REVISTA CIENTIFICA AVANCES ISSN 1562-3297 RNPS 1893

Editada por el Centro de Información y Gestión Tecnológica. CIGET Pinar del Río

Vol. 18, No.4, octubre-diciembre, 2016

ARTÍCULO ORIGINAL

Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux

Methodology for Detecting Vulnerabilities in data networks using Kali Linux

Luis Rolando Roba Iviricu[1], José Raúl Vento Alvarez[2], Luis Ernesto García Concepción[3]

[1]Ingeniero en Telecomunicaciones. Oficina de Seguridad para las Redes Informáticas (OSRI), Pinar del Río, Cuba. Alameda No. 11A Teléfono: 48755371. E-mail: luis.rolando@osri.gob.cu
[2]Doctor en Ciencias en Telecomunicaciones. Universidad de Pinar del Río "Hermanos Saíz ", Pinar del Río, Cuba. José Martí final No. 270. Teléfono: 4875 5031 / 4877 9666 E- mail: vento@upr.edu.cu
[3]Máster en Ciencias en Telecomunicaciones. Universidad de Pinar del Río "Hermanos Saíz ", Pinar del Río, Cuba. José Martí final No. 270. Teléfono: 4875 5031 / 4877 9666 E- mail: lernesto@upr.edu.cu

RESUMEN

El objetivo principal de este trabajo fue diseñar una metodología para la detección de vulnerabilidades en redes de datos. Para esto se desarrollaron diferentes etapas: valoración, ejecución e informe, cada una de las cuales es soportada por diferentes herramientas incluyendo los software(s) utilizados. Los resultados de cada etapa suministran datos necesarios para la ejecución de la investigación. Con el fin de validar la utilidad de la metodología propuesta se llevó a cabo su implementación en la red de datos perteneciente a la Unidad Empresarial de Base Logística de la Empresa de Construcción y Montaje de Pinar del Río, encontrando diferentes tipos de vulnerabilidades, apoyándose en los resultados obtenidos demostramos 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 informática.

Palabras clave: Detección de vulnerabilidades, Enumeración de servicios, Escaneo de puertos, Seguridad informática.

ABSTRACT

The main objective of this work was to design a methodology for detecting vulnerabilities in data networks. Appraisal, and report execution, each of which is supported by various tools including software used: for this different stages were developed. The results of each stage provide data necessary for the execution of the investigation. In order to validate the usefulness of the proposed methodology was carried out implementation in the data network belonging Base Business Unit Logistics Company Construction and Installation of Pinar del Rio, finding different types of vulnerabilities, based on the results obtained was found that the proposed methodology is useful to detect vulnerabilities in data networks, demonstrating its importance to the area of computer security.

***Key words*:** Vulnerability detection, Enumeration of services, Port scanning, Security.

INTRODUCCIÓN

Para finales del siglo XX, los Sistemas Informáticos se convirtieron en las herramientas más poderosas capaces de materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial: "Los Sistemas de Información", que según autores como Peralta (2008) lo definen como el conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Teniendo muy en cuenta el equipo computacional necesario para que el sistema de información pueda operar y el recurso humano que interactúa con el mismo.

Ligado al sostenimiento de estos sistemas donde la información se socializa en función de los objetivos de las entidades surge el concepto de seguridad, aplicada tanto a las telecomunicaciones o a la informática, con el fin de la protección de la información y de los sistemas que permiten el acceso, uso, divulgación o destrucción no autorizada de ella.

Existen entonces dos términos usados con frecuencia: La Seguridad de la Información y Seguridad Informática, que aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la Información; cabe resaltar que se diferencian principalmente en el enfoque, en las metodologías utilizadas y en las zonas en las que se concentran.

Es común cuando se habla de estos términos que se confundan los conceptos y asocien con lo mismo. Según Canon citado por López Santoyo (2015) plantea que: la seguridad informática es la disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que establecen la forma de actuar y asegurar las situaciones de fallas

parciales o totales, cuando la información es el activo que se encuentra en riesgo, refiriendo también que la seguridad de la información es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

