Metodología de explotación de vulnerabilidades para el incremento de la seguridad en aplicaciones Web

Ibar Mario Vásquez Ramos
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
ibar.sistemas@gmail.com

***Resumen*—Se presenta el proyecto de la metodología de explotación de vulnerabilidades para el incremento de la seguridad en aplicaciones web, la cual brindará herramientas para guiar el análisis de la seguridad informática en una determinada aplicación web mediante explotación de vulnerabilidades y mitigación de los riesgos que ellas implican.**

Palabras clave—explotación, vulnerabilidades, explotación, seguridad.

I. INTRODUCCIÓN

Hoy en día es normal y rutinario el leer noticias sobre intrusiones en alguna red privada o sistemas ajenos, esto sin el permiso previamente concedido. Por ende, es muy necesario saber las falencias de seguridad en cualquier aplicación web informática, para así poder securizarla y eliminar aquellas vulnerabilidades mediante las cuales cualquier individuo con conocimiento suficiente en informática podría aprovecharlas y perjudicarnos gravemente.

Uno de los pilares fundamentales para cualquier organización es la información, esta misma tomada muchas veces como el activo más valuado, no solo monetariamente sino como algo íntimo y confidencial de la empresa. Mantener la información a salvo garantizando su confidencialidad, integridad y disponibilidad "la triada CDI", son los principios básicos sobre los que se sustenta cualquier política de seguridad. Garantizar dichos principios requiere de una arquitectura de seguridad que tenga por objetivo proteger los activos de información mediante un conjunto de estándares, procedimientos y controles.

A. Antecedentes

En Bolivia no se tiene promulgada ninguna ley completa referente al tema de delitos informáticos, pero si tenemos algunos artículos dentro del código penal donde si se indican sanciones, por ejemplo:

El Código Penal Boliviano tipifica la Manipulación Informática (art. 363 bis) y la Alteración, acceso y uso indebido de datos informáticos (363 ter.) como delito. Otro delito que se tiene tipificado es el acoso cibernético. "Esta es una nueva figura legal que ha sido incluida en el Código Niño, Niña Adolescente, aprobado el 2015 en la Asamblea Legislativa Plurinacional", dice. La pena para quienes incurran en este delito será de entre cuatro y ochos años de privación de libertad.

Sin embargo, existen otros delitos conexos a la informática que son las formas más frecuentes; es decir, formas delincuenciales cometidas utilizando medios informáticos (SMS, redes sociales, sitio web, blogs), como el robo de información, suplantación de identidad, difamación, injurias o calumnias por internet y pornografía, entre otros.

Al momento no se tiene establecido si las pruebas de testeo a vulnerabilidades son o no permitidos como en otros países, por ello q tendríamos una selva tecnológica boliviana en la que solo dominaría la ley del más fuerte en este caso un administrador de seguridad informática debe estar preparado y protegido para cualquier incidente por sí mismo ya que actualmente en nuestro medio, no hay norma bien establecida al respecto.

Los continuos ataques a empresas, corporaciones e instituciones ya sean estatales o privadas han sido la preocupación de muchas personas siendo este un tema muy delicado debido a las consecuencias del mismo.

Los administradores de seguridad informática, encargados de unidad, jefes de las unidades de sistemas son responsables del buen funcionamiento de su red, buscan medios de verificación de vulnerabilidades para de alguna manera poder tener preparación previa ante una eventualidad y contar con contramedidas necesarias.

Se debe tomar en cuenta que muchos estudios indican que más del 80% de los ataques se realizan internamente desde la misma red LAN y para ello debemos enfocarnos más en asegurar tanto el ambiente interno como externo de las aplicaciones web.

B. Problemática

Muchas empresas, cuentan con aplicaciones sin normas de seguridad, no se basan en ningún tipo de control preventivo, ni correctivo, ni emplean tiempo específico para la realización de un correcto análisis y mitigación de vulnerabilidades a sus aplicaciones.

C. Objetivo general

Crear una metodología de explotación de vulnerabilidades con herramientas que guíen el aseguramiento de aplicaciones web, brindando al analista, técnicas de hallazgo de vulnerabilidades en aplicaciones web, técnicas inmersas en una metodología que le permita tomar decisiones sobre acciones y mejoras en las políticas de seguridad.

Para referenciar este artículo (IEEE):

[N] I. Vásquez, «Metodología de explotación de vulnerabilidades para el incremento de la seguridad en aplicaciones Web,» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 47-48, 2020.

D. Alcances

La investigación se enfocará en realizar el estudio y análisis de la explotación de vulnerabilidades en aplicaciones web mediante esta nueva metodología, de esta manera se logrará incrementar la seguridad en la red que se aplique. Con el empleo de la metodología se quiere llegar a la máxima seguridad en una aplicación incrementando su seguridad.

