Metodologías de testeo de redes de datos

Data network testing methodologies

Cristhian Villa Palma [1]

Jessica Morales Carrillo [2]

[1]Universidad Laica Eloy Alfaro de Manabí Dirección de Posgrado, Cooperación y Relaciones Internacionales, Chone, Manabí, Ecuador. e-mail: cristhian.villa@pg.uleam.edu.ec

[2]Grupo de Investigación SISCOM, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Campus Politécnico Sitio El Limón vía a la Pastora. Calceta, Manabí, Ecuador. e-mail: jmorales@espam.edu.ec

Contacto: cristhian.villa@pg.uleam.edu.ec

Resumen

El objetivo de esta investigación es proporcionar un enfoque general de las metodologías de testo de redes de datos que permitan identificar errores de seguridad y vulnerabilidad de las redes y definir la metodología que mejor se adapte. La metodología de trabajo utilizada fue la Revisión Sistémica de Literatura. En primer lugar, se definieron los criterios de búsqueda, luego se efectuó la búsqueda seleccionando los trabajos que cumplían con estos criterios, para luego identificar los campos que se analizarían y clasificarlos en una tabla, por último, se analizaron los criterios identificados en las metodologías y herramientas de testeo. Como resultado se pudo identificar que la metodología más empleada y efectiva para realizar testeo de redes es la OSSTMM (Open Source Security Testing Methodology Manual) con uso del 66,67% de los artículos analizado en esta revisión. La metodología OSSTMM, es la más usada entre las metodologías de testeo de redes y análisis de vulnerabilidades, siendo esta de uso libre y permite evaluar riesgo, que ayudan diferenciar y clasificar los diferentes problemas de seguridad de las organizaciones, así mismo permite a los profesionales contribuir con nuevas seguridades basadas en la metodología.

Palabras Clave: Metodología, Testeo, Redes de Internet, Vulnerabilidades.

CC BY NC ND

Abstract

The objective of this research is to provide a general approach to data network testing methodologies that allow identifying security errors and network vulnerabilities and defining the methodology that best suits them. The work methodology used was the Systemic Literature Review. In the first place, the search criteria were defined, then the search was carried out by selecting the works that met these criteria, to then identify the fields that would be analyzed and classify them in a table, finally, the criteria identified in the methodologies were analyzed. and testing tools. As a result, it was possible to identify that the most used and effective methodology for network testing is the OSSTMM (Open Source Security Testing Methodology Manual) with the use of 66.67% of the articles analyzed in this review. The OSSTMM methodology is the most used among the network testing and vulnerability analysis methodologies, being free to use and allows risk assessment, which helps to differentiate and classify the different security problems of organizations, as well as allowing professionals contribute with new securities based on the methodology.

Keywords: Methodology, Testing, Internet Networks, Vulnerabilities.

Introducción

Debido a las amenazas y los riesgos a los que se exponen los activos informáticos en las organizaciones, se vuelve muy importante contar con herramientas de control y supervisión, (Sendón-Varela et al., 2021). Es por eso por lo que se debe definir la metodología de testeo de vulnerabilidades de redes fiscas que sean de fácil implementación en organizaciones que empiezan procesos de reestructuración de los modelos de seguridad informática en sus redes de internet.

Una metodología define un conjunto de reglas prácticas y procedimientos que son ejecutados durante el curso de evaluación de cualquier programa de seguridad de la información y permite ordenar y estandarizar este proceso. La adopción de cualquier metodología debe ser un proceso aplicado de manera iterativa y reiterada en el tiempo, con el fin de descubrir los puntos débiles de la seguridad que pueden provocar que los datos y/o los equipos se vean afectados en mayor o menor medida por ataques,(Pinzon et al., 2013).

Es importante conocer las diferentes metodologías de testeo de redes que permitan preparar escenarios donde se puedan poner a prueba todas las técnicas y habilidades de un ataque, es por esta razón, que el

CC BY NC ND

conocimiento de las metodologías abiertas o de pago es de gran utilidad para anticiparse a un ataque de redes de internet.