Con el propósito de alinear las acciones dirigidas al sostenimiento de estos sistemas, se investigó un grupo de estándares y modelos que sirven como ayuda o procedimiento relacionado de alguna forma u otra con la seguridad a nivel informático o de telecomunicaciones, entre ellos tenemos los estándares referidos por López Santoyo (2015), Penetration Testing Execution Standard (PTES) (2014); para la realización de pruebas de penetración y Open Web Application Secutiry Project (OWASP) (2016), la organización MITRE (2016), The Common Weakness Enumeration (CWE) y Red Hat (2016), The Open-source Security Content Automation Protocol (OpenSCAP) de la Comunidad, todas ellas determinan y catalogan las vulnerabilidades en los software. Para la verificación de la seguridad en redes inalámbricas sirve de referencia Tarascó (2013) con Open Wireless Security Assessmennt Methodology (OWISAM). Con el fin de estandarizar la seguridad de la información y su correcta gestión y organización existen las normas ISO 17799/ISO 27002 e ISO/IEC 27001 dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización. En Cuba como marco regulatorio de la actividad en las Tecnología de Informática y las Comunicaciones (TIC) se cuenta con la Resolución 127/07 del Ministerio de las Comunicaciones (MINCOM), que tiene por objeto establecer los requerimientos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país.

Dentro de las metodologías comprendidas para la realización de auditorías informáticas se destaca Open Source Security Testing Methodology Manual (OSSTMM), la que provee herramientas con el objetivo de realizar una medición precisa de la seguridad a nivel operacional. Es administrada por el Instituto de Seguridad y Metodologías Abiertas (ISECOM por sus siglas en inglés), la misma es diseñada para ser consistente, repetible y como un proyecto de fuente abierta, permitiéndole a cualquier profesional de la especialidad contribuir con ideas para realizar pruebas de seguridad más precisas, concretas y eficientes, instruyéndonos la misma para el para el desarrollo de nuestra investigación, ya que constituye uno de los estándares profesionales más completos y utilizados en auditorías de Seguridad a Tecnologías de Informática y Comunicaciones (TICs) en el mundo.

Como se puede apreciar y ante los grandes avances en materia tecnológica, son disímiles los distintos sistemas y programas usados en las instituciones ya sea a nivel de servidores como de usuarios finales; por lo que la seguridad ha tenido que ir a la par de este desarrollo, tomando importancia la gestión de las vulnerabilidades, poniéndose de manifiesto el incremento en la amenaza de asaltos cuando se instalan y configuran

aplicaciones de diversa procedencia, utilizándose virtualmente en cualquier sistema operativo disponible, hay autores como González Maturín que al referirse a los problemas del control en este tipo de entornos; plantea que las empresas tienen necesidades cada día más complejas y eso muchas veces implica poner a personas que realmente saben algo a hacer cosas para las que no están capacitadas. Es ahí donde empiezan a producirse problemas informáticos en la empresa. Problemas que se han ido acumulando con el tiempo y de los que ni siquiera son conscientes.

En el desarrollo de este trabajo investigativo se han revisado varios autores que han profundizado en el proceso de elaboración de una metodología que permita la detección oportuna de estas vulnerabilidades, podemos citar a Romero et al. (2009) ellos presentan una herramienta metodológica para identificar los activos relevantes en un proceso de identificación de riesgo en aplicaciones web, para soportar el instrumento metodológico propuesto se implementa un caso de estudio y se realiza un análisis cuantitativo y cualitativo del mismo; sin embargo, este trabajo se limita a la identificación de activos expuestos a riesgos y no hace proposiciones para la detección del peligro al que estos están expuestos, es decir, no propone mecanismos prácticos para la detección de vulnerabilidades.

Pfleeger y Ciszek (2008), presentan una metodología de cuatro pasos con el propósito de ayudar a las organizaciones a evaluar los activos relevantes a ser protegidos, pero sin precisar las técnicas para la evaluación de la seguridad de dichos activos, por lo que da lugar a proteger elementos carentes de riesgo.

Xinlan et al. (2010) evalúan el riesgo de seguridad de la información, basada en un análisis matemático y no aporta herramientas para evaluar el grado de vulnerabilidad de un activo dentro de una organización.

Ruiz et al. (2009) proponen una metodología de cinco pasos para ayudar a disminuir los problemas de seguridad en las pequeñas y medianas empresas mexicanas, no proporcionando la misma los mecanismos concretos para la detección de vulnerabilidades y limita su alcance a cierto tipo de organizaciones de un país concreto. Watanabe et al. (2010) plantean que existe como problema la presencia de vulnerabilidades en redes de datos, causando grandes pérdidas a organizaciones e individuos en la actualidad, por lo que se han desarrollado diferentes metodologías para la detección de las mismas.

