https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121

Vol. 3, Núm. 3. julio-septiembre 2025, págs. 81 - 90

Implementación de Nessus para el análisis de vulnerabilidades en un centro de datos

Información del reporte:

Para citar este reporte técnico:

Pérez Santillán, P. T. (2025). Implementación de Nessus para el análisis de vulnerabilidades en un centro de datos. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginass(81 - 90).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121

Pedro Temachti Pérez Santillán

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

ptsantillan@unam.mx

ORCID: 0009-0000-2626-9073

Resumen

El Centro de Datos de una universidad alberga información vital y sensible, por lo que la identificación y corrección de vulnerabilidades en su infraestructura digital es crucial. La creciente complejidad de las infraestructuras digitales, especialmente con la adopción de tecnologías de virtualización y servicios en la nube, introdujo nuevos desafíos de seguridad, lo que hace indispensable la gestión de vulnerabilidades. Ante la gran cantidad de servidores virtuales y la diversidad de sistemas operativos en ellos, la revisión manual de seguridad ya no es viable, lo que motivó la necesidad de implementar herramientas de automatización para el análisis de vulnerabilidades. Se decidió implementar y evaluar la herramienta Nessus en un entorno de pruebas, con el objetivo de identificar y reportar posibles brechas de seguridad en la infraestructura virtualizada del Centro de Datos de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). La elección de Nessus se fundamentó en su amplio reconocimiento en la industria, así como su uso de manera exitosa en otras instituciones académicas para la detección proactiva y automatizada de vulnerabilidades.

La metodología consistió en instalar Nessus en una máquina virtual, dentro de un clúster de pruebas con el hipervisor Proxmox y diversas máquinas virtuales con algunas brechas de seguridad. Para las direcciones IP objetivo, se realizaron escaneos básicos y con credenciales,

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 82 - 90

y se emplearon los rangos de puertos predeterminados. Los resultados del análisis proporcionaron un número total de vulnerabilidades identificadas y su distribución por nivel de gravedad, lo que permitió realizar recomendaciones específicas para mejorar la seguridad del entorno de pruebas. El análisis demostró la eficiencia de Nessus para identificar y clasificar vulnerabilidades en infraestructuras virtualizadas complejas, en las que múltiples recursos físicos como servidores, almacenamiento y redes han sido virtualizados, resaltando la importancia de un programa continuo de gestión de vulnerabilidades y la adopción de mejores prácticas de seguridad para mejorar la capacidad de la infraestructura digital, con el fin de resistir y recuperarse de incidentes.

Palabras clave:

Nessus, vulnerabilidades, centro de datos, máquina virtual, virtualización, seguridad, ciberseguridad.

Abstract

A university's data center hosts vital and sensitive information, making identification and correction of vulnerabilities in its digital infrastructure crucial. The increasing complexity of digital infrastructures, especially with the adoption of virtualization technologies and cloud services, has introduced new security challenges, making vulnerability management essential. Given the large number of virtual servers and the diversity of operating systems within them, manual security reviews are no longer viable, which motivated the need to implement automated tools for vulnerability analysis. It was decided to implement and evaluate the Nessus tool in a testing environment to identify and report potential security breaches in the virtualized infrastructure of the Data Center of the Directorate General of Computing and Information and Communication Technologies (DGTIC). The choice of Nessus was based on its broad recognition in the industry, as well as its successful use in other academic institutions for proactive and automated vulnerability detection.

The methodology consisted of installing Nessus on a virtual machine within a test cluster running the Proxmox hypervisor and several virtual machines with some security breaches. For the target IP addresses, basic and credentialed scans were performed, and default port ranges were used. The analysis results provided a total number of identified vulnerabilities and their distribution by severity level, allowing for specific recommendations to improve the security of the test environment. The analysis demonstrated Nessus's effectiveness in identifying and classifying vulnerabilities in complex virtualized infrastructures, where multiple physical resources such as servers, storage, and networks have been virtualized. This highlights the importance of an ongoing vulnerability management program and the adoption of security best practices to improve the digital infrastructure's ability to withstand and recover from incidents.

