ESTRUCTURA DEL DOCUMENTO PARA LA ESTRUCTURA DEL RESUMEN ANALÍTICA ESPECIALIZADO -RAE

Fecha de Realización:	23/05/2020
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Análisis de vulnerabilidades al servidor de pruebas del departamento de sistemas de la E.S.E. hospital marco Felipe afanador del municipio de Tocaima Cundinamarca generando las recomendaciones para realizar un proceso de hardening
Autor(es):	Diego Francisco Ballén León
Palabras Claves:	Análisis, Vulnerabilidades, Hardening, Servidor, Kali Linux,
Descripción:	Trabajo de grado para optar al título de Especialista en Seguridad Informática

Fuentes bibliográficas destacadas:

1. aprendizdesysadmin.com (2018). *Guía Hardening Instalación del Sistema*. [online] Aprendiz de sysadmin. Available at: https://aprendizdesysadmin.com/guia-hardening-instalacion-del-sistema/[Accessed 17 Oct. 2018].

2. Castro, I. (2018). *¿Qué es un Análisis de Vulnerabilidades Informáticas?*. [online] Blog de #NextGenSecurity. Available at: http://blog.cerounosoftware.com.mx/que-es-un-analisis-de-vulnerabilidades-inform%C3%A1ticas [Accessed 17 Oct. 2018].

3. descargas.pntic.mec.es (2018). *Vulnerabilidades de un sistema informático | Seguridad Informática*. [online] Descargas.pntic.mec.es. Available at: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html [Accessed 17 Oct. 2018].

4. Gómez, A. (2018). *Anexo III Análisis y Gestión de Riesgos en un Sistema Informático*. [online] Academia.edu. Available at: https://www.academia.edu/5971566/Anexo_III_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_en_un_Sistema_Inform%C3%A1tico [Accessed 17 Oct. 2018].

5. Mifsud, E. (2018). *MONOGRÁFICO: Introducción a la seguridad informática - Vulnerabilidades de un sistema informático | Observatorio Tecnológico*. [online] Recursostic.educacion.es. Available at: http://recursostic.educacion.es/observatorio/web/gl/software/software-

general/1040-introduccion-a-la-seguridad-informatica?start=3 [Accessed 17 Oct. 2018].

6. Otegui, A. (2018). *Herramientas de análisis de vulnerabilidades*. [online] Es.slideshare.net. Available at: https://es.slideshare.net/alejandro_otegui96/herramientas-de-anlisis-de-vulnerabilidades-81021908 [Accessed 17 Oct. 2018].

7. Prandini, P. (2018). *Vulnerabilidades, amenazas y riesgo en "texto claro" | Magazcitum*. [online] Magazcitum.com.mx. Availableat:http://www.magazcitum.com.mx/?p=2193[Accessed 17 Oct. 2018].

8. seguinfo.wordpress.com (2018). *Proceso de Hardening*. [online] Seguridad Informática. Available at: https://seguinfo.wordpress.com/2012/04/03/proceso-de-hardening/

9. Seguridad, N. (2018). *¿Cómo hacer análisis de vulnerabilidades informáticas?*. [online] Noticiasseguridad.com. Available at: http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

10. Smartekh, G. (2018). *¿QUÉ ES HARDENING?*. [online] Blog.smartekh.com. Available at: http://blog.smartekh.com/que-es-hardening

11. Andrés, R. (2016). Qué es Kali Linux y qué puedes hacer con él. [online] ComputerHoy. Available at: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671 [Accessed 15 Nov. 2018].

12. ecured.cu (n.d.). Kali linux. [online] EcuRed. Available at: https://www.ecured.cu/Kali_linux [Accessed 17 Nov. 2018].

13. L4bs, S. (2016). Snifer@L4b's: Listado Completo Herramientas en Kali Linux. [online] Snifer@L4b's. Available at: https://www.sniferl4bs.com/2014/03/listado-completo-herramientas-en-kali.html [Accessed 17 Nov. 2018].

14. Universidadviu.com (2018). Vulnerabilidad informática, tipos y debilidades principales | VIU. [online] Universidadviu.com. Available at: https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/ [Accessed 18 Nov. 2018].
15. Garcia, U. (2017). ¿Qué es una vulnerabilidad?. [online] Blog de #NextGenSecurity. Available at: http://blog.cerounosoftware.com.mx/qu%C3%A9-es-una-vulnerabilidad [Accessed 18 Nov. 2018].