Las metodologías más usadas en el Ethical Hacking (Chicaiza, 2019) son las siguientes:

• Osstmm (Fuente abierta de seguridad manual de métodos de prueba)

• Issaf (Marco de evaluación en sistemas de información de seguridad)

• Owasp (Solicitud del proyecto de seguridad open web)

• Ceh (Ethical hacking certificate)

• Offensive Security

Las pruebas de penetración son un paso crítico en el desarrollo de cualquier producto o sistema seguro. Aunque muchas empresas actuales definen las pruebas de penetración como la aplicación de escáneres de vulnerabilidad de red a un sitio operativo, las verdaderas pruebas de penetración es mucho más que eso. Las pruebas de penetración hacen hincapié no sólo en el funcionamiento, sino la implementación y el diseño de un producto o sistema.

Las redes de comunicaciones han experimentado un desarrollo vertiginoso en los últimos años, sin embargo, (López, 2016) se menciona que continúan enfrentando el factor seguridad informática que puede afectar su eficiente aprovechamiento. Entre las alternativas existentes para hacerle frente a este problema, se han destacado los llamados Diagnósticos de Red (Penetración Test).

Los riesgos de ataques a la información (Chicaiza, 2019) surgen a partir de las debilidades de las redes de Datos y de los sistemas, estos ataques ya sea internos o externos pueden dejar inoperables ciertos servicios y recursos de hardware y software generando pérdidas económicas y exponiendo nuestra información.

De acuerdo a McDermott,(2000) muchas empresas actuales definen las pruebas de penetración como la aplicación de escáneres de vulnerabilidad de red a un sitio operativo, las verdaderas pruebas de penetración es mucho más que eso. Las pruebas de penetración hacen hincapié no sólo en el funcionamiento, sino la implementación y el diseño de un producto o sistema.

CC BY NC ND

El Testing o penetración son las pruebas de penetración con la que las que disponen empresas e individuales de comprobar hasta ¿qué punto su red y/o dispositivos son seguros ante un ataque informático externo o interno? En un test de penetración (auditoría) la persona que lo realiza (pentester) no solo descubre posibles vulnerabilidades que podrían ser usadas por atacantes, sino que las explota hasta donde sea posible para identificar, (De la Torre et al., 2018).

En la siguiente sección se analizan las bibliografías existentes de las diferentes metodologías de testeo de redes de datos y se define como resultado la metodología de detección de errores de seguridad y vulnerabilidades que más se utilice en los diferentes trabajos analizados y por último se presentan las conclusiones de este trabajo.

Materiales y Métodos

En este trabajo se empleó la metodología de Revisión Sistemática que se caracterizan por tener y describir el proceso de elaboración transparente y comprensible para recolectar, seleccionar, evaluar críticamente y resumir toda la evidencia disponible con respecto a la efectividad de un tratamiento, diagnóstico, pronóstico, esta consta de tres etapas: definición de la búsqueda, ejecución de la búsqueda y discusión de los resultados, (Carrizo & Moller, 2018)**.**

Definición para la búsqueda

En primer lugar, se realizó una investigación de las metodologías más utilizadas para el testeo de redes, para esto se definieron las siguientes palabras claves: metodología, testeo, redes de internet, vulnerabilidades. Las mismas que se usaron base de datos de búsqueda avanzada tales como Google Scholar, Scielo, Dialnet, IEEE, etc. Se logró identificar 30 artículos relacionas de los cuales sólo 18 especificaban una metodología utilizada para el testeo de redes que en la tabla 5 se mencionan.

Ejecución de la búsqueda

A continuación, se muestra los campos que se tomaron en cuenta para la extracción de información de los 18 artículos seleccionados.

La tabla 1 muestra los campos que se tomaron en cuenta para la extracción de los datos. Los atributos más relevantes para el análisis fueron: metodología de testeo, año de publicación, herramientas utilizadas, tipo de metodología.

Tabla 1. Campos definidos en la extracción de datos.

Campos	Descripción
Tema	Nombre de Artículo
Año	*Año de publicación del artículo*
Autor(es)	Nombre del autor(es) del artículo
Metodología de testeo	Nombre de la metodología utilizada para el testeo de redes
Herramienta	Nombre de la herramienta utilizada para el testeo de redes
Tipo de Metodología	Metodología libre o de pago
Servicio y pruebas de proceso	DNS, IMAP, POP, FTP, HTTPS y servicios de Windows.

Análisis de la información

Una vez seleccionada y clasificada la información, se analizaron los datos obtenidos de los 18 artículos escogidos, en los cuales se obtuvo resultados de la frecuencia de uso de las diferentes metodologías de testeo, herramientas de testeo y clasificación por tipo de metodología. Se identificó también aquella con más periodicidad de uso en los últimos años.

