Metodologías Ethical Hacking

Leidi Stefani Valencia Blanco
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
Leiste.f@hotmail.com

RESUMEN

El presente artículo trata de darnos un vistazo a las principales y más usadas metodologías que existen para realizar una práctica correcta en el área de Ethical Hacking.

El Ethical Hacking, es de las especializaciones de seguridad informática más apetecidas por las empresas a nivel mundial, todos los días crece la necesidad de tener personas con los principales conocimientos es estas áreas, para contrarrestar los ataques de la creciente comunidad de Hackers, la cual tiene mayor representación en Asia y Medio Oriente, pero que esta regada por todo el mundo.

Palabras Clave

Metodología, vulnerabilidades, riesgos y seguridad.

1. INTRODUCCIÓN

Es muy delgada la línea entre un hacker de sombrero blanco y un hacker de sombrero negro, a nivel de conocimientos ambos tienen la capacidad de reconocer vulnerabilidades y/o fallos en sistemas, para sacar provecho de la situación, el hacker ético tiene como misión explotar estas vulnerabilidades y reportar las mismas, el fin nunca es el sacar provecho económico de la situación, por lo contrario el objetivo es hacer recomendaciones y/o diseñar controles para la mejora del sistema.

Las metodologías más usadas en el Ethical Hacking son las siguientes:

2. OSSTMM (FUENTE ABIERTA DE SEGURIDAD MANUAL DE MÉTODOS DE PRUEBA)

Fig. 1 Logotipo OSSTMM

Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, a estos niveles de seguridad se le denominan comúnmente “Dimensiones de Seguridad” y normalmente consiste en analizar los siguientes factores.

- ✓ Visibilidad
- ✓ Acceso
- ✓ Confianza
- ✓ Autenticación
- ✓ Confidencialidad
- ✓ Privacidad
- ✓ Autorización
- ✓ Integridad
- ✓ Seguridad
- ✓ Alarma

Como parte de un trabajo secuencial la metodología OSSTMM consta de 6 ítems los cuales comprenden todo sistema actual, estos son:

- ✓ Seguridad de la Información
- ✓ Seguridad de los Procesos
- ✓ Seguridad en las tecnologías de Internet
- ✓ Seguridad en las comunicaciones
- ✓ Seguridad inalámbrica
- ✓ Seguridad Física

3. ISSAF (MARCO DE EVALUACIÓN EN SISTEMAS DE INFORMACIÓN DE SEGURIDAD)

Fig. 2 Logotipo ISSAF

Marco metodológico de trabajo desarrollado por la OISSG que permite clasificar la información de la evaluación de seguridad en diversos dominios usando diferentes criterios de prueba. Algunas de las características más representativas de ISSAF son:

Brinda medidas que permiten reflejar las condiciones de escenarios reales para las evaluaciones de seguridad.

Esta metodología se encuentra principalmente enfocada en cubrir los procesos de seguridad y la evaluación de los mismos para así obtener un panorama completo de las vulnerabilidades existentes.

Permite el desarrollo de matriz de riesgo para verificar la efectividad en la implementación de controles.

4. OWASP (SOLICITUD DEL PROYECTO DE SEGURIDAD OPEN WEB)

Fig. 3 Logotipo OWASP

Metodología de pruebas enfocada en la seguridad de aplicaciones, El marco de trabajo descrito en este documento pretende alentar a las personas a evaluar y tomar una medida de la seguridad a través de todo el proceso de desarrollo. Así, pueden relacionar los costes de un software inseguro al impacto que tiene en su negocio, y de este modo gestionar decisiones de negocio apropiadas (recursos) para la gestión del riesgo, algunas de las características más representativas de OWASP son:

- ✓ Pruebas de firma digital de aplicaciones Web.
- ✓ Comprobaciones del sistema de autenticación.
- ✓ Pruebas de Cross Site Scripting.
- ✓ Inyección XML
- ✓ Inyección SOAP
- ✓ HTTP Smuggling
- ✓ Sql Injection
- ✓ LDAP Injection
- ✓ Polución de Parámetros
- ✓ Cookie Hijacking
- ✓ Cross Site Request Forgery

5. CEH (ETHICAL HACKING CERTIFICADO)

Fig. 4 Logotipo CEH

Metodología de pruebas de seguridad desarrollada por el International Council of Electronic Commerce Consultants (EC-Council) algunas de las fases enunciadas en esta metodología son:

- ✓ Obtención de Información.
- ✓ Obtención de acceso.
- ✓ Enumeración.
- ✓ Escala de privilegios.
- ✓ Reporte

6. OFENSIVA DE SEGURIDAD

Fig. 5 Logotipo OFFENSIVE SECURITY

Metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, la metodología contempla principalmente los métodos para el desarrollo de estudios de seguridad enfocados en seguridad ofensiva y teniendo como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades, las principales ventajas de adoptar este marco metodológico son:

- ✓ Enfoque sobre la explotación real de las plataformas.
- ✓ Enfoque altamente intrusivo.
- ✓ Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.

7. CONCLUSIÓN

El resultado de la violación de los sistemas y las redes de informáticas en todo el mundo ha provocado la pérdida o modificación de los datos sensibles a las organizaciones, representando daños que se traducen en miles o millones de dólares.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial y por qué no existe conocimiento relacionado con la planeación de un sistema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

Podemos afirmar entonces que las metodologías para Ethical Hacking nos ayudan a alcanzar una seguridad informática apropiada para cualquier red o sistema, sin duda alguna, las empresas que se dedican a estos menesteres, jugando un rol importante en esta área de Ethical Hacking.

8. REFERENCIAS

[14] La Seguridad Informática Hoy (Disponible en:) http://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html (Fecha de Búsqueda: 04/05/2013)

[15] Ethical hacking: Test de intrusion. Principales metodologías (Disponible en:) http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtml (Fecha de Búsqueda: 04/05/2013)