E. Justificación

Para todo administrador de seguridad informática es necesario el conocimiento de vías de acceso, manipulación de vulnerabilidades, de acuerdo a necesidades con un estudio de riesgos y seguridad.

Denotamos que lo nuevo que tiene la metodología de explotación de vulnerabilidades en comparación a otras es que tiene un enfoque mucho más técnico y práctico ya que otras como MAGERIT son más administrativas y de gestión siendo así más aplicativa. También debemos tomar en cuenta que actualmente existen varias metodologías para desarrollo de software, pero no así en gran cantidad de seguridad de información y protección a sistemas. Existen normas como la ISO 27001 con sus variantes, estas indican desde un punto de vista de gestión, que se debería cumplir para lograr un aseguramiento efectivo de los activos informáticos, pero no así que técnicas y herramientas existen actualmente en nuestro medio para ser aplicadas en esas tareas.

Dar un aporte a la sociedad dejando lo creado con licencia GPL de todo lo realizado en la presente tesis con el objetivo de dar un aporte al ámbito tecnológico y académico para su futuro estudio, posible continuidad y análisis.

II. Métodos

Es una investigación exploratoria, que es aplicable cuando el objeto de estudio es un tema o problema de investigación poco estudiado, pero no nuevo ya que existen metodologías del mismo ámbito como, por ejemplo: ISSAF, OSSTMM, OWASP, PTES, y la misma NIST SP800-115.

Se buscaron bastantes referentes al respecto sin embargo no se logró encontrar un documento realizado específicamente a la explotación de vulnerabilidades por lo tanto este fue el causal para incursionar el presente documento en esa vía.

III. Resultados esperados

A. Adaptación de MAGERIT para la metodología de explotación de vulnerabilidades

Debido a que MAGERIT realiza una gestión del riesgo que podría ser provocado por vulnerabilidades, la gestión del mismo es indispensable para lograr una buena mitigación de los mismos, por lo tanto, se persigue los siguientes objetivos:

a) Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de mitigarlos a tiempo.
b) Ofrecer un método sistemático para analizar riesgos encontrados.
c) Ayudar a descubrir y planificar las medidas oportunas para mitigar los riesgos.
d) Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación.

Supervisa los siguientes factores:

a) Actitud general de los miembros del equipo basándose en las presiones del proyecto.
b) El grado de compenetración del equipo.
c) Relaciones interpersonales entre los miembros del equipo.

B. Uso de herramientas de seguridad informática

La metodología menciona el uso de herramientas para el incremento de seguridad en aspectos de administración de redes [1]. Así también de pautas y guías en el ámbito de las aplicaciones web para la realización de auditorías [2][6]. La gestión de la seguridad informática desde un punto de vista por acceso web [3]. Prueba pentesting que se debería realizar a cualquier aplicación web expuesta a LAN o WAN se debe analizar mediante herramientas avanzadas de penetración (Exploit), mismos que van actualizándose de acuerdo a las nuevas vulnerabilidades descubiertas día a día [4][5].

IV. Conclusiones

De este análisis se ha logrado determinar que la metodología puede brindar herramientas útiles para el análisis de vulnerabilidades y de esta manera coadyuvar la elaboración de informes y contramedidas que se deben asumir a la hora de implementar políticas de seguridad.

El autor de la presente continuará con la actualización del presente estudio.

Referencias

[1] Dnsknowledge. DNS Autoritativo, DNS. [En línea] 2000. http://dnsknowledge.com/whatis/authoritative-name-server/. 2000.

[2] Echenique, J. Auditoria en Informática. s.l.: Editorial McGraw Hill, 2001.

[3] El portal de ISO 27001 en español. 2012. [En línea] 2012. www.iso27001.es.

[4] Metasploit_Developer_Guide, Comunidad. 2012. Metasploit Web Official-Developer Guide. [En línea] 2012. http://dev.metasploit.com/redmine/projects/framework/wiki/DeveloperGuide.

[5] Mitnick., K. 2005. The Art of Intrusion.: Wiley Publishing Inc., 2005.

[6] Portal ISACA (Information Systems Audit and Control Association). 2012.

Breve CV del autor

Ibar Mario Vásquez Ramos es Ingeniero de Sistemas, Maestría MBA en DAE, certificación internacional ISO 27001 como Lead Implementor, estudios MTCNA, CCNA, DBA. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoría de Sistemas en el PGI-UMSA. Más de 8 años en ethical hacking, administración de herramientas de seguridad informática y análisis de riesgos. Actualmente trabaja como Analista de Riesgo Tecnológico en BMSC S.A. Email: ibar.sistemas@gmail.com.