Keywords:

Nessus, vulnerabilities, data center, virtual machine, virtualization, security, cybersecurity.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 83 - 90

1. INTRODUCCIÓN

El Centro de Datos tiene servidores de almacenamiento digitales que albergan una gran cantidad de datos sensibles para el desarrollo de las actividades académicas y administrativas de la Universidad. La identificación y la remediación de vulnerabilidades de esta infraestructura digital es esencial para asegurar los servicios digitales que se ofrecen.

La evolución de las infraestructuras digitales de un Centro de Datos ha llevado a un aumento considerable en su complejidad. La adopción de tecnologías de virtualización, si bien ofrece beneficios en términos de optimización de recursos y flexibilidad, también introduce nuevos desafíos de seguridad. La gestión de la seguridad, en entornos con múltiples hipervisores, requiere conocimientos especializados de cada una de las herramientas utilizadas. Existen estudios que abordan la optimización del rendimiento de la virtualización y explican que múltiples niveles de hipervisores pueden complicar la gestión de la seguridad (Lim, J. y Nieh, J., 2020).

La gestión de vulnerabilidades, entendida como el proceso de identificar, clasificar, remediar y mitigar las debilidades de seguridad, se vuelve fundamental para mantener la integridad de estos entornos complejos. Es necesario adoptar estrategias proactivas, por ejemplo, utilizar herramientas de escaneo automatizado en la detección de fallos de seguridad susceptibles de ser explotados por agentes maliciosos (Elastic. s.f.).

No obstante, la tarea de garantizar la seguridad se vuelve particularmente compleja cuando se trata de infraestructuras tecnológicas de gran tamaño. El caso del Centro de Datos de la DGTIC, que aloja a más de mil servidores virtuales que se ejecutan sobre múltiples hipervisores, presenta un desafío significativo para la realización de revisiones de seguridad de manera manual. La magnitud de esta infraestructura hace inviable la inspección individual de cada servidor, tanto por la cantidad de tiempo y recursos que demandaría como por la dificultad de mantener una visión coherente y actualizada del estado de seguridad. La diversidad de sistemas operativos con los que se entregan los servidores virtuales añade una capa adicional de complejidad, ya que cada sistema operativo puede tener sus propias vulnerabilidades y requerir tanto herramientas como conocimientos específicos para su análisis. Ante esta situación, la necesidad de implementar soluciones de automatización para el análisis de vulnerabilidades se hizo indispensable.

El presente reporte técnico describe el proceso de implementación de la herramienta Nessus en un entorno de pruebas y un análisis de los resultados obtenidos al emplearla como analizador de vulnerabilidades en un clúster de servidores del Centro de Datos, con el objetivo de evaluar su capacidad para identificar y reportar las vulnerabilidades de seguridad presentes en la infraestructura virtualizada, realizado en el segundo semestre de 2024.

2. DESARROLLO TÉCNICO

Elección de la herramienta

Existen investigaciones sobre la implementación de Nessus en redes de campus universitarios, en las que se destaca su eficacia en la identificación de vulnerabilidades (Railkar, D., 2022). Esto brinda un precedente para elegir la herramienta y sugiere que Nessus se ha implementado con éxito en otras

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 84 - 90

universidades (Chhillar, K., 2021). Entre ellas, la Universidad de Harvard emplea Nessus para realizar pruebas de vulnerabilidad proactivas y automatizadas en sus instancias de servidores; lo integran con sistemas de gestión de tickets para dar seguimiento a los riesgos detectados y su remediación (Harvard University Information Technology Security Operations, 2024).

Otras universidades de Estados Unidos incluyen la herramienta como parte de sus procedimientos de seguridad. Por ejemplo, la Universidad de Texas en Austin (2021) utiliza Nessus para realizar escaneos de vulnerabilidades en sus sistemas. La Universidad de California en Berkeley (2025), por medio de su Oficina de Seguridad, realiza escaneos de vulnerabilidades utilizando Nessus.

Estos casos sugieren que Nessus es una herramienta considerada adecuada para la gestión de vulnerabilidades en entornos académicos.

2.1 METODOLOGÍA

Nessus opera bajo un modelo cliente-servidor, donde el servidor (nessusd) es responsable de realizar las pruebas de vulnerabilidad y los clientes son utilizados en los puntos finales para configurar y lanzar escaneos específicos (Kak, A., 2024).