16. cursodehackers.com (2017). Curso de hackers - Escaner Nessus de vulnerabilidades. [online] Cursodehackers.com. Available at: http://www.cursodehackers.com/nessus.html [Accessed 15 Nov. 2018].

17. Mendoza, M. (2014). Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/ [Accessed 15 Nov. 2018].

18. infosegur (2018). Vulnerabilidades | Seguridad Informática. [online] Infosegur.wordpress.com. Available at: https://infosegur.wordpress.com/tag/vulnerabilidades/ [Accessed 18 Nov. 2018].

19. López, D. (n.d.). Evolución de la Seguridad Informática | Grupo Control. [online] Grupocontrol.com. Available at: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica [Accessed 26 Nov. 2018].

20. tecnologia-informatica.com (n.d.). Vulnerabilidades informáticas - Tecnología & Informática. [online] Tecnología & Informática. Available at: https://tecnologia-informatica.com/vulnerabilidades-informaticas/ [Accessed 27 Nov. 2018].

21. http://descargas.pntic.mec.es (n.d.). Vulnerabilidades de un sistema informático | Seguridad Informática. [online] Descargas.pntic.mec.es. Available at: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html [Accessed 27 Nov. 2018].

22. infosegur.wordpress.com (2013). Vulnerabilidades | Seguridad Informática. [online] Infosegur.wordpress.com. Available at: https://infosegur.wordpress.com/tag/vulnerabilidades/ [Accessed 27 Nov. 2018].

23. Universidadviu.com (2018). Vulnerabilidad informática, tipos y debilidades principales | VIU. [online] Universidadviu.com. Available at: https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/ [Accessed 27 Nov. 2018].

24. El-nacional.com (2017). Los 10 incidentes de seguridad informática más importantes del último año. [online] El Nacional. Available at: http://www.el-nacional.com/noticias/empresas/los-incidentes-seguridad-informatica-mas-importantes-del-ultimo-ano_75387 [Accessed 27 Nov. 2018].

25. Martínez, E. (2017). 7 de los ciberataques más famosos de la historia. [online] Icorp.com.mx. Available at: http://www.icorp.com.mx/blog/ciberataques-mas-famosos/ [Accessed 27 Nov. 2018].

26. seguinfo.wordpress.com (2007). ¿Qué es Nmap?. [online] Seguridad Informática. Available at: https://seguinfo.wordpress.com/2007/06/27/%C2%BFque-es-nmap/ [Accessed 27 Nov. 2018].

27. http://facilitamos.catedu.es (n.d.). Práctica con Nmap/Zenmap | Unidad Didáctica: 7 Propuesta Didáctica: Instalación/configuración de los equipos de red. [online] Facilitamos.catedu.es. Available at: http://facilitamos.catedu.es/previo/fpinformatica/INFOR_U6_1_tcp-ipZIP/prctica_con_nmapzenmap.html [Accessed 27 Nov. 2018].

28. Pérez, I. (2015). Auditando con Nmap y sus scripts para escanear vulnerabilidades. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/ [Accessed 27 Nov. 2018].

29. Mendoza, M. (2014). Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/ [Accessed 27 Nov. 2018].

30. Heidegger, Z. (2011). Manual práctico de OpenVAS en Español | Blackploit [PenTest]. [online] Blackploit.com. Available at: https://www.blackploit.com/2011/04/manual-practico-de-openvas-open.html [Accessed 27 Nov. 2018].

31. VILLAR, M. (2018). METODOLOGÍAS Y HERRAMIENTAS DE ETHICAL HACKING. RETRIEVED FROM HTTPS://SEGURIDADINFORMATICAHOY.BLOGSPOT.COM/2013/02/METODOLOGIAS-Y-HERRAMIENTAS-DE-ETHICAL.HTML

32. El Tiempo (2018). En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia. [online] El Tiempo. Available at: https://www.eltiempo.com/archivo/documento/CMS-16493604 [Accessed 10 Oct. 2018].

