OSSTMM 3

M. Sc. Aldo Valdez Alvarado
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
aldo_valdez@hotmail.com
arvaldez@umsa.bo

RESUMEN

Este artículo presenta una introducción al Manual de la Metodología Abierta de Testeo de Seguridad en su Versión 3, estándar de facto en la realización de auditorías de seguridad.

Palabras Clave

OSSTMM, ISECOM, Seguridad, Test, Intrusión.

1. INTRODUCCIÓN

El OSSTMM por sus siglas en inglés "Open Source Security Testing Methodology Manual" o "Manual de la Metodología Abierta de Testeo de Seguridad" tal como fue nombrada oficialmente suversión en español, es uno de los estándares profesionales mas completos y comúnmente utilizados a la hora de revisar la Seguridad de los Sistemas desde Internet.

Creado en 2001 por Pete Herzog, Director Ejecutivo de ISECOM (Instituto para la Seguridad y Metodologías Abiertas), y fruto del esfuerzo ininterrumpido de más de ciento cincuenta colaboradores directos, quienes junta a la comunidad de profesionales en seguridad en su conjunto, con tribuyeron con conocimiento, experiencia y horas de revisión de este proyecto.

Este manual también contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001 – 27002 e ITIL entre otras, lo que la hace uno de los manuales mas completos en cuanto a la aplicación de pruebas a la seguridad de la información en las instituciones.

A continuación, se presenta la versión 3 de este manual, que presenta muchas mejoras algunas a partir de la versión 2.2, particularmente relacionadas al manejo de riesgos y otras relacionadas con el uso de algunos test de manera mejorada y ampliada.

2. OSSTMM 3

2.1 Propósito

Su principal propósito es proveer de una metodología científica para examinar la organización, realizando pruebas sobre la seguridad de adentro hacia afuera.

Un segundo propósito es proveer guías para el auditor de sistemas, destinadas a la certificación de la organización en cuanto a los requisitos del ISECOM.

El Documento provee una serie de descripciones específicas para el desarrollo de un test de seguridad operacional sobre todos los canales incluyendo aspectos físicos, humanos, telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra descripción derivada de una métrica real.

2.2 Tipos de test

Las pruebas de seguridad pueden abarcar todas las formas y tipos, que van desde la intrusión, hasta la auditoria guiada. El OSSTMM contempla seis tipos de test.

- Blindaje o Hacking Ético.
- Doble blindaje, auditoría de Caja Negra o Pruebas de Penetración.
- De Caja Gris.
- De Doble Caja Gris.
- Test Tándem o Secuencial.
- Inverso

2.3 Ámbito o competencia

El ámbito debe abarcar toda la seguridad operativa, y comprometerse en las diferentes áreas o canales como lo describe el manual, y se observa en la siguiente tabla:

Canal	Sección	Descripción
Seguridad Física	Humano	Todos aquellos comprometidos con la organización
	Físico	Objetos tangibles de la organización
Seguridad de las comunicaciones	Redes de datos	Sistemas electrónicos y redes de datos.
	Telecomunicaciones	Comunicaciones digitales y analógicas.
Seguridad del Espectro electromagnético	Comunicaciones inalámbricas	Señales Electromagnéticas empleadas.

Tabla 1. Ámbito del Manual

2.4 Módulos

El flujo de este manual OSSTMM comienza con determinar la situación objetivo, esta situación esta determinada por la cultura, reglas, normas, regulaciones, legislación y políticas definidas en esta. La metodología propone un modelo jerárquico de Canales, Módulos y

Tareas, donde los vectores son simplemente las líneas de análisis que apuntan a cada uno de los canales.
Los módulos son áreas específicas de cada canal, pudiendo encontrar actividades que se encuentran en la frontera entre dos canales.

2.5 Esquema General

El esquema general del proceso de las pruebas de seguridad presenta las siguientes fases:

- Fase de Reglamentación. Se establece la dirección de las pruebas, el auditor comprende los requisitos, el alcance y las limitaciones de la auditoría. En esta fase se considera: la postura de la revisión, la logística, y la detección activa de verificación.
- Fase de Definición. Se define el ámbito de la aplicación. La base de las pruebas de seguridad requiere el conocer el alcance y el ámbito en relación de los objetivos y activos. En esta fase se considera la visibilidad de la auditoria, la verificación de accesos, de confianza, de controles.
- Fase de Información. El auditor va descubriendo información, donde la intención es descubrir la mala gestión de la información. En esta fase se considera la verificación de procesos, de configuración, la validación de propiedad, una revisión de segregación y de exposición, una exploración de la Inteligencia Competitiva.
- Fase Interactiva de Pruebas de Controles. Estas se centran en la penetración y perturbación. Es por lo regular la fase final de las pruebas de seguridad, y esta no puede realizarse mientras las otras no se hayan realizado. En esta fase se considera la verificación de la cuarentena, la auditoria de privilegios, la validación de sobrevivencia, revisión de alertas y registros

3. CONCLUSIONES

Como se observa el Manual para la Metodología Abierta de Testeo de Seguridad, tiene una estructura esquemática muy completa para el análisis de seguridad, en las organizaciones, tanto por expertos en seguridad de TI, como también de auditores de seguridad..

4. BIBLIOGRAFÍA

[16] DragoJAR. OSSTMM. Manual de la Metodología Abierta de Testeo de Seguridad [en línea]. [Disponible en:] http://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml. [Fecha de búsqueda:] Mayo de 2013.

[17] Garcia, L. Metodología OSSTMM [en línea]. [Disponible en:] http://www.securitybydefault.com/2010/03/metodologia-osstmm.html. [Fecha de búsqueda:] Mayo de 2013.

[18] Gregg, M.Certified Ethical Hacker. 2006. Que Publishing. USA.

[19] Herzog, P. OSTMM 3 The Open Source Security Testing Methodology Manual. 2010. ISECOM.

Racciati, H. OSSTMM 3. Una Introducción [en línea]. [Disponible en:] http://hernanracciatti.blogspot.com. [Fecha de búsqueda:] Mayo de 2013