Resultados y Discusión

Análisis con respecto a la metodología que se utilizaron en los diferentes artículos

Con los artículos detallados, se logró hacer un análisis de las diferentes metodologías de testeo planteadas por los autores en cada uno de los trabajos desarrollados, donde de los 30 artículos sólo 18 de ellos plantearon una metodología de testeo de redes de datos.

En el análisis se identificó el año de publicación, tema tratado, la metodología usada o planteada, el tipo de metodología usada (abierta o de pago), el Servicio y pruebas de proceso. Con los datos recopilados se pudo evidenciar la frecuencia de usó de las metodologías en el testeo de redes de datos.

A continuación, en la Tabla 2, se muestran las metodologías que fueron identificadas en los 18 artículos analizados:

Tabla 2. Metodologías identificadas

Metodologías	Tipo de Metodologías (libre/pago)	N°
Metodología OSSTMM	Abierta	12
Métodología OWASP	Abierta	1
Métodología Mdrvi 1.0	Abierta	1
Metodología Ataque de arboles	Pago	1
Metodología T.A.M.A.R.A	Pago	1
Metodología para detección de vulnerabilidades en redes de datos	Pago	1
Pentest	Pago	1

En la tabla 3 se muestran las herramientas de testeo que fueron identificadas en los artículos:

Tabla 3. Herramientas identificadas

Herramientas de Testeo	Tipo de Herramientas (Abierta/pago)
Nessus	Abierta
Zenmap	Abierta
Robtex	Pago
Selenium	Abierta
Kaly-linux	Abierta
Backtrack	Pago

Las herramientas de testeo analizadas en los artículos encontramos tres herramientas libres mientras que las de pago también encontramos tres hallando en total 6 herramientas de testeo de redes de datos.

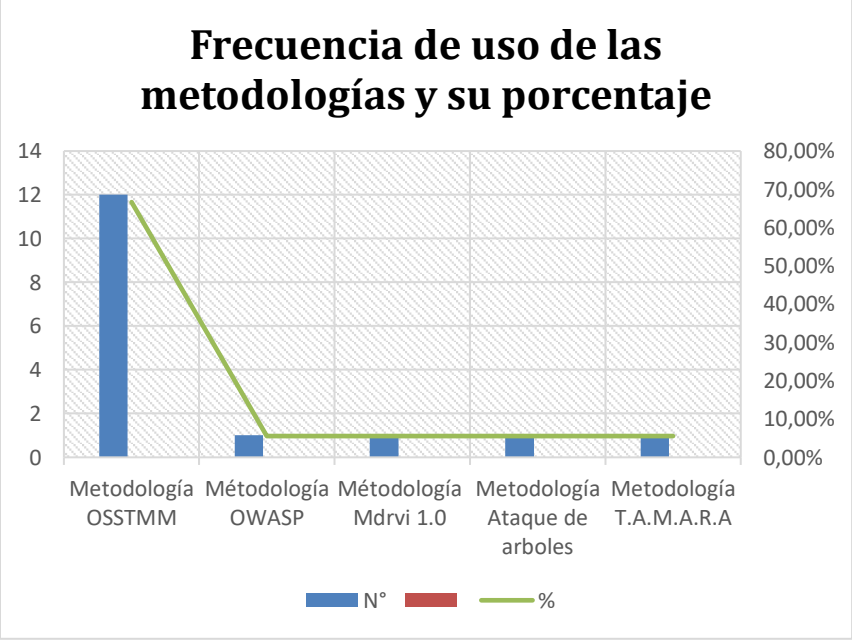
En la tabla 4 se muestras el número de metodologías analizadas en los diferentes artículos y el porcentaje.

Tabla 4. Frecuencia de uso de las metodologías y su porcentaje.

Metodología	N°	%
Metodología OSSTMM	12	66,67%
Metodología OWASP	1	5,56%
Metodología Mdrvi 1.0	1	5,56%
Metodología Ataque de arboles	1	5,56%
Metodología T.A.M.A.R.A	1	5,56%
Metodología para detección de vulnerabilidades en redes de datos	1	5,56%
Pentest	1	5,56%
Total	**17**	**100%**

De acuerdo con el análisis realizado se identificaron el número de metodologías encontradas en cada artículo analizado donde la Metodología OSSTMM (Open Source Security Testing Methodology Manual) se encontró en 12 artículos con un 66.67 % siendo la metodología más utilizada en el testeo de redes de datos.

