ataques XSS (Cross-Site Scripting), que ocurren cuando se inyectan scripts maliciosos en el sitio web. Esta ausencia puede ser explotada cuando la entrada del usuario no se valida o codifica adecuadamente antes de mostrarse en la salida.

2.5. Etapa III – Modelado de Amenazas

En esta etapa del proceso, la información previamente recopilada fue cuidadosamente analizada para identificar amenazas a la infraestructura. Se evaluaron factores como el activo en riesgo, las posibles amenazas, las consecuencias del ataque y las vulnerabilidades explotadas.
Para esta evaluación, se utilizó la metodología OWASP, especializada en la auditoría de aplicaciones web y el descubrimiento de vulnerabilidades, incluyendo las conocidas "Top 10 vulnerabilidades". Estas vulnerabilidades, a menudo pasadas por alto, pueden ser explotadas para causar un impacto negativo en la organización.
Entre las principales vulnerabilidades identificadas se encuentran:

- Fallos de control de acceso en OWASP.
- Fallos criptográficos.
- Inyecciones.
- Diseño inseguro.
- Configuración de seguridad incorrecta.
- Componentes vulnerables y desactualizados.
- Fallos de identificación y autenticación.
- Fallos de integridad del software y de los datos.
- Fallos en el registro y monitoreo de seguridad.

Estos hallazgos se organizaron en una matriz de riesgos descriptiva utilizando la metodología OWASP como guía. Esta matriz consideró eficazmente las vulnerabilidades específicas asociadas con los servidores web y aplicó medidas adecuadas para mitigar estos riesgos.
Para abordar sistemáticamente las vulnerabilidades, se desarrolló una matriz de evaluación que considera aspectos cualitativos y cuantitativos. Esta matriz proporciona una comprensión detallada del impacto, la probabilidad y la frecuencia asociada con cada vulnerabilidad, permitiendo una evaluación precisa de su riesgo potencial, como se muestra en la tabla 3.

Tabla 3: *Matriz de Riesgo Cualitativa y Cuantitativa*

Vulnerabilidad	Impacto	Probabilidad	Frecuencia
Open IDS	Muy alto (10)	Muy alto (10)	Muy frecuente (9)
Cross Site Scripting	Alto (8)	Muy alto (10)	Muy frecuente (9)
Data Validacion	Alto (8)	Media (7)	Media (7)
Robots.txt	Muy alto (10)	Media (7)	Muy frecuente (9)
Request Flooding	Muy alto (10)	Muy alto (10)	Muy frecuente (9)
Open headers	Media (7)	Media (7)	Media (7)
Brechas de seguridad	Alto (8)	Bajo (4)	Media (7)
Deseralización insegura	Alto (8)	Bajo (4)	Bajo (4)

Fuente: *Elaboración propia.*

2.6. Etapa IV – Análisis de Vulnerabilidades

En la fase anterior del proyecto, se empleó una variedad de herramientas, lo que produjo resultados detallados durante el proceso de escaneo, variando según el área específica y el enfoque presentado. Estas herramientas no solo ayudaron en el análisis de las vulnerabilidades identificadas en la fase de recopilación, sino que también sirvieron para validar y descubrir vulnerabilidades adicionales. Esto se logró mediante la utilización de comandos específicos, basados en modelado de amenazas y estudios previos para comprender el impacto en la infraestructura crítica evaluada.

Entre las herramientas utilizadas, Nmap destacó como una opción integral, proporcionando información sobre vulnerabilidades, estados de puertos y servicios en cada puerto, así como fallos de actualización, entre otras detecciones. Un comando específico, como "-v -O -oscan-guess (Dirección IP)," permitió un proceso agresivo para detectar el sistema operativo, identificando dispositivos como cámaras y teléfonos, e indicando la presencia de puertos en estados cerrados y filtrados. Además, Nmap ofreció la capacidad de realizar un seguimiento de actividad, analizando versiones y servicios. Se utilizó un filtro de captura de paquetes y la herramienta MassDNS para identificar la superficie de ataque de una aplicación web. A través de este proceso, se obtuvieron direcciones IP y se envió un ping a la IP del servidor, revelando información sobre puertos abiertos y cerrados junto con sus respectivos servicios. Esta información fue crucial para evaluar posibles vulnerabilidades en la infraestructura crítica, especialmente las relacionadas con el protocolo TCP. Además, se exploró el script "vulners" de Nmap, como se ve en la figura siguiente, que permitió consultas externas para identificar vulnerabilidades basadas en la lista CVE, enumerando las vulnerabilidades existentes. Esta función desempeñó un papel crucial al proporcionar detalles específicos sobre las vulnerabilidades detectadas, ofreciendo una comprensión más profunda de los riesgos potenciales para la infraestructura evaluada. Juntas, estas herramientas y técnicas contribuyeron significativamente al análisis integral de vulnerabilidades en el proyecto.