En el presente artículo se persigue como objetivo diseñar una metodología que se pueda aplicar a cualquier tipo de organización con independencia de la entidad, lugar o país en el que se encuentre, para poder brindar y mejorar los ambientes de seguridad a un bajo costo, dándole un enfoque social, permitiendo la eficacia y eficiencia en la detección de vulnerabilidades en los distintos controles que se realizan, para lograr al final de este proceso un resultado integral que refleje con claridad los problemas en materia de vulnerabilidades detectadas; lográndose con esto elevar la confidencialidad, integridad y disponibilidad de los datos críticos o sensibles que se manejan y establecer la prioridad de

eliminar las vulnerabilidades detectadas o mitigar su impacto ante la ocurrencia de incidentes de seguridad.

MATERIALES Y MÉTODOS

Se realizó una investigación acción con el objetivo de diseñar una metodología para la detección de vulnerabilidades en las redes de datos utilizando Kali-Linux. Con el fin de probar en la práctica la metodología creada, se aplicó la misma en la Unidad Empresarial de Base Logística de la Empresa de Construcción y Montaje de Pinar del Río, donde a partir del sistema propuesto y las herramientas Nmap, Wireshark y Nessus, se realizó la búsqueda de vulnerabilidades en la red de datos de la citada entidad. Para el desarrollo de nuestra investigación se tomó como referencia la metodología OSSTMM, adaptando la misma a nuestras condiciones, definiendo también nuestras herramientas y sistemas propios para su implementación.

La misma consta de tres etapas: 1) Valoración 2) Ejecución 3) Informe. Detallando en cada una de ellas las acciones que se llevaron cabo; la *figura* muestra el orden secuencial de la metodología.

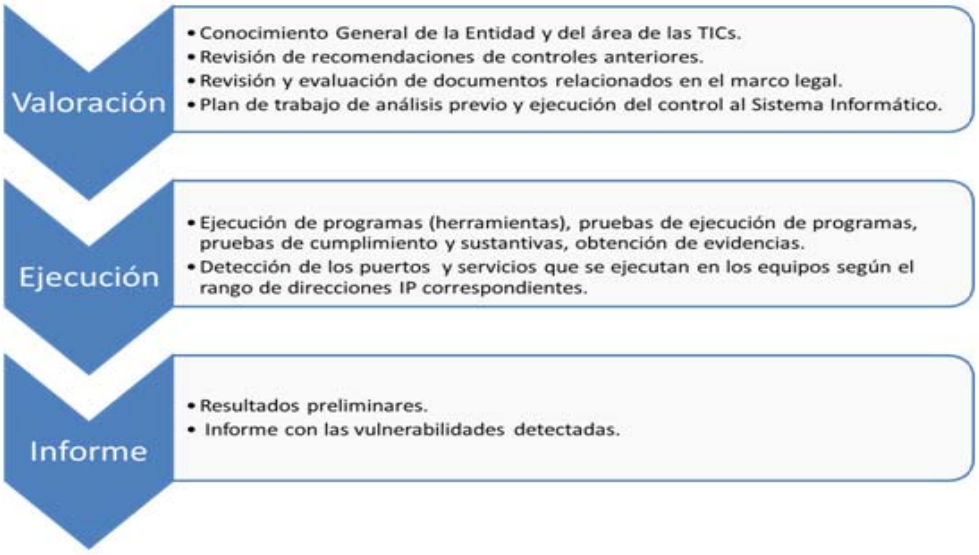

Figura 1. Esquema de la metodología para la detección de vulnerabilidades en redes de datos.

Fuente: Elaboración propia.

Etapa 1. Valoración

Esta etapa se enfocó en conocer, comprender, analizar la misión, visión y el organigrama de la entidad, recursos humanos , productos y servicios que brida, así como la relación que mantiene con otras organizaciones y del conocimiento de la función del área de tecnología de información y comunicaciones principalmente en aspectos como: Arquitectura organizacional, ideas rectoras, objetivos y metas operativas, instrumentos administrativos, organización y función, procesos, productos y/o servicios, insumos y el entorno de la

función de tecnología de información y comunicaciones (clientes), aplicando procedimientos generales tales como:

- Revisar y evaluar si la función de las TICs está alineada con la misión, visión, valores, objetivos y estrategias de la organización y deberá revisar el desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.
- Verificar la gestión que se tiene sobre el Sistema Informático a partir de los máximos responsables en la entidad y demás actores, relacionado con el Acuerdo 6058 del CECM, a través del cual se valorará la eficacia de los recursos de las TICs y el desempeño de los procesos administrativos.
- Revisar y evaluar el ambiente de control de la organización.
- Comprobar las áreas físicas de las TICs, con el propósito de evaluar si está en condiciones para su operatividad.
- Revisar las funciones de cada uno de los responsables (Adiministradores, Técnicos y otros especialistas) para comprobar si estos cuentan con herramientas y condiciones necesarias para realizar su trabajo y de la optimización de los recursos tecnológicos.
- Verificar y analizar si el Plan de Seguridad Informática (PSI) se encuentra acorde con el marco legal establecido en nuestro país a través de la Resolución 127/2007 del MINCOM.