El servidor necesita estar en la misma subred que las máquinas virtuales que se van a escanear. Nessus realizará escaneo de puertos para identificar los servicios y verificar vulnerabilidades conocidas a través de una base de datos de *plugins,* una colección central de *scripts* y algoritmos que el escáner utiliza para detectar vulnerabilidades específicas en sistemas y redes. La eficacia de Nessus reside en esta base de datos de *plugins*, por lo que es de suma importancia realizar actualizaciones de manera periódica para poder detectar vulnerabilidades recién descubiertas.

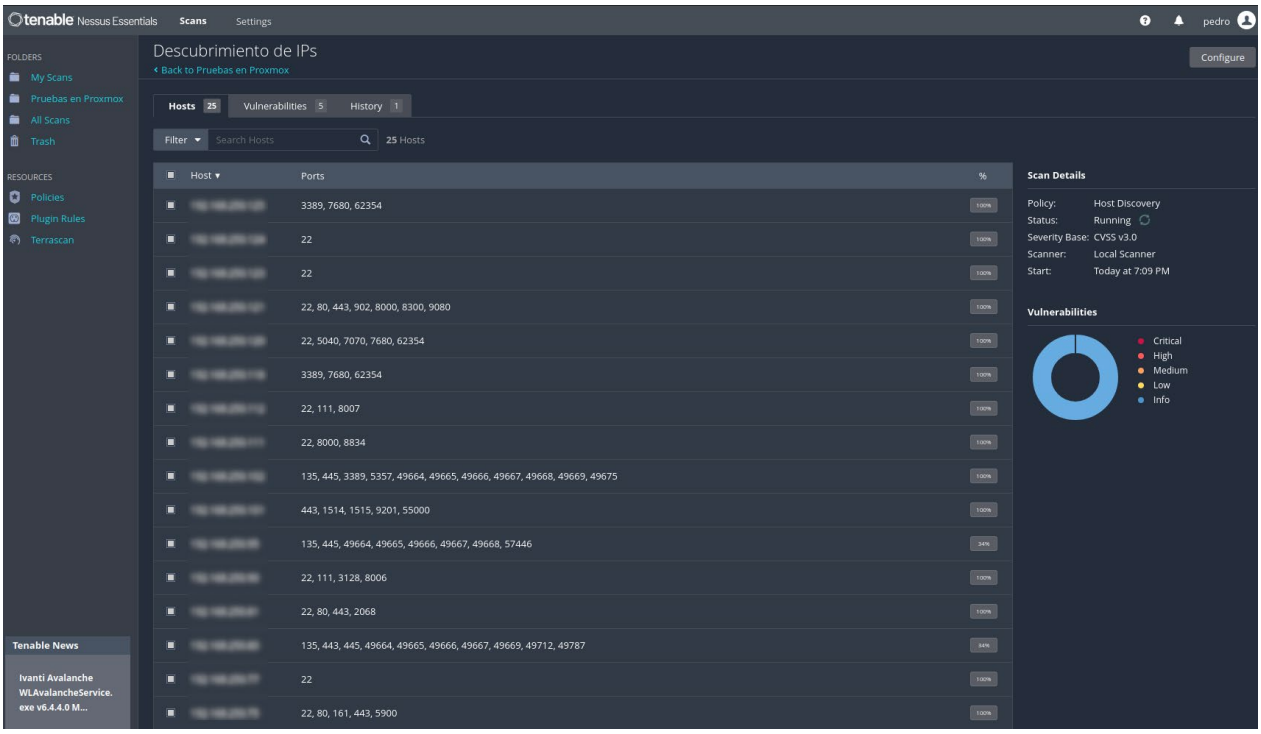
Implementación de Nessus en el hipervisor Proxmox

Dentro de un clúster de pruebas, se instaló el hipervisor Proxmox y, en él, se instalaron máquinas virtuales corriendo diversos sistemas operativos. Se utilizaron versiones desactualizadas de Ubuntu Server para poder encontrar algunas alertas de seguridad. También se instalaron máquinas virtuales con Windows Server. Dentro de una máquina virtual en el hipervisor, se instaló la herramienta de análisis de vulnerabilidades Nessus versión 6.3, en la misma subred que las máquinas virtuales a analizar. En la Figura 1, es posible ver cómo, en un primer escaneo, la herramienta nos muestra información inicial de las máquinas visibles en el segmento de red, así como los puertos abiertos.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 85 - 90

