RESUMEN ANALÍTICO EN EDUCACIÓN - RAE -	UNIVERSIDAD CATÓLICA de Colombia Vigilada Mineducación RIUCaC

FACULTAD DE INGENIERIA
PROGRAMA DE POSGRADOS
ESPECIALIZACIÓN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C.

LICENCIA CREATIVE COMMONS: Señale en la casilla la licencia que insertó en el trabajo de grado, tesis o artículo:

Atribución		Atribución no comercial		Atribución no comercial sin derivadas	X
Atribución no comercial compartir igual		Atribución sin derivadas		Atribución compartir igual	

AÑO DE ELABORACIÓN: 2019

TÍTULO: DEFINICIÓN DE UNA METODOLOGÍA PERSONALIZADA DE HACKING ÉTICO PARA EMPRESAS PÚBLICAS DE CUNDINAMARCA S.A. E.S.P Y EJECUCIÓN DE UNA PRUEBA A LA PÁGINA WEB Y A LOS SERVIDORES DE LA ENTIDAD, SOPORTADA SOBRE LA METODOLOGÍA DEFINIDA.

AUTOR (ES):

Rodriguez Vasquez, Elkin German y Sarmiento Acosta, William Andres.

DIRECTOR(ES)/ASESOR(ES):

Osorio Reina, Diego.

MODALIDAD:

Investigación Software inteligente y convergencia tecnológica

PÁGINAS:	107	TABLAS:	10	CUADROS:	0	FIGURAS:	40	ANEXOS:	4

CONTENIDO:

DESCRIPCIÓN: Con la ejecución de la prueba de Hacking Ético en Empresas Públicas, se le permitirá a la entidad determinar qué tan segura se encuentra su página web y la información alojada en sus servidores, así como generar de manera oportuna estrategias para fortalecer la seguridad de la información y la potencial remediación de un incidente de seguridad que se pueda presentar en un momento determinado

METODOLOGÍA:

FASES DEL TRABAJO DE GRADO

Para el desarrollo de nuestro proyecto de grado se define las siguientes fases:

Fase de Planeación

En esta fase buscamos las organizaciones en las cuales cada uno de quienes participamos en la realización de este proyecto trabajamos con el fin de reunirnos con los directivos y exponerles el proyecto académico.

Fase de Ejecución

En esta fase presentamos la propuesta formal de trabajo a Empresas Publicas y nos reunimos primero con el área directiva para exponerles el proyecto, posteriormente nos reunimos con los ingenieros del área de tecnología

socializarles el plan de trabajo propuesto y acordar la forma en la cual realizaríamos las pruebas técnicas y así mismo especificarles los protocolos de seguridad que debían tener previstos para garantizar que en dado caso que se presentara algún tipo de falla tuviéramos lo necesario para restablecer los servicios de forma oportuna y sin poner en riesgo la operación de la organización.

Fase de Análisis

En esta fase se realiza una reunión técnica con el área de tecnología que nos permita tener una visual de la infraestructura física que tiene la entidad, sus servicios web y su centro de procesamiento de datos. Bajo este primer contexto determinar las herramientas que se usarían en la realización de las pruebas técnicas y las condiciones adecuadas de ejecución que no interfirieran en el normal funcionamiento de los procesos de la entidad.
De igual forma en esta fase se procede a hacer un análisis de la metodología PTES que nos permita a partir de esta generar una nueva metodología personalizada para la ejecución de un ethical hacking en Empresas Publicas de Cundinamarca.

Fase de Informe

En esta fase final se procede a realizar la elaboración de los informes técnicos y gerenciales a partir de los resultados obtenidos en las pruebas técnicas realizadas previamente que serán socializados en Empresas Publicas y serán soporte como entregables del proyecto.

Se realiza el respectivo diseño de la metodología personalizada para Empresas Públicas de Cundinamarca.

PALABRAS CLAVE:

CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, RIESGO, AMENAZA, VULNERABILIDAD, CAJA BLANCA, CAJA GRIS, CAJA NEGRA, ETHICAL HACKING, ANALISIS DE VULNERABILIDADES, PENETRATION TEST, RED TEAM.

CONCLUSIONES:

- Se evidencio que la entidad lleva un paso lento respecto en la implementación del modelo de seguridad y privacidad de la información MINTIC, sin embargo, en el área de tecnología ha hecho lo posible para realizar un adecuado aseguramiento de la infraestructura, aseguramiento que será reforzado con los resultados y recomendaciones del desarrollo de las pruebas de ethical hacking por parte de los estudiantes de la Universidad Católica.

- Se debe tener en cuenta que hoy en día cada vez los ataques cibernéticos son más sofisticados y que buscan fines lucrativos; la protección de las infraestructuras tecnológicas de las entidades deben evolucionar y buscar la forma de contar con altos estándares de seguridad con el fin de minimizar los riesgos y asegurar los sus activos.

- Por parte del área de tecnología se debe configurar el certificado digital de forma adecuada a la página web de la compañía para que el tráfico vaya cifrado, se debe tener en cuenta que este está próximo a vencer.

- Se debe considerar solo dejar un solo administrador de contenidos para la gestión de la página web ya que tienen dos, uno de estos está muy desactualizado y vulnerables, y tiene un riesgo muy alto de que sea blanco de atacantes.

- Es de resaltar que el administrador de contenidos WordPress se encuentra actualizado.

- En los portales de autenticación se debe implementar un sistema captcha así como el bloqueo después de unos pocos intentos no exitosos de logueo, ya que en este momento un atacante se puede aprovechar de esta debilidad.