Esta etapa se apoyó en la aplicación de cuestionarios dirigidos a: Directivos, Informáticos, Departamentos de recursos humanos y Usuarios (Anexos 1, 2, 3, 4); en la cual una vez obtenido los resultados sirvieron de valoración en cuanto a la preparación del personal en el sostenimiento del sistema; los cuales se pueden aplicar indistintamente a la red que sea objeto de análisis.

Etapa 2: Ejecución

En esta segunda etapa se inicia un proceso que comprende desde escaneo de puertos y enumeración de servicios, hasta el análisis específico de vulnerabilidades. Por lo que se comienza con el descubrimiento de todos los medios informáticos conectados, con el fin de tener la lista lo más completa posible de cada uno de los mismos. Con el resultado de este proceso podremos saber la función que cumplen los diferentes dispositivos dentro de la red y su naturaleza (servidores, enrutadores, equipos inalámbricos o nodos terminales). Soportando el trabajo en herramientas software implementadas en el sistema utilizado en nuestra investigación Kali-Linux, una distribución con un conjunto de más de 300 herramientas ya preinstaladas para propósitos de pentesting (Pruebas de Penetración).

A través de herramientas de análisis de redes como Ethereal y Wireshark, se pudo realizar la intercepción de los mensajes intercambiados entre los dispositivos de red (Sniffeo de red), inventario de activos a través de herramientas como Nmap para el escaneo de IPs/puertos e identificación de Sistemas Operativos/Aplicaciones que se encuentran obsoletas o con configuraciones incorrectas.

Una vez concluido este proceso se procedió al escaneo de vulnerabilidades, utilizando para ello el software Tenable Nessus instalado y actualizado previamente a la realización del control a la entidad. Esta herramienta utiliza el repositorio de vulnerabilidades que se encuentran en las bases de datos de la National Vulnerability Database (NVD); con sus estándares de Common Vulnerabilities and Exposures (CVE)y Common Vulnerability Scoring System (CVSS), con lo que se garantiza que las vulnerabilidades analizadas son todas las reportadas hasta la fecha del análisis, aquí nos concentramos en detectar los riesgos potenciales a los que se encuentran expuestos los equipos dentro del segmento de red obtenido anteriormente. Ingresamos el equipo, conjunto de equipos o segmento de red a escanear, los resultados de esta herramienta son a través de un reporte individual por host de las vulnerabilidades detectadas en cada uno de ellos.

Etapa 3: Informe

En el informe se reflejan las amenazas y vulnerabilidades que presenta el sistema informático de la entidad en correspondencia con los artículos violatorios del marco legal y además constituye una herramienta de trabajo para los autocontroles sistemáticos que deben de programarse para ir solucionando cada una de ellas.

Teniendo en cuenta que un control a las TICs consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestreo) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos.

Cabe aclarar que las personas que hagan uso de esta metodología, tales como administradores de red, profesionales de seguridad informática, etc. deben tener conocimientos básicos de arquitecturas de redes, configuración de sistemas operativos y dispositivos de red, con el fin de no crear malos entendidos respecto a las recomendaciones y los pasos a seguir.

RESULTADO Y DISCUSIÓN

La metodología anteriormente expuesta ha sido aplicada en la red de datos de la Unidad Empresarial de Base Logística de la Empresa de Construcción y Montaje de Pinar del Río, arrojando los siguientes resultados:

Etapa 1: Valoración (recolección de información). Mediante la ejecución de esta etapa se detectaron las siguientes deficiencias:

1. Se determinó el estado y gestión del sistema informático de la entidad, su desarrollo, gestión y actualización periódica del mismo.

2. Evaluación del Plan de Seguridad Informática, realizando recomendaciones para una correcta elaboración siempre aclarando su elaboración a través de la metodología aprobada por nuestra oficina (OSRI).