Figura 1

Escaneo general del segmento de red



Se optó por esta configuración para que sea más fácil evaluar todas las capacidades de la herramienta. Se instaló la versión más reciente de Nessus Essentials, que es una versión gratuita, de uso no comercial y que permite escanear direcciones IP en el momento de las pruebas. Durante la instalación, se configuraron direcciones IP estáticas para asegurar una comunicación consistente con las máquinas objetivo. No se realizaron configuraciones especiales adicionales en la instalación de Nessus más allá de la configuración inicial del administrador y la activación de la licencia.

Configuración y ejecución de los escaneos de vulnerabilidades

Nessus cuenta con una gran variedad de tipos de escaneo, como se muestra en la Tabla 1. Se eligieron aquellos adaptados a los sistemas operativos de las máquinas objetivo. Se llevaron a cabo escaneos de red básicos (*Basic Network Scan*) complementados con escaneos con credenciales (*Credentialed Scan*), proporcionando las credenciales de administrador correspondientes. El uso de éstos últimos permite a Nessus obtener una visión más profunda de la configuración del sistema operativo y las aplicaciones instaladas, lo que mejora la precisión de la detección de vulnerabilidades.

Se utilizaron los rangos de puertos predeterminados para los escaneos básicos. No se deshabilitaron *plugins* específicos, lo que permitió que Nessus utilizara su conjunto completo de pruebas de vulnerabilidad.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 86 - 90

Tabla 1

Tipos de escaneos de Nessus

Incluidos en Nessus Essentials	No incluidos en Nessus Essentials
Host Discovery	Web Application Tests
Basic Network Scan	Audit Cloud Infrastructure
Advanced Scan	Internal PCI Network Scan
Advanced Dynamic Scan	MDM Config Audit
Malware Scan	Offline Config Audit
Mobile Device Scan	PCI Quarterly External Scan
Credentialed Patch Audit	Policy Compliance Auditing
Active Directory Starter Scan	SCAP and OVAL Auditing
Find AI	

Consideraciones de seguridad al ejecutar Nessus en el mismo hipervisor

Al ejecutar Nessus dentro del mismo hipervisor Proxmox donde residen los servidores analizados, se deben tener ciertas consideraciones de seguridad. Una de las principales preocupaciones es la utilización de recursos. La ejecución de escaneos de vulnerabilidades puede consumir una cantidad significativa de recursos de CPU, memoria y red, lo que podría afectar el rendimiento de otras máquinas virtuales que se ejecutan en el mismo hipervisor (Proxmox Support Forum, 2023). Además, existe un riesgo de que una instancia de Nessus comprometida pueda ser utilizada para atacar otras máquinas virtuales o el propio hipervisor. Sin embargo, esta configuración también podría ofrecer algunas ventajas, como una mejor visibilidad de la red dentro del entorno virtual, lo que podría mejorar la precisión de los escaneos. Para mitigar los riesgos, es crucial asegurar la instancia de Nessus que se ejecuta en el entorno de producción y aplicar las mismas prácticas de seguridad que se utilizarían con cualquier otro servidor, como mantener el sistema operativo y las aplicaciones actualizadas, implementar controles de acceso y utilizar contraseñas seguras (GeeksforGeeks, 2024).

Identificación y clasificación de vulnerabilidades

Nessus utiliza el sistema de puntuación CVSS (*Common Vulnerability Scoring System*), uno de los estándares más reconocidos de la industria, diseñado para evaluar y comunicar la gravedad de las vulnerabilidades de seguridad en los sistemas informáticos, para clasificar la gravedad de cada vulnerabilidad detectada durante el escaneo (West Virginia University, 2022). Esta clasificación ayuda a los usuarios a entender el potencial impacto de cada vulnerabilidad y a priorizar las acciones de remediación. Los niveles de gravedad propuestos por el fabricante (Tenable, 2025) que se encuentran en los resultados de Nessus se presentan en la Tabla 2.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 87 - 90