Gráfico 1. Frecuencia de uso de las metodologías y su porcentaje



Como se puede observar en el gráfico 1, la metodología más utilizada es la OSSTMM (Open Source Security Testing Methodology Manual) según la literatura revisada, esta metodología permite probar la seguridad operativa de las ubicaciones físicas, las interacciones humanas y todas las formas de

comunicación, como inalámbrica, por cable, analógica y digital, encontrándose publicado bajo la licencia Creative Commons 3.0; permitiendo la libre utilización y distribución, (Sendón-Varela et al., 2021).

De acuerdo con sus autores Herzog & Barceló (2010) el Manual de la Metodología Abierta de Pruebas de Seguridad OSSTMM proporciona un camino para realizar pruebas o auditorías exhaustivas de seguridad, con un enfoque abierto. Esta metodología puede ser aplicada en conjunto con estándares y normativas reconocidas a nivel mundial o local, y actualmente se encuentra vigente la versión 3.0 de la misma.

La metodología OSSTMM es una de las más utilizadas porque se adapta a cualquier tipo de organización y es de código abierto, además se encarga de testear toda la seguridad en las comunicaciones de redes de datos, donde la interacción se lleva a cabo mediante un cable establecido y líneas de la red cableadas, así mismo esta emite resultados objetivos y cuantitativos del testeo.

Tabla 5. Análisis de los artículos

Tema	Autor(es)	Metodología de testeo	Herramienta	Tipo de Metodología	Servicio y pruebas de proceso
Metodología abierta de testeo en Seguridad NESSUS	(Chicaiza, 2019)	OSSTMM	Nessus	libre	DNS
Pruebas De Intrusión Y Metodologías Abiertas	(Pinzon et al., 2013)	OSSTMM	Nd	libre	DNS
Metodología para el análisis de vulnerabilidades	(Serrato, 2016)	OSSTMM	Robtex	libre	DNS
Propuesta De Una Metodología De Pruebas De Penetración Orientada A Riesgos	(Alvarez & Gamboa, 2018)	OSSTMM	Nd	libre	Nd
Análisis comparativo entre distintas metodologías para la realización de auditorías de seguridad informática, aplicando el Proceso Analítico Jerárquico (AHP)	(Sendón-Varela et al., 2021)	OSSTMM	Nd	libre	Nd
Análisis Y Pruebas De Niveles De Seguridad De La Información	(Quintana, 2018)	OSSTMM	Nessus	libre	Nd

Basados En Las Guías Del Osstmm V3					
Attack Net Penetration Testing	(McDermott , 2000)	Ataque de arboles	Nd	Pago	Nd
Pentesting	(De la Torre et al., 2018)	OWASP	Nd	libre	Nd
Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux	(Roba-Iviricu et al., 2016)	OSSTMM	Kali-Linux	libre	Nd
Metodología para la Detección de Vulnerabilidades en Redes de Datos	(Franco et al., 2012)	Metodología para detección de vulnerabilidades en redes de datos	Nd	Pago	DNS
Análisis de estrategias de gestión de seguridad informática con base en la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la intranet de una Institución de Educación Superior.	(Mera & Benavides, 2018)	OSSTMM	Nd	libre	Nd
Pentesting Empleando Tecnicas De Ethical Hacking En Redes Ipv6	(Rojas-Osorio et al., 2016)	Pentest	Nd	libre	DNS
Metodología de seguridad en REDES T.A.M.A.R.A: Testeo, análisis, manejo de redes y acceso	(Viteri et al., 2016)	T.A.M.A.R.A	Nd	Pago	DNS
Diseño De Metodología Para El Diagnóstico De Seguridad A Las Redes De Datos De Etecsa	(López, 2016)	OSSTMM	Backtrack	libre	Nd
Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001	(Solarte-Solarte et al., 2015)	OSSTMM	Nessus	Libre	Nd
Propuesta De Una Metodología De Detección Y Respuesta A Vulnerabilidades Para Mejorar La Seguridad En La Red De Datos.	(Conya, 2018)	Mdrvi 1.0	Nd	Pagada	Nd

Caso Práctico: Intranet De La Organización No Gubernamental Worl Vision Ecuador					
Estudio de Metodologías para la Implantación de la Seguridad en Redes Inalámbricas de Área Local	(Méndez, 2006)	OSSTMM	Nd	Libre	Nd
Instrumento para la auditoría técnica de seguridad informática en pequeños proveedores de Internet	(Navia & Zambrano, 2021)	OSSTMM	libre	Backtrack	Nd