3. Al evaluar los resultados de los cuestionarios aplicados encontramos que: más de un 40% de los trabajadores de la entidad no tenían conocimiento de la base legal vigente en los temas de seguridad informática, se verificó que los Directivos no participaban en la elaboración del Plan de Seguridad Informática; a pesar de que en los consejos de dirección se trataban estos temas. No utilizaban las herramientas puestas a su disposición para los autocontroles al sistema informático implementado.

En el departamento de Recursos Humanos en un 80% no se realizaba la correcta selección del personal encargado del sistema informático, encontrándose en el 100% de las verificaciones realizadas no se tenían plasmados planes de capacitación con respecto a seguridad informática. En las entrevistas realizadas a los informáticos en el 100% de ellos no contaban con la conectividad suficiente para la realización de su trabajo, además de tener una obsolescencia tecnológica e insuficiente personal para llevar la actividad.

Con respecto a los usuarios en un 25% no conocían sus deberes y derechos en cuanto al uso de las TICs, además de que un 47% refirió no estar capacitado en el uso de estas tecnologías.

Etapa 2: Ejecución

Es importante anotar que no se muestran los resultados detallados del caso de estudio, para proteger la integridad de la red de datos evaluada.

1. Verificado el segmento de red, para comprobar todos los host activos en el momento del análisis de la red. Se determinaron servidores críticos y PCs dentro del segmento de red para realizar el posterior escaneo de vulnerabilidades.

2. Determinamos los sistemas operativos de los servidores encontrados: PROXMOX y Windows Server 2003. Se Recomendó en uno la actualización hacia versión superior y en el otro la sustitución del mismo por no contar con soporte de actualizaciones.

3. Determinados PCs con Windows XP, el cual es obsoleto sin soporte de actualizaciones, se recomendó en los casos más críticos por la información que se procesaba en los mismos su sustitución inmediata.

4. Se tabularon las IPs que presentaron servicios críticos con el objetivo de realizar una búsqueda de vulnerabilidades y otras cuestiones que pueden amenazar su seguridad.

5. Al realizar el análisis se detectó que el 100 % de los servidores presentó vulnerabilidades críticas (requieren atención inmediata, ya que son fáciles de aprovechar por parte de los atacantes para obtener control total sobre el sistema) y altas (son más difíciles de explotar que las anteriores y no proveen el mismo nivel de acceso).

6. Se pudo constatar que uno de los servicios web presentaba usuario y contraseña por defecto " admin", "admin".

7. Además se detectaron en el 100% de las PCs analizadas, vulnerabilidades medias y moderadas.

8. Se logró establecer una categorización de las vulnerabilidades encontradas con relación a los servicios afectados por las mismas.

Etapa 3: Informe

Al finalizar el análisis se presentó un informe detallado con todas las deficiencias encontradas. En el mismo se desglosan los artículos violados de la Resolución 127/07 del MINCOM, y brinda a través de la discusión una serie de explicaciones de cada uno de los problemas hallados y en cómo estos afectan el cumplimiento de la seguridad informática de la entidad. Como centro del informe se muestran los resultados de las vulnerabilidades encontradas a través del análisis. Cabe señalar que mediante del reporte se categorizan por nivel de riesgo cada una de las vulnerabilidades halladas y se explica cómo cada una de ellas pudiera afectar el correcto funcionamiento del sistema. Una vez expuesto estos resultados y realizándose todas las aclaraciones pertinentes se exigió la elaboración de un plan de medias con el propósito de resolver cada una de las dificultades encontradas.

Los resultados obtenidos a través del desarrollo de la investigación coinciden con los previstos en la metodología OSSTMM adaptada a las condiciones del territorio, corroborando su efectividad. Se probó la validez de su implementación con la utilización de la distribución libre Kali-linux y el conjunto de herramientas disponibles, demostrando con ello la factibilidad para su aplicación, manteniendo los estándares de detección y logrando la calidad y eficiencia en la detección de vulnerabilidades en las redes de datos.

Se recalca que el control y la verificación periódica de la seguridad no es una tarea única sino una sistematicidad permanente que tiene que estar integrada a los procesos cotidianos de la estructura institucional, que debe incluir a todas y todos administrativos, prestadores y usuarios de los servicios. Sin estas características esenciales no están garantizados, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

CONCLUSIONES

Este artículo presentó el desarrollo de una metodología para la detección de vulnerabilidades en redes de datos, lo cual favorece la detección periódica de agujeros de seguridad que no reciben la atención adecuada.