Tabla 2

Clasificación de gravedad de vulnerabilidades de Nessus

Crítica	CVSS 9.0-10.0	Estas vulnerabilidades representan el mayor riesgo, ya que pueden ser explotadas fácilmente por un atacante remoto no autenticado y podrían resultar en que el sistema afectado sea comprometido.
Alta	CVSS 7.0-8.9	Las vulnerabilidades de gravedad alta pueden permitir a usuarios locales obtener privilegios elevados, a usuarios remotos no autenticados, visualizar recursos que deberían estar protegidos y a usuarios remotos autenticados, ejecutar código arbitrario o causar una denegación de servicio.
Media	CVSS 4.0-6.9	Estas vulnerabilidades son más difíciles de explotar que las críticas o altas, pero aún podrían llevar a la vulneración del sistema bajo ciertas circunstancias específicas.
Baja	CVSS 0.1-3.9	Las vulnerabilidades de gravedad baja generalmente requieren condiciones muy específicas para ser explotadas o, si se explotan con éxito, tienen un impacto mínimo en el sistema
Informativa	CVSS 0	Este nivel no indica una vulnerabilidad real, sino que proporciona información general sobre la configuración del sistema y su funcionamiento.

Comprender estos niveles de gravedad es fundamental para poder priorizar eficazmente la remediación de las vulnerabilidades encontradas en las máquinas virtuales del clúster de pruebas. La estandarización de la clasificación de vulnerabilidades mediante el sistema CVSS facilita la comunicación y la priorización de los riesgos de seguridad entre diferentes equipos y partes interesadas, así como promueve el empleo de un lenguaje común y una métrica reconocida en la industria.

3. RESULTADOS

Para medir el éxito y la efectividad del análisis de vulnerabilidades realizado en la infraestructura de prueba del Centro de Datos, se deben considerar métricas clave. Estas métricas proporcionan una medida cuantitativa de los hallazgos y ayudan a rastrear el progreso hacia la mejora de la postura de seguridad. Algunos autores han estudiado métodos para correlacionar las métricas CVSS con los resultados de herramientas de código abierto (Sllame et al., 2021).

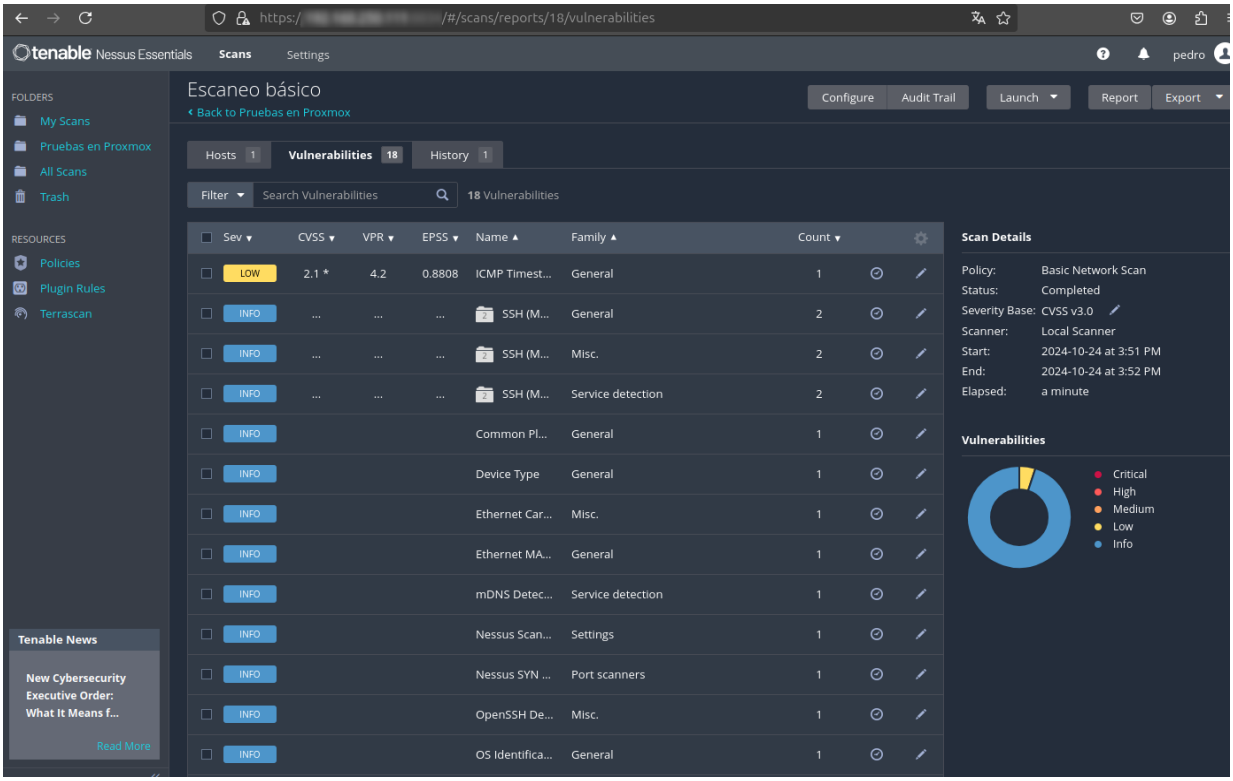
El número total de vulnerabilidades identificadas en todos los componentes escaneados de la infraestructura virtual fue una métrica principal. Esto proporcionó una indicación general del número de posibles debilidades de seguridad presentes. Además, la distribución de estas vulnerabilidades por nivel de gravedad (Crítica, Alta, Media, Baja, Informativa) ofreció información crítica sobre los riesgos más urgentes por atender. Un mayor porcentaje de vulnerabilidades críticas y de alta gravedad indicaría