33. Redacción El Tiempo. (2018). CLASIFICACION DE LOS HOSPITALES. Retrieved from https://www.eltiempo.com/archivo/documento/MAM-627858

34. Clasificacionde. (2018). Clasificación de los hospitales - ¿Cómo se clasifican?. Retrieved from https://www.clasificacionde.org/hospitales/

35. Solvetic.com (2018). Hardening seguridad de servidores y sistemas operativos. [online] Solvetic. Available at: https://www.solvetic.com/tutoriales/article/1875-hardening-seguridad-de-servidores-y-sistemas-operativos/

36. Dragonjar.org (2018). Hardening, Conceptos básicos. [online] Dragonjar.org. Available at: https://www.dragonjar.org/hardening-conceptos-basicos.xhtml

37. [Villanueva, C. (2018). Hardening de un Sistema Operativo de Red. [online] https://www.lawebdelprogramador.com. Available at: https://www.lawebdelprogramador.com/pdf/10383-Hardening-de-un-Sistema-Operativo-de-Red.html

38. thesecuritysentinel.es (2018). Curso de Hardening de Servidores Windows - The Security Sentinel. [online] The Security Sentinel. Available at: https://thesecuritysentinel.es/curso/hardening-servidores-windows/

39. Seguridad, N. (2018). ¿Cómo hacer análisis de vulnerabilidades informáticas?. [online] Noticiasseguridad.com. Available at: http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

40. Otegui, A. (2018). Herramientas de análisis de vulnerabilidades. [online] Es.slideshare.net. Available at: https://es.slideshare.net/alejandro_otegui96/herramientas-de-anlisis-de-vulnerabilidades-81021908 [Accessed 17 Oct. 2018].

41. paraisolinux.com (2017). Que es y como usar NMAP - Paraiso Linux. [online] Paraiso Linux. Available at: https://paraisolinux.com/que-es-y-como-usar-nmap/ [Accessed 12 Dec. 2018].

42. Nmap.org (n.d.). Guía de referencia de Nmap (Página de manual) |. [online] Nmap.org. Available at: https://nmap.org/man/es/index.html [Accessed 12 Dec. 2018].

43. Pinilla, L. (2015). Que es y Como usar Nmap. [online] Es.slideshare.net. Available at: https://es.slideshare.net/luispinilla96/que-es-y-como-usar-nmap [Accessed 12 Dec. 2018].

44. Murcia, C. (2003). Introducción a Nmap. [online] Maestros del Web. Available at: http://www.maestrosdelweb.com/nmap/ [Accessed 12 Dec. 2018].

45. Avila, F. (2018). Scanner de vulnerabilidades (Herramientas #2) | Security Hack Labs. [online] Security Hack Labs. Available at: https://securityhacklabs.net/articulo/escaner-de-vulnerabilidades-herramientas-2 [Accessed 12 Dec. 2018].

46. Khepri, W. (2018). Las 25 mejores herramientas de Kali Linux – William Khepri – Medium. [online] Medium. Available at: https://medium.com/@williamkhepri/las-25-mejores-herramientas-de-kali-linux-b8c2a92f2ab4 [Accessed 12 Dec. 2018].

47. Bornik, S. (n.d.). Pruebas de penetración Para principiantes: 5 herramientas Para empezar. [online] Revista.seguridad.unam.mx. Available at: https://revista.seguridad.unam.mx/print/2233 [Accessed 12 Dec. 2018].

48. Trust Network (2018). Análisis de Vulnerabilidades. [online] Trust-network.net. Available at: http://www.trust-network.net/blog-trustnet/analisis-de-vulnerabilidades [Accessed 13 Dec. 2018].

49. Caballero, A. (n.d.). Escaneo de Vulnerabilidades Externo utilizando OpenVAS | Alonso Caballero Quezada / ReYDeS. [online] Reydes.com. Available at: http://www.reydes.com/d/?q=Escaneo_de_Vulnerabilidades_Externo_utilizando_OpenVAS [Accessed 12 Dec. 2018].

50. E.S.E. Hospital Marco Felipe Afanador de Tocaima (2019). *Política de Tratamiento de Datos*. [online] Hmfa-tocaima-cundinamarca.gov.co. Available at: http://www.hmfa-tocaima-cundinamarca.gov.co/politicas-y-lineamientos/politica-de-tratamiento-de-datos [Accessed 18 Mar. 2019].

