INCLUSIÓN DE HACKING ÉTICO EN EL PROCESO DE TESTING DE SOFTWARE

Ariel Giannone, Sebastian Martins, Hernán Amatriain, Darío Rodríguez, Hernán Merlino

Laboratorio de Investigación y Desarrollo en Ingeniería de Explotación de Información
Grupo de Ingeniería de Explotación de Información y Grupo Investigación en Sistemas de Información
Departamento de Desarrollo Productivo y Tecnológico. Universidad Nacional de Lanús
29 de Septiembre 3901 (1826) Remedios de Escalada, Lanús. Argentina. Tel +54 11 5533 5600 Ext. 5194
giannoneariel@gmail.com, smartins089@gmail.com, hamatriain@gmail.com, dariorodriguez1977@gmail.com, hmerlino@gmail.com

RESUMEN

Como ocurre con la mayoría de los avances tecnológicos, el crecimiento explosivo de Internet tiene un lado oscuro: los hackers. La escalada natural de amenazas ofensivas contra las medidas defensivas ha demostrado una y otra vez que no hay sistemas prácticos que se puedan construir que sean invulnerables a los ataques. Las organizaciones informatizadas se dieron cuenta de que una de las mejores formas de evaluar la amenaza de intrusión sería tener profesionales independientes de seguridad informática intentando entrar en sus sistemas. Estos "hackers éticos" emplean las mismas herramientas y técnicas que los intrusos, pero sin dañar el sistema de destino ni robar información. En su lugar, permiten evaluar la seguridad de los sistemas de destino e informar de a los propietarios sobre las vulnerabilidades encontradas junto con las instrucciones de cómo remediarlos. Este proceso debe ser planificado con antelación. Todos los aspectos técnicos, de gestión y estratégicos deben estar sumamente cuidados. Estas etapas deben realizarse en un marco de control, gestión y supervisión constante. Es allí donde apunta este proyecto, poder incluir de manera segura y metódica la fase de revisión por hacking ético dentro del proceso de Testing de software.

Palabras clave: Hacking Ético, Testeo de Software, Formación de Recursos Humanos.

CONTEXTO

El Proyecto articula líneas de investigación en el área de Seguridad de Espacios Virtuales de Trabajo del Laboratorio de Investigación y Desarrollo en Espacios Virtuales de Trabajo (LIDEVT UNLa) y Metodologías de Ingeniería de Software con radicación en el Departamento de Desarrollo Productivo y Tecnológico de la Universidad Nacional de Lanús. Las líneas de investigación del área cuentan con financiamiento de la Secretaría de Ciencia y Técnica de la misma Universidad.

FUNDAMENTACION

En general, las políticas de seguridad de la información o los controles por sí solos no garantizan la protección total de la información, ni de los sistemas de información, servicios o redes. Después de los controles que se han implementado, vulnerabilidades residuales probablemente permanezcan haciendo ineficaz la seguridad de la información y por lo tanto los incidentes son aún más posibles. Esto puede llegar a tener efectos negativos tanto directos e indirectos sobre las operaciones de negocio de una organización. Además, es inevitable que se produzcan nuevos casos de amenazas no identificadas previamente. Una preparación insuficiente por una organización para hacer frente a este tipo de incidentes hará cualquier respuesta menos efectiva, y aumentar así el grado de impacto comercial potencial adverso. [ISO/IEC 27035:2011]

En su búsqueda de una manera de abordar el problema, las organizaciones informatizadas se dieron cuenta de que una de las mejores formas de evaluar la amenaza de intrusión a sus intereses sería tener profesionales independientes de seguridad informática intentando entrar en sus sistemas. Este esquema es similar a tener auditores independientes entrando en una organización para verificar sus registros de contabilidad. En el caso de seguridad informática, estos "hackers éticos" emplean las mismas herramientas y técnicas que los intrusos, pero sin dañar el sistema de destino ni robar información. En su lugar, permiten evaluar la seguridad de los sistemas de destino e informar de a los propietarios sobre las vulnerabilidades encontradas junto con las instrucciones de cómo remediarlos.

En resumidas palabras, la evaluación de la seguridad de un sistema por parte de un hacker ético busca responder 3 preguntas básicas:

¿Qué puede ver un intruso en los sistemas atacados?
¿Qué puede hacer un intruso con esa información?