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 88 - 90

una mayor necesidad de atención inmediata y esfuerzos de remediación. El número de vulnerabilidades únicas identificadas también se rastreó para comprender la diversidad de fallos de seguridad presentes, independientemente de cuántas veces apareciera una vulnerabilidad específica en diferentes activos. En la Figura 2, se muestra toda la información que nos presenta el panel de resultados de la herramienta. Es posible ver que la herramienta utiliza una interfaz intuitiva y ordenada que ayuda a identificar fácilmente el nivel de gravedad de cada alerta.

Figura 2

Panel de resultados de un escaneo básico



Si bien cada vulnerabilidad puede estudiarse de manera individual, existen casos de estudio que contemplan tablas de recomendaciones asociadas a distintas vulnerabilidades comunes (Paspuel y Pablo, 2024). Con base en esta información, junto con los resultados del análisis de Nessus, se realizaron las siguientes recomendaciones específicas para el entorno de pruebas:

- **Deshabilitar versiones obsoletas de TLS:** Deshabilitar inmediatamente TLS 1.0 y 1.1 en servidores web y sistemas operativos, así como forzar el uso de TLS 1.2 o superior, siguiendo las instrucciones específicas para cada servidor.
- **Reforzar la configuración SSH:** Revisar la configuración de SSH de los servidores. Revisar y aplicar políticas de contraseñas seguras para todos los usuarios de SSH. Considerar deshabilitar la autenticación basada en contraseñas, utilizar claves SSH en su lugar y evitar usar el puerto 22 predeterminado.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 89 - 90

- **Asegurar la configuración SNMP:** Cambiar la cadena de comunidad SNMP predeterminada en el segmento de red virtual a un valor privado seguro y restringir el acceso a estaciones de gestión autorizadas. Evaluar la viabilidad de actualizar a SNMPv3 para mejorar la seguridad.
- **Implementar encabezados de seguridad HTTP:** Configurar el servidor web que aloja la interfaz de gestión para incluir los encabezados Strict-Transport-Security (HSTS) y X-Frame-Options en sus respuestas HTTP, siguiendo la documentación de cada servidor web para obtener detalles de configuración.
- **Establecer un programa continuo de gestión de vulnerabilidades:** Implementar un cronograma para escaneos de Nessus regulares y automatizados de la infraestructura virtual. Establecer un proceso para revisar y remediar las vulnerabilidades identificadas en función de su gravedad.

Al implementar estas mejores prácticas y abordar las recomendaciones específicas derivadas del análisis de Nessus, se puede mejorar significativamente la postura de seguridad de las máquinas virtuales alojadas en el Centro de Datos.