Este comando ágil y detallado proporciona referencias a CVE y evalúa el nivel de severidad de las vulnerabilidades, incluso ofreciendo sugerencias de explotación para la explotación. Esta herramienta, crucial para validar Shodan utilizado previamente en la fase de recopilación, mostró similitudes en la detección de vulnerabilidades. Se tomaron en cuenta las vulnerabilidades más recientes detectadas, validadas tanto por Shodan durante la recopilación de información como por Nmap a través de comandos combinados con scripts específicos de análisis de vulnerabilidades. Esta comparación exhaustiva garantizó una evaluación integral y precisa de las amenazas identificadas.

2.7. Etapa V - Explotación

En esta etapa, se evaluaron y explotaron las vulnerabilidades para entender su naturaleza y medir su riesgo, enfocándose particularmente en CVE-2022-29404, que permite un ataque de denegación de servicio (DoS). Este tipo de ataque busca abrumar a un servidor web específico con un flujo abrumador de tráfico o solicitudes, causando que el servidor se bloquee e interrumpa el servicio para los usuarios.

Para explotar esta vulnerabilidad, se utilizó la herramienta especializada LOIC, que envía múltiples solicitudes mediante el protocolo TCP. A pesar de un ataque de 4 horas que generó más de 431 millones de solicitudes, no fue suficiente debido a la escala del servidor objetivo y las limitaciones de velocidad impuestas por la naturaleza del ataque DoS.

Después de una pausa previa, se reanudó el envío continuo de solicitudes durante aproximadamente 24 horas, totalizando 2,067,940,318 solicitudes hasta que la aplicación cesó el tráfico, confirmando la ejecución completa del ataque de denegación de servicio.

Para verificar el correcto funcionamiento del tráfico, se utilizó Wireshark, una herramienta de control de tráfico, que mostraba detalles como las direcciones de origen y destino, los puertos y los protocolos utilizados, junto con la comunicación ACK entre las máquinas de origen y destino.

Cuando se sospechó de una posible denegación de servicio, se accedió al sitio web desde varios dispositivos (portátil y celular) para validar la situación. Esto confirmó el tiempo de inactividad del servidor durante un breve período, aproximadamente 8 minutos, durante el cual la denegación de servicio fue evidente, impidiendo el acceso de los usuarios al sitio web.

2.8. Etapa VI - Post-Explotación

En esta fase, considerada opcional dentro de la metodología OWASP para el pentesting de

servidores web, se evaluó la respuesta del sistema de seguridad UTM (Gestión Unificada de Amenazas) al ataque de denegación de servicio. Tras el exitoso ataque de denegación de servicio, el sistema de seguridad bloqueó la dirección IP de origen durante aproximadamente una hora como medida de contrarresto. Esta acción limitó la ejecución completa de la fase de post-explotación, incluyendo funciones como la escalada de privilegios, la evasión de mecanismos de autenticación y la adquisición de información no visible para los usuarios generales.

2.9. Etapa VII - Reporte

El informe detalla todo el proceso, desde la confirmación hasta la evaluación y los resultados obtenidos. Se realizó un análisis específico de las vulnerabilidades encontradas durante el año 2023, considerando los tipos de ataques a los que son propensas, sus consecuencias, impactos y las mitigaciones correspondientes. Se especifica a qué ataque del Top 10 de OWASP pertenece cada vulnerabilidad.

Al comparar los resultados por impacto y origen, se concluye que las vulnerabilidades encontradas en el servidor web están principalmente relacionadas con problemas de versionado y compatibilidad en su código de Apache. Estos problemas deben abordarse durante las actualizaciones para evitar que los atacantes exploten estas vulnerabilidades. Cada una de estas vulnerabilidades se clasifica con un nivel de gravedad alto, lo cual es motivo de preocupación, ya que requieren revisión y soluciones antes de que ocurra un ataque real y comprometa la integridad de los datos del usuario o la infraestructura misma. Las vulnerabilidades se han categorizado según su gravedad, clasificándose como críticas, altas, medias y bajas. Muestra la tabla 4.