¿Hay alguien en el sistema atacado que se dé cuenta de los ataques o éxitos del intruso?
Este proceso debe ser planificado con antelación. Todos los aspectos técnicos, de gestión y estratégicos deben estar sumamente cuidados. La planificación es importante para cualquier todas las pruebas, ya sea desde un simple análisis de contraseña a una prueba de penetración completa en una aplicación web [Mayorga Jácome et al, 2015; Santos Castañeda, 2016; Onofa Calvopiña et al, 2016; López Vallejo, 2017]. El resguardo de datos debe garantizarse, de lo contrario la prueba puede volverse en contra si alguien afirma que nunca se autorizaron las pruebas. Por lo tanto, un alcance bien definido implica la siguiente información:

- Sistemas específicos para probar.
- Estimar los riesgos que están involucrados.
- Tiempo que llevara la prueba y evaluación del calendario general.
- Recoger y explorar el conocimiento de los sistemas que tenemos antes de la prueba.
- Entrega de informes específicos incluyendo informes de evaluación de la seguridad y un informe de nivel superior describiendo las vulnerabilidades generales que deben abordarse, junto con las medidas correctivas que se deben implementar.

Ahora bien el profesional de seguridad, al llevar a cabo un test de penetración como parte de su trabajo de hacking ético, necesita contar con ese tipo de lógica y tiene que aplicarla, más allá de utilizar las técnicas y herramientas open source [Comunidad Linux,2014; OISSG, 2012; GNU, 2014], comerciales o privadas [Tenable Network Security, 2014], dado que necesita imitar un ataque de la mejor manera y con el máximo nivel posible [Coronel Suarez, 2016; Hurtado Sandoval et al, 2016; López Alvarez, 2016; López Vallejo, 2017]. Para eso, tendrá que emplear todos los recursos de inteligencia que tenga a su alcance, utilizar al extremo sus conocimientos, poder de deducción y análisis mediante el razonamiento y así determinar qué es lo mejor que puede intentar, cómo, dónde y con qué. Por ejemplo, saber si un pequeño dato, por más chico o insignificante que parezca, le será útil y cómo proseguir gracias a él. Continuamente se deberá enfrentar a etapas que le demanden la mayoría de estas aptitudes [Tori, 2008].

- Definir patrones de conducta y acción.
- Hacer relevamientos pasivos de información.
- Interpretar y generar código y cifrado de datos.
- Descubrir manualmente descuidos en el objetivo.
- Descubrir vulnerabilidades presentes de todo el escenario técnico.
- Proyectarse sobre la marcha en modo abstracto, táctica y estratégicamente.
- Ser exhaustivo, pero a la vez saber cuándo es el momento de recurrir a la distensión para no agotar la mente.

Ahora bien, estas etapas deben realizarse en un marco de control, gestión y supervisión constante la cual otorgue tranquilidad y seguridad tanto al profesional que se "coloca" en los pies del criminal como a la organización en su totalidad [Tamayo Veintimilla, 2016; Onofa Calvopiña et al, 2016; Paillacho Pozoet al, 2016]. Es allí donde apunta este trabajo, poder incluir de manera segura y metódica la fase de revisión por hacking ético dentro del proceso de Testing de software.

METODOLOGÍA DE DESARROLLO

Para construir el conocimiento asociado al presente proyecto de investigación, se seguirá un enfoque de investigación clásico [Riveros y Rosas, 1985] [Creswell, 2002] con énfasis en la producción de tecnologías [Sábato y Mackenzie, 1982]; identificando métodos, materiales y abordaje metodológico necesarios para desarrollar el proyecto:

Métodos

A continuación se definen los métodos que se llevarán a cabo en el presente trabajo. Ellos son:

Revisiones Sistemáticas

Las revisiones sistemáticas [Argimón, 2004] de artículos científicos siguen un método explícito para resumir la información sobre determinado tema o problema. Se diferencia de las revisiones narrativas en que provienen de una pregunta estructurada y de un protocolo previamente realizado.

Prototipado Evolutivo Experimental (Método de la Ingeniería)

El prototipado evolutivo experimental [Basili, 1993] consiste en desarrollar una solución inicial para un determinado problema, generando su refinamiento de manera evolutiva por prueba de aplicación de dicha solución a casos de estudio (problemáticas) de complejidad creciente. El proceso de refinamiento concluye al estabilizarse el prototipo en evolución.

Materiales

Para el desarrollo de los formalismos y procesos propuestos se utilizarán:

Formalismos de modelado conceptual usuales en la Ingeniería de Software [Rumbaugh et al., 1999][Jacobson et al., 2013] y en la Ingeniería del Conocimiento [García-Martínez y Britos, 2004].