4. CONCLUSIONES

El análisis realizado ha demostrado que Nessus puede ser un mecanismo de utilidad para la identificación y clasificación de vulnerabilidades en una infraestructura virtualizada compleja.

Nessus tiene la capacidad de descubrir un gran número de vulnerabilidades de seguridad de forma automática, una versión Professional o Expert la harían una solución viable para el escaneo en entornos con una gran cantidad de servidores virtuales y diversidad de sistemas operativos Windows, Linux y versiones recientes de macOS.

La clasificación de las vulnerabilidades por nivel de gravedad proporciona una visión clara de cuáles son los riesgos más graves que requieren atención inmediata. La presencia de vulnerabilidades en el entorno de pruebas, aunque esperado dada la inclusión de sistemas operativos desactualizados, recuerda la potencial exposición a amenazas significativas en un entorno de producción si alguno de los elementos de la infraestructura del Centro de Datos no se actualiza o configura debidamente, o si no se toman las medidas necesarias de detección.

Finalmente, se debe tener en cuenta que las recomendaciones, derivadas del análisis hecho por una herramienta de detección automatizada, serán sólo una parte de las medidas de seguridad necesarias. La adopción de mejores prácticas y cumplimiento de las políticas de seguridad establecerán un entorno propicio para la detección y respuesta ante futuras amenazas, lo que fortalece la resiliencia de la infraestructura digital que soporta el desarrollo de actividades sustantivas de la Universidad.

REFERENCIAS

Chhillar, K. (2021). *University computer network vulnerability assessment using NESSUS*. Paper Code: RDMOCS-P62. https://www.researchgate.net/publication/356998084_University_Computer_Network_Vulnerability_Assessment_using_NESSUS_Paper_Code_RDMOCS-P62

Elastic. (s.f.). ¿Qué es la gestión de vulnerabilidades? https://www.elastic.co/es/what-is/vulnerability-management

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 90 - 90

GeeksforGeeks. (2024). *Explain Nessus Tool in Security Testing.* https://www.geeksforgeeks.org/explain-nessus-tool-in-security-testing/

Harvard University Information Technology Security Operations. (2024). *HUIT Server security requirements standard v1.5*. https://enterprisearchitecture.harvard.edu/sites/hwpi.harvard.edu/files/enterprise/files/huit_server_security_requirements_standard_v1.5.pdf

Kak, A. (2024). *Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing*. Purdue University. https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf

Lim, J. T., & Nieh, J. (2020). *Optimizing nested virtualization performance using direct virtual hardware*. In Proceedings of the Twenty-Fifth International Conference on *ASPLOS Architectural Support for Programming Languages and Operating Systems* (pp. 557-574). https://www.cs.columbia.edu/~nieh/pubs/asplos2020_dvh.pdf

Paspuel, T., & Pablo, J. (2024). *Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades.* Universidad Tecnológica Israel. Paper Code: MASTER-SEG.INF-PRO;012. (pp. 56-63).

Proxmox Support Forum. (2023). *Compatibility with vulnerability scanners [Mensaje en un foro].* https://forum.proxmox.com/threads/compatibility-with-vulnerability-scanners.120807/

Railkar, D. (2022). A Study on Vulnerability Scanning Tools for Network Security. *International Journal of Scientific Research in Computer Science Engineering and Information Technology.* 8(6):340. (pp. 68-75). https://www.researchgate.net/publication/361951998_A_Study_on_Vulnerability_Scanning_Tools_for_Network_Security

Sllame, A. M., Tomia, T. E., & Rahuma, R. M. (2024). A Holistic Approach for Cyber Security Vulnerability Assessment Based on Open Source Tools: Nikto, Acunitx, ZAP, Nessus and Enhanced with AI-Powered Tool ImmuniWeb. In 2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA) (pp. 68-75).

University of California, Berkeley. (2025). Frequently asked questions. Information security office. https://security.berkeley.edu/faq-page_

University of Texas at Austin. (2021). *Minimum security standards for systems.* https://security.utexas.edu/content/min-security-standards/systems

Tenable, Inc. (2025). *Risk metrics*. https://docs.tenable.com/nessus/Content/RiskMetrics.htm

West Virginia University. (2022). *Vulnerability management standard.* https://it.wvu.edu/policies-and-procedures/security/vulnerability-management-standard