Contenido del documento:	El objetivo de este proyecto es analizar las vulnerabilidades del servidor de pruebas de la E.S.E. Hospital marco Felipe afanador de Tocaima Cundinamarca ubicado en el departamento de sistemas de esa institución, por medio de las herramientas OPENVAS y NMAP, que vienen incluidas en la distribución de seguridad KALI LINUX, una vez realizado este análisis se generaran las recomendaciones necesarias para que el líder de procesos del departamento de sistemas implemente un proceso de Hardening.
Marco Metodológico:	La metodología de esta monografía, se divide en dos partes la primera es la investigación donde se recopila información relacionada con esta temática y las herramientas que se van a manejar y la segunda parte es del desarrollo del análisis de vulnerabilidades una parte práctica que ejecuta la información recopilada junto con los conocimientos adquiridos en la especialización en seguridad informática donde obtendremos como resultado las

	vulnerabilidades encontradas para desarrollar las recomendaciones que el líder del departamento debe en lo posible de implementar y así realizar el proceso de Hardening
Conceptos adquiridos :	Análisis de vulnerabilidades, herramientas y recursos libres para análisis, automatización de informes, mitigación o eliminación de vulnerabilidades, evolución y adaptabilidad de la seguridad informática y sus amenazas
Conclusiones:	Las evidencias en el análisis de vulnerabilidades realizadas en el servidor de pruebas demuestran hallazgos de vulnerabilidades que hasta esa fecha eran desconocidas por el departamento de sistemas del hospital de tocaima, esto demuestra que no importa el tipo de infraestructura que se tenga ningún sistema es perfecto o infalible, y puede estar expuesto a posibles intrusiones o fallos que pueden causar colapso en la prestación de un servicio. Encontrar evidencias de vulnerabilidades en cualquier tipo de infraestructura en este caso un servidor de pruebas, es una alerta a tomar en cuenta para cualquier administrador de sistemas o líder de departamento de sistemas, este tipo de procesos hace replantear las practicas realizadas referentes a seguridad informática y como estas deben evolucionar así como las amenazas y vulnerabilidades cambian con el pasar del tiempo volviendo más robustos todos los objetos que integran una infraestructura. Por otro lado tenemos una gran y versátil herramienta de análisis de vulnerabilidades OPENVAS, esta herramienta demostró una gran flexibilidad al momento de ejecutar el análisis ofreciendo muy buenas opciones para usuarios principiantes que están iniciando en este tipo de actividades de

	seguridad informática, esto demuestra que una herramienta de naturaliza gratuita como lo es openvas puede hacerle frente a herramientas de pago y ofrecer resultados de calidad. Otra de las herramientas que fueron de gran ayuda fue la suite de seguridad informática KALILINUX, al igual que openvas, esta distribución es totalmente gratuita y sirve como complemente perfecto para realizar pentesting reconociendo posibles fallas a diferentes niveles y objetivos que posiblemente los analizadores de vulnerabilidades puedan pasar por alto, lo que demuestra que al igual que la infraestructuras los métodos de análisis no son perfectos y pueden necesitar complementos adicionales para dar una visión adicional al escenario analizado. Posteriormente tenemos el informe de vulnerabilidades arrojado por GREENBONE, que es el asistente integrado de openvas, este informe fue la herramienta fundamental para generar las recomendaciones a tener en cuenta para el proceso de hardening, en el están todas la amenazas clasificadas a detalle y como mitigarlas, adicionalmente greenbone incluyo links a comunidades que contienen información adicional sobre las vulnerabilidades encontradas en relación a lo anterior al igual que kalilinux, greenbone es un complemento perfecto una herramienta robusta y precisa que ofrece justo lo que se necesitaba para este tipo de procesos. Por ultimo se puede concluir que la revisión de vulnerabilidades en una infraestructura informática ya sea en su totalidad o a un solo componente que la integra como lo fue

	el servidor de pruebas y sin importar de que entidad u organización se trate, debe ser un proceso estandarizado y obligatorio que genere un posterior hardening a la infraestructura, documentando todos los resultados obtenidos para conocer qué tipo de vulnerabilidades fueron encontradas y como mitigarlas.