Fuente: Los autores

De acuerdo con la revisión bibliográfica de los artículos se pudo determinar que la metodología de código abierta OSSTMM es la que más se utiliza si de testeo de redes se habla ya que da la facilidad que cualquier persona realice pruebas de seguridad y que contribuya con nuevas ideas de seguridad que sean mejores que las existentes. Además, desde el año 2006 según la investigación realizada se utiliza la metodología de testeo OSSTMM hasta la actualidad siendo esta la más utilizada durante los últimos 15 años. En el Servicio y pruebas de proceso se logró observar en seis artículos analizados en los cuales hace referencia a la prueba de proceso mediante DNS.

Discusión de los resultados

En esta etapa, se analizaron los datos obtenidos de los 18 artículos, en los cuales se obtuvo resultados de cuál es la metodología de testeo de redes físicas que se utilizan en este caso es la metodología de testeo de código abierto OSSTMM. Estos datos mencionados de los artículos ayudaron a identificar la metodología, y el tipo de metodología que es (abierta o de pago).

La OSSTMM, es una metodología actualizada constantemente por la comunidad. Esta es de complejidad media y de fácil implementación en aquellas organizaciones que inician procesos de reestructuración de los modelos de seguridad informática, como las del sector pesquero industrial del cantón Manta, presentando formatos y métricas, no probabilísticas como en MAGERIT, sino más bien, operativas y reales. Como resultado se pudo corroborar que la alternativa más acorde a las características del sector es OSSTMM, debido a su complejidad media y de fácil implementación en aquellas organizaciones que inician procesos de reestructuración de los modelos de seguridad informática (Sendón-Varela et al., 2021).

En el artículo de Navia & Zambrano (2021) presenta una herramienta de ayuda para realizar auditorías de seguridad informática en pequeños ISP, basándose en la metodología OSSTMM. Esta herramienta busca ser una guía al momento de cuantificar el nivel de seguridad de este tipo de organizaciones, mediante el cálculo de RAVs.

En la investigación de Franco et al.,(2012) que tiene como tema "Metodología para la Detección de Vulnerabilidades en Redes de Datos", se desarrollaron diferentes fases llamadas reconocimiento, escaneo de puertos y enumeración de servicios, y escaneo de vulnerabilidades, cada una de las cuales es soportada por herramientas de software. Los resultados de cada fase suministran datos necesarios para la ejecución de las etapas. Con el fin de validar la utilidad de la metodología propuesta se llevó a cabo su implementación en la red de datos de la Universidad de Cartagena en Colombia, encontrando diferentes tipos de vulnerabilidades. Finalmente apoyándose en los resultados obtenidos, se encontró que la metodología propuesta es de gran utilidad para detectar vulnerabilidades en redes de datos, lo que demuestra su importancia para el área de la seguridad.

Conclusiones

Este artículo científico de revisión bibliográfica permitió analizar las diferentes metodologías de testeo de redes y si eran libres o de pago basándonos en la literatura consultada. La metodología OSSTMM, es la más usada entre las metodologías de testeo de redes y análisis de vulnerabilidades, siendo esta de uso libre y permite evaluar riesgo, que ayudan diferenciar y clasificar los diferentes problemas de seguridad de las organizaciones, así mismo permite a los profesionales contribuir con nuevas seguridades basadas en la metodología.

Las herramientas de testeo que más se utiliza en esta revisión bibliográfica es Nessus mencionándola en tres artículos, esta herramienta es gratuita y permite evaluar, identificar y reparar vulnerabilidades de manera rápida así mismo realiza un escaneo de hasta de 16 IP.

De acuerdo con la revisión, en los últimos 5 años las metodologías de testeo de redes han sido muy acogida por las organizaciones resguardando sus datos mediante escaneos constantes de vulnerabilidades existente ya que los riegos de ataque informáticos han incrementado de manera exponencial por los ciberdelincuentes.

Referencias

Alvarez, K., & Gamboa, A. (2018). *Propuesta de una Metodología de Pruebas de penetración orientada a riesgos*. *c*, 1–25.

