ANALISIS DE RIESGOS INFORMÁTICOS

Ezaleth Emith Serrano**.**
Facultad de Ingeniería, Estudiantes Ingeniería de sistemas, Universidad Nacional Abierta y a Distancia, Colombia.

***Abstracto*—La empresa ha tenido en el último año inconvenientes con sus sistemas de información y redes de comunicaciones en sus diferentes sedes por todo el mundo.**
El equipo de dirección estratégica, junto con el área de tecnológica, se ha reunido para buscar una solución de fondo. Su negocio está siendo afectado por la pérdida de información crítica, que se ha filtrado a la competencia y por la disponibilidad de sus sistemas ha afectado los tiempos de respuesta hacia el cliente. Además, esta situación ha afectado la productividad, y todo esto ha repercutido en el no cumplimiento sus metas trimestrales en ventas. Por tanto, el equipo ha decidido buscar un grupo de expertos externos que le brinde los servicios de auditoría de sistemas y les presente una metodología para desarrollar al interior de la organización un Ethical Hacking focalizado sobre los sistemas informáticos que corren sobre diferentes sistemas operativos para implementar las respectivas mejoras y controles.

1. INTRODUCCIÓN

A Pesar que los empresarios realizan grandes inversiones a fin de tener productos y servicios que salvaguarden la información interna y confidencial que se maneja en ella, de modo que no se pierdan o se dañen – sea por error o con intención –, no se dan a la tarea de verificar las consecuencias reales de un ataque a los sistemas de información.
Por esto mismo, es que se recomienda hacer periódicamente pruebas de intrusión a fin de evaluar las repercusiones reales de cada una de las vulnerabilidades que existen y el alcance de las mismas.

Para tal fin, es que existen metodologías que preparan escenarios que ponen a prueba las técnicas y habilidades de los ataques [1] y que, por ser abiertas, no presentan problemas si son modificadas o distribuidas. Por lo anterior, en este documento se basa en la recopilación de información de 5 de las principales metodologías abiertas y la forma en que podría ayudar a solucionar los problemas que actualmente se presentan en SO Solutions.

2. PRUEBAS DE INTRUSIÓN

Las pruebas de intrusión se basan en probar los métodos de protección del sistema de información, sometiendo el sistema a una situación real.

Generalmente se usan tres métodos:

A. Método de caja negra

Consiste en intentar ingresar al sistema con los mismos recursos que un hacker tendría. El auditor solo dispone de información pública y realiza ataques controlados para detectar vulnerabilidades. Una vez las detecta, se procede a la corrección o implantación de métodos de protección.

B. Método de caja blanca

Para este caso, el auditor posee información necesaria para evaluar mejor la seguridad del entorno, sometiendo a prueba, incluyendo códigos fuente, archivos de configuración, documentación, etc.

C. Tamaños y Tipos de Fuente

En este test se combinan los dos test anteriores; realiza ataques similares a los de caja negra. La diferencia es que se dispone información técnica sobre el sistema. Es efectivo para poder identificar un mayor número de amenazas. [2]

Una vez se evidencias las vulnerabilidades, se precisa realizar una clasificación de las mismas. Para llevar a cabo este proceso, el Forum of Incident Response and Security Teams (FIRST), plantea un modelo topológico basado en métricas cualitativas, temporales y del entorno, como se muestra a continuación [3]:

TABLA I
TOPOLOGÍA BASADA EN MÉTRICAS PARA CLASIFICAR VULNERABILIDADES.

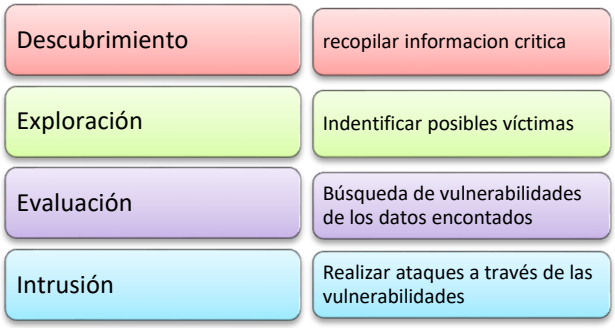
Grupos	Métricas	Tipos
Métricas Base	Vector de