La metodología diseñada e implementada proporcionó como resultado el hallazgo de diferentes problemas de seguridad en la entidad, ya que ayudó a encontrar de manera satisfactoria vulnerabilidades críticas, altas y moderadas en servidores que conforman redes de datos, permite la categorización de las mismas, clasificándolas de acuerdo a los servicios afectados, es de gran utilidad y de fácil acceso teniendo un gran impacto en las organizaciones que deseen implementarla.

REFERENCIAS BIBLIOGRÁFICAS

- González Maturín, Y. (2015). *Auditoria de Sistemas. Auditoria Informática dentro de una Institución*. República Bolivariana de Venezuela. Instituto Universitario Politécnico "Santiago Mariño".
- González Pérez, P. (2014). *Ethical Hacking: Teoría y práctica para la realización de un pentesting*. [ISBN: 978-84-617-0576-4].
- Herzog, Pete (2015). Open Source Security Testing Methodology Manual. Institute for Security and Open Methodologies. Recuperado de: http://www.isecom.org/research/
- Kali-Linux (2016). *Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments*. Recuperado de: https://www.kali.org/
- López Santoyo, R. (2015). Metodología PTES (Penetration Testing Execution Standard) Estándar de Ejecución de Tests de Intrusión En: *Propuesta de implementación de una metodología de auditoría de seguridad informática*. Universidad Autónoma de Madrid. Escuela Politécnica Superior. Recuperado de: http://www.pentest-standard.org/index.php/Main_Page
- Ministerio de las Comunicaciones. Oficina de Seguridad para Redes Informáticas OSRI (2007). *Metodología para la gestión de la seguridad informática*. Oficina de seguridad para redes informáticas. p.4-68
- MITRE (2016). *The Common Weakness Enumeration (CWE) Community-Developed Dictionary of Software Weakness Types.* Recuperado de: https://cwe.mitre.org/
- NC-ISO/IEC 27001: 2007 *Tecnología de la Información—Técnicas de Seguridad—Sistemas de Gestión de la Seguridad de la Información—Requisitos*. Oficina Nacional de Normalización. p.41
- Nmap Security Scanner (2016). *Audit your Network Now* Recuperado de: https://nmap.org/>
- Peralta, M. (2008). *Sistemas de Información*. Recuperado de: http://www.econlink.com.ar/sistemas-informacion/definicion
- Pfleeger, S., Ciszek, T., (2008). Choosing a Security Option: Methodology, IT Professional, *The InfoSecure 10*(5), 46-52
- Red Hat (2016). The Open-source Security Content Automation Protocol (OpenSCAP) Audit, Fix and be Merry. Recuperado de: https://www.open-scap.org/
- Romero, B., Haddad, H. y Molero, J.A. (2009). *Methodological Tool for Asset Identification in Web Applications: Security Risk Assessment*, Fourth International Conference on Software Engineering Advances. p.413-418
- Ruiz, J., Ponce, I., Díaz, O., Zavala, J., Zarate, J. y Fuente, S.A. (2009). *MISMA: An Approach to Mexican Information Security Methodology and Architecture for PYMES*, International Conference on Electrical, Communications, and Computers. p.65-68

- Tarascó, Andrés, Tarascó, Miguel, Mallo, Óscar y Fernández Ángel (2013). OWISAM (*Open WIreless Security Assessment Methodology*) Recuperado de:https://www.owisam.org/en/Main_Page
- Tenable network security (2016). *Nessus-vulnerability-scanner* Recuperado de: http://www.tenable.com/products/nessus-vulnerability-scanner >
- Watanabe Takanobu, Cheng Zixue, KansenMizuo y Hisada Masayuki (2010). *A New Security Testing Method for Detecting Flash Vulnerabilities by Generating Test Patterns*. 13th International Conference on Network-Based Information Systems. p. 469-474
- Xinlan Zhang, Zhifang Huang, Guangfu Wei y Zhang Xin, (2010). *Information Security Risk Assessment Methodology Research: Group Decision Making and Analytic Hierarchy Process.* Second WRI World Congress on Software Engineering. p.157-160

Recibido: septiembre 2016
Aprobado: noviembre 2016

Ing. Luis Rolando Roba Iviricu. Oficina de Seguridad para las Redes Informáticas (OSRI), Pinar del Río, Cuba. Alameda No. 11A Teléfono: 48755371. E-mail: luis.rolando@osri.gob.cu