Carrizo, D., & Moller, C. (2018). Estructuras metodológicas de revisiones sistemáticas de literatura en Ingeniería de Software: un estudio de mapeo sistemático. *Ingeniare. Revista Chilena de Ingeniería*, *26*, 45–54. https://doi.org/10.4067/s0718-33052018000500045

Chicaiza, V. (2019). *Metodología abierta de testeo en Seguridad NESSUS Open NESSUS Security Testing Methodology*. 35–41. http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index

Conya, R. E. (2018). *Propuesta De Una Metodología De Detección Y Respuesta A Vulnerabilidades Para Mejorar La Seguridad En La Red De Datos. Caso Práctico: Intranet De La Organización No Gubernamental Worl Vision Ecuador*.

De la Torre, C., De la Torre, M., De la Torre, A., & De la Torre Micaela. (2018). *Pentesting* (Vol. 148, pp. 148–162). https://www.scprogress.com/cinco/

Franco, D., Perea, J., & Puello, P. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. *Informacion Tecnologica*, *23*(3), 113–120. https://doi.org/10.4067/S0718-07642012000300014

Herzog, P., & Barceló, M. (2010). *OSSTMM 3 – The Open Source Security Testing Methodology Manual* (Vol. 148). https://www.isecom.org/research.html#content5-a0

López, A. (2016). Diseño De Metodología Para El Diagnóstico De Seguridad A Las Redes De Datos De Etecsa. In F. T. de la I. y Software & G. T. P. del Río (Eds.), Informacion Tecnologica. http://www.bvs.hn/cu-2007/ponencias/SEG/seg037.pdfd e e t e c s a. In F. T. de la I. y Software & G. T. P. del Río (Eds.), *Informacion Tecnologica*. http://www.bvs.hn/cu-2007/ponencias/SEG/seg037.pdf

McDermott, J. (2000). Attack net penetration testing. *Proceedings of the 2000 Workshop on New Security Paradigms - NSPW '00*, 15–21. https://doi.org/10.1145/366173.366183

Méndez, J. (2006). *Estudio de Metodologías para la Implantación de la Seguridad en Redes Inalámbricas de Área Local*.

Mera, D., & Benavides, V. M. (2018). *Análisis de estrategias de gestión de seguridad informática con base en la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la intranet de una Institución de Educación Superior.* 55.

Navia, M., & Zambrano, W. (2021). *Introducción OSSTMM y su difusión Estructura de OSSTMM*. 119–128.

Pinzon, L., Talero, M., & Bohada, J. (2013). Intrusion Test and Open Source. *Revista Ciencia, Innovacion y Tegnologia (RCYIT)*, *1*(Enero-Diciembre), 25–38.

Quintana, O. G. (2018). *ANALISIS Y PRUEBAS DE NIVELES DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN LAS GUIAS DEL OSSTMM v3*. 11. http://files/470/Quintana y Oswaldo - ANALISIS Y PRUEBAS DE NIVELES DE SEGURIDAD DE LA I.pdf

Roba-Iviricu, L., Vento-Alvarez, J., & García-Concepción, L. (2016). Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux. *Revista Avances*, *18*(4), 334–344.

Rojas-Osorio, J., Medina-Cardenas, Y., & Rico-Bautista, D. (2016). Pentesting empleando técnicas de Ethical Hacking en redes IPv6. *Revista Ingenio*, *11*(1), 79–96. https://revistas.ufps.edu.co/index.php/ingenio/article/view/2096/3126%0Ahttps://revistas.ufps.edu.co/index.php/ingenio/article/view/2096

Sendón-Varela, J., Herrera-Tapia, J., Fernández-Capestany, L., Cruz-Felipe, M., Chancay-García, L., & García-Quilachamín, W. (2021). Análisis comparativo entre distintas metodologías para la realización de auditorías de seguridad informática, aplicando el Proceso Analítico Jerárquico (AHP). *Revista Ibérica de Sistemas e Tecnologias de Informação*, *40*, 352–367.

Serrato, G. (2016). Metodología para el análisis de vulnerabilidades. *Tecnología Investigación y Academia*, *4*(2), 20–27.

Solarte-Solarte, F. N., Enriquez-Rosero, E. R., & Benavides-Ruano, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), 497–498. http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Viteri, M. F., Orellana, P., & Marin-Garcia, I. (2016). *Metodología de Seguridad en Redes T . A . M . A . R . A : Testeo , Análisis , Manejo de Redes y Acceso Resumen*. *1*.

CC BY NC ND