- Garantizar la creación de código seguro en aplicaciones y servicios de la organización disminuyendo los incidentes de seguridad.

- Eliminar información obsoleta que se encuentra en la página, ya que estos aparecen como enlaces rotos al ingresar a ellos.

- Realizar una revisión de los recursos visibles dentro de los sitios web.

FUENTES

Acunetix. (n.d.). Introducción a Acunetix | Acunetix. Retrieved June 2, 2019, from https://www.acunetix.com/support/docs/introduction/

Alycia Mitchell. (2015). WPScan: Encontrando Vulnerabilidades de WordPress. Retrieved June 1, 2019, from https://blog.sucuri.net/espanol/2015/12/usando-wpscan-encontrando-vulnerabilidades-de-wordpress.html

Angarita Pinzón, C., & Guzmán Flórez, C. (2017). *Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá*. Retrieved from https://repository.ucatolica.edu.co/handle/10983/15321

CCP-MINTIC. (2016). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

COLPRENSA. (2018). Colombia, el sexto país con más ciberataques en 2017. Retrieved from https://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174

Congreso de la República de Colombia. Ley 527 de 1999 (1999). Retrieved from https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

Congreso de la República de Colombia. Ley 1266 de 2008 (2008). Retrieved from https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488&dt=S

Congreso de la República de Colombia. Ley 1712 de 2014 (2014). Retrieved from https://www.mintic.gov.co/portal/604/articles-7147_documento.pdf

E.P.C. (2018). *Plan de Comunicaciones EPC*. Retrieved from http://www.epc.com.co/intranet2012/sig/Servicio al cliente/planes/SAC-Pl002 Plan de Comunicaciones.pdf

El Tiempo, T. (2017). Resultados del estudio Impacto de los incidentes de seguridad digital en Colombia 2017 - Novedades Tecnología - Tecnología - ELTIEMPO.COM. Retrieved from https://www.eltiempo.com/tecnosfera/novedades-tecnologia/resultados-del-estudio-impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017-137222

EUGENIO DUARTE. (2012). Las 8 Mejores Herramientas de Seguridad y Hacking. Retrieved November 25, 2018, from http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

Fernando Catoira. (2012). Penetration Test, ¿en qué consiste? Retrieved November 25, 2018, from https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

GNU Free Documentation. (2014). The Penetration Testing Execution Standard. Retrieved May 20, 2019, from http://www.pentest-standard.org/index.php/Main_Page

ICONTEC. (2006). *NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001*. Retrieved from

http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma. NTC-ISO-IEC 27001.pdf

Iniseg. (2018). ¿Qué es el Hacking ético? Concepto y formación profesional | Ciberseguridad. Retrieved June 3, 2019, from https://www.iniseg.es/blog/ciberseguridad/que-es-el-hacking-etico/

Llanos Ruiz, A. J., & Meneses Ortiz, M. A. (2016). *Diseño de un protocolo para la detección de vulnerabilidades en los principales servidores de la Superintendencia de Puertos y Transporte*. Retrieved from https://repository.ucatolica.edu.co/handle/10983/14013

Miguel Ángel Mendoza. (2015). De la identificación y análisis a la gestión de riesgos de seguridad. Retrieved November 25, 2018, from https://www.welivesecurity.com/la-es/2015/07/16/analisis-gestion-de-riesgos-seguridad/

Ministerio de la Comunicaciones. Decreto 1151 de 2014 (2014). Retrieved from https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf

OWASP-ZAP. (2019). Proyecto Proxy Zed Attack de OWASP - OWASP. Retrieved June 1, 2019, from https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP Foundation. (2017). *OWASP Top 10 -2017*. Retrieved from https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP Joomla. (2018). Categoría: Proyecto de escáner de vulnerabilidad Joomla OWASP - OWASP. Retrieved June 1, 2019, from

https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project

Revista Dinero. (2017). Sectores más afectados por cibercrimen en Colombia. Retrieved November 25, 2018, from https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

Revista Dinero. (2018). Incremento de ataques cibernéticos en el 2018. Retrieved from https://www.dinero.com/internacional/articulo/incremento-de-ataques-ciberneticos-en-el-2018/264180

Senado de la República de Colombia. Ley 1273 de 2009 Nivel Nacional, iario Oficial 47.223 de enero 5 de 2009 § (2009). Retrieved from https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Senado de la República de Colombia. Ley 1581 de 2012 Nivel Nacional, Diario Oficial 48587 de octubre 18 de 2012 § (2012). Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Wikipedia. (2017). Nessus - Wikipedia, la enciclopedia libre. Retrieved June 1, 2019, from https://es.wikipedia.org/wiki/Nessus

Wikipedia. (2019). Nikto (escáner de vulnerabilidad) - Wikipedia. Retrieved May 31, 2019, from https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)

Wikipedia. (2019). Burp Suite - Wikipedia. Retrieved June 3, 2019, from https://en.wikipedia.org/wiki/Burp_Suite

Wikipedia. (2019). Proyecto Metasploit - Wikipedia. Retrieved June 3, 2019, from https://en.wikipedia.org/wiki/Metasploit_Project

MINTIC. (s.f.). Glosario. Retrieved from https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html

Alfonso Lorenzo Perez. (2019). Riesgo, Amenaza y Vulnerabilidad (ISO 27001) - EQ2B Consulting. Retrieved June 3, 2019, from https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/

Nota: No olvide borrar las instrucciones del formato: sólo deje la información solicitada, incluyendo esta nota.