Tabla 4: *Análisis de Riesgo de Vulnerabilidades Detectadas*

	CVE-23943	CVE-29404	CVE-22721	CVE-22720
Valor	7.5	5.0	5.0	5.0
Ataque	Desbordamiento de Buffer	Desbordamiento de Buffer	Desbordamiento de Buffer	Desbordamien to de Buffer
Consecuencia	Permite al atacante sobrescribir la memoria con datos generados por el mismo	Permite al atacante sobrescribir la memoria con datos generados por el mismo	Permite al atacante sobrescribir la memoria con datos generados por el mismo	Permite al atacante sobrescribir la memoria con datos generados por el mismo
Top 10 OWASP	Fallos en el software y en la integridad de datos	Fallos en el software y en la integridad de datos	Fallos en el software y en la integridad de datos	Fallos en el software y en la integridad de datos
Impacto	Control remoto de un host y escalar privilegios	Control remoto de un host y escalar privilegios	Control remoto de un host y escalar privilegios	Control remoto de un host y escalar privilegios
Mitigación	Actualización	Actualización	Actualización	Actualización

Fuente: *Elaboración propia.*

3. DISCUSIÓN

Este trabajo se basó en rigurosas pruebas de penetración realizadas en el servidor web de una institución educativa. Utilizando las metodologías PTES y OWASP, se exploraron y evaluaron a fondo las vulnerabilidades y las medidas de seguridad. Basado en este meticuloso análisis, surgieron las siguientes recomendaciones, destacando la importancia de adoptar medidas proactivas para proteger la integridad de los datos y servicios de la institución.

- **Implementación de OWASP:** Se insta a adoptar la metodología OWASP para auditorías preventivas. Esta metodología proporciona análisis detallados, detectando incluso vulnerabilidades aparentemente simples pero impactantes.
- **Revisión Continua de Configuraciones:** Es crucial revisar regularmente las configuraciones del servidor y asegurar la compatibilidad para evitar conflictos que podrían abrir puertas a ataques. Las actualizaciones frecuentes son esenciales.
- **Fortalecimiento del Firewall:** Mejorar el sistema de seguridad del firewall para una respuesta rápida al tráfico inusual. El bloqueo de direcciones IP debe hacerse de manera proactiva, anticipándose a posibles explotaciones de vulnerabilidades.

4. CONCLUSION

Finalmente, es importante presentar los procesos y resultados obtenidos a partir del análisis crítico y reflexivo sobre la exploración e identificación de vulnerabilidades a través de los siguientes puntos:

- **Selección Estratégica de Metodologías**: La combinación de las metodologías PTES y OWASP demostró ser efectiva para evaluar el servidor. Este enfoque específico proporciona una evaluación integral y permite la identificación proactiva de vulnerabilidades. Además, la unificación de estas metodologías asegura una cobertura amplia, abarcando tanto la infraestructura como las aplicaciones web, garantizando así una protección más robusta y detallada.
- **Importancia del Red Team**: El enfoque del Red Team fue crucial. Al adoptar la perspectiva del atacante, se identificaron deficiencias antes de que pudieran ser

explotadas. Este enfoque permitió implementar acciones preventivas y proteger proactivamente los datos y servicios. La metodología del Red Team no solo evaluó las defensas existentes, sino que también destacó áreas de mejora en los protocolos de respuesta a incidentes, incrementando así la resiliencia global de la infraestructura de seguridad.

- **Reporte Detallado para Acción Inmediata**: Los resultados alarmantes, como los ataques de denegación de servicio (DoS), subrayan la necesidad de medidas inmediatas. El reporte detallado proporciona recomendaciones específicas para fortalecer el sistema y proteger la integridad de los datos y servicios de la entidad. Además de las recomendaciones, el reporte incluye un plan de acción con prioridades y cronogramas para la implementación de medidas correctivas y preventivas, asegurando una mejora continua de la postura de seguridad.
- **Capacitación y Concienciación**: Aparte de las medidas técnicas, es esencial implementar programas de capacitación y concienciación para el personal. La educación continua en prácticas de seguridad cibernética y la sensibilización sobre las amenazas actuales pueden reducir significativamente los riesgos de seguridad relacionados con errores humanos.
- **Monitoreo Continuo y Evaluación**: Establecer un sistema de monitoreo continuo es vital para detectar y responder rápidamente a nuevas amenazas. La evaluación periódica de la infraestructura y la actualización constante de las medidas de seguridad garantizan que la organización se mantenga protegida frente a un panorama de amenazas en constante evolución.

AGRADECIMIENTOS

Gracias a la Universidad del Cauca, especialmente al grupo de investigación GTI, a la Institución Universitaria Colegio Mayor del Cauca, y a la Universidad de Antioquia y su grupo In2lab por proporcionar los recursos y el apoyo para el desarrollo de esta propuesta.

REFERENCIAS

[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