Modelos de Proceso usuales en Ingeniería de Software [IEEE, 1997; ANSI/IEEE, 2007; Oktaba et al., 2007].

Metodología

Para alcanzar los Objetivos trazados se propone: (i) realizar una investigación documental exploratoria acerca de las técnicas de hacking ético para la evaluación de vulnerabilidades más utilizados, identificando casos de estudio y de validación, (ii) realizar una valoración de las técnicas de hacking ético para la evaluación de vulnerabilidades estudiadas en base a una comparación de cada una de sus características en los casos de estudio relevados, especificando detalladamente las vulnerabilidades explotadas por cada técnica y la afectación potencial a un sistema, elaborando un ranking de acuerdo a la peligrosidad de cada una, (iii) realizar un estudio detallado de las fases del proceso de testeo de sistemas para determinar las actividades donde deberían incorporarse las técnicas de hacking ético, (iv) proponer un modelo integrador de proceso de testeo que incluya el hacking ético para la evaluación de vulnerabilidades, definiendo fases, actividades y recomendando herramientas, (v) realizar pruebas de concepto en los casos de estudio y casos de validación identificados, que validen el método propuesto.

RESULTADOS ESPERADOS

El presente proyecto busca desarrollar e incorporar un método de hacking ético para la evaluación de vulnerabilidades dentro del procedimiento mismo de Testeo de un sistema. De esta manera, se aporta a los encargados de testing en sectores de Seguridad Informática de un grupo de actividades y herramientas que les brinde el soporte necesario para poder prevenir los problemas que en la actualidad son de creciente interés por las pérdidas económicas que conllevan.

FORMACIÓN DE RECURSOS HUMANOS

El grupo de trabajo se encuentra formado por dos investigadores formados y tres investigadores en formación. En su marco se desarrollan dos Tesis de Maestría y dos Especializaciones en Sistemas de Información.

REFERENCIAS

ANSI/IEEE, (2007). Draft IEEE Standard for software and system test documentation. ANSI/IEEE Std P829-2007.

Argimón J. (2004). Métodos de Investigación Clínica y Epidemiológica. Elsevier España, S.A. ISBN 9788481747096.

Basili, V. (1993). The Experimental Paradigm in Software Engineering. En Experimental Software Engineering Issues: Critical Assessment and Future Directions (Ed. Rombach, H., Basili, V., Selby, R.). Lecture Notes in Computer Science, Vol. 706. ISBN 978-3-540-57092-9.

Comunidad Linux. 2014 <http://www.linux.org/> Página Válida a 05/2017

Coronel Suarez, I.A. (2016). Aplicar hackeo ético para detección de vulnerabilidades mediante herramientas Open Source en las aplicaciones web de una institución de educación superior. Tesis Maestría de la Escuela Superior Politécnica del Litoral. Repositorio Digital URI: <http://www.dspace.espol.edu.ec/xmlui/handle/123456789/37397>

Creswell, J. (2002). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research. Prentice Hall. ISBN 10: 01-3613-550-1.

Evans, Bob (2001). The Sorry State of Software. InformationWeek 112.

García Martínez, R., Britos, P. (2004). Ingeniería de Sistemas Expertos. Editorial Nueva Librería. ISBN 987-1104-15-4.

GNU (2014) Operating System Sponsored by the Free Software Foundation. 2014/05/15 <http://www.gnu.org/> Página Válida a 05/2017

Hurtado Sandoval, M.E., Mendaño Mendaño, L.A. (2016). Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado. Tesis Grado. Escuela Politécnica Nacional de Ecuador. Repositorio Digital URI: <http://bibdigital.epn.edu.ec/handle/15000/16836>

ISO 27035:2011 (2010). Information technology – Security techniques – Information security incident management. [Online]. http://www.iso.org/iso/catalogue_detail?csnumber=44379. Página Válida a 05/2017.

IEEE, (1997). IEEE Standard for Developing Software Life Cycle Processes. IEEE Std 1074-1997 (Revision of IEEE Std 1074-1995; Replaces IEEE Std 1074.1-1995)

Jacobson, I., Ng, P. W., McMah, P. E., & Jaramillo, C. M. Z. (2013). La esencia de la ingeniería de software: El núcleo de Semat. Revista Latinoamericana de Ingeniería de Software, 1(3), 71-78.

López Alvarez, D.M. (2015). Hacking ético para detección de vulnerabilidades de una empresa del sector de telecomunicaciones. Tesis Maestría de la Escuela Superior Politécnica del Litoral. Repositorio Digital URI: < http://www.dspace.espol.edu.ec/xmlui/handle/123456789/36478>

López Vallejo, M.R. (2017) Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN

1390-9304. <http://rmlconsultores.com/revista/index.php/crv/article/view/407/pdf_259> Página Válida a 05/2017

Mayorga Jácome, T., Quisaguano Belduma, F.J. (2015). Implementación de hacking ético para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red de la empresa Construlec Cía. Ltda. en Quito Ecuador. Editorial: Quito: Universidad Israel. Repositorio Digital URI: <http://repositorio.uisrael.edu.ec/handle/47000/647>

OISSG (2012) Open Information Systems Securty Group. 2003 – 2012 <http://www.oissg.org/> Página Válida a 05/2017

Oktaba, H., Garcia, F., Piattini, M., Ruiz, F., Pino, F., Alquicira, C. (2007). Software Process Improvement: The Competisoft Project. IEEE Computer, 40(10): 21-28. ISSN 0018-9162.

Onofa Calvopiña, F.O., Pilatuña Chica, I. (2016). Análisis y evaluación de riesgos y vulnerabilidades del nuevo portal web de la Escuela Politécnica Nacional, utilizando metodologías de hackeo ético. Tesis Grado. Escuela Politécnica Nacional de Ecuador. Repositorio Digital URI: <http://bibdigital.epn.edu.ec/handle/15000/16740>

OWASP Top 10 - 2013 (2013). [Online]. http://www.owasp.org. Página Válida a 05/2017.

Paillacho Pozo, P.A. (2016). Análisis, diseño y pruebas de hacking ético sobre la infraestructura institucional de la Superintendencia de Control del Poder de Mercado. Tesis Grado. Universidad Politécnica Salesiana de Ecuador. Repositorio Digital URI: <http://dspace.ups.edu.ec/handle/123456789/13425>

Palmer, Charles (2001). Ethical hacking, IBM Systems Journal, Vol. 40, N°3

Raymond E (1991). The New Hacker's Dictionary, MIT Press, Cambridge, MA

Riveros, H. y Rosas, L. (1985). El Método Científico Aplicado a las Ciencias Experimentales. Editorial Trillas. México. ISBN 96-8243-893-4.

Rumbaugh, J., Jacobson, I., Booch, G. (1999). The Unified Modeling Language, Reference Manual. Addison Wesley, ISBN-10: 02-0130-998-X.

Sabato J, Mackenzie M. (1982). La Producción de Tecnología: Autónoma o Transnacional. Instituto Latinoamericano de Estudios Transnacionales - Technology & Engineering. ISBN 9789684293489.

Santos Castañeda, D.M. (2016). Análisis y diagnóstico de vulnerabilidades informáticas en la red de datos de la empresa YOUPHONE Cía. Ltda. Utilizando Hacking Ético. Tesis Grado. Institucional de la Universidad de las Fuerzas Armadas ESPE. Repositorio Digital URI: <http://repositorio.espe.edu.ec/handle/21000/12142>

Schneier, Bruce. (2000). Secrets & Lies: Digital Security in a Networked World. John Wiley & Sons.

Sheoran, Pankaj & Singh, Sukhwinder (2014). Applications of Ethical Hacking, International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463 Vol. 3 Issue 5, May-2014, pp: (112-114), Impact Factor: 1.252, Available online at: www.erpublications.com Page | 112

Software Enginnering Institute (2014) – Carnegie Mellon University. 2014 <http://www.cert.org/tech_tips/malicius_code_mitigation.html> Página Válida a 05/2017

Tamayo Veintimilla, O.A. (2016). Desarrollo de una guía técnica estándar para aplicar herramientas de Ethical Hacking en redes de datos, dirigido a PYMES. Tesis Grado de Pontificia Universidad Católica de Ecuador. Facultad de Ingeniería. Escuela de Sistemas. Repositorio Digital URI: <http://repositorio.puce.edu.ec/handle/22000/12612>

Tenable Network Security (2014), provedora de la herramienta Nessus, 2014 <http://www.tenable.com/products/nessus?gclid=CK2xwJGavr4CFScHwwod9VMAZA> Página Válida a 05/2017

Tori C. (2008). Hacking Ético (1ra Ed). Buenos Aires: Mastroianni.

Zimmerman, Christine. (2001). Race to Deploy May Magnify Software Bugs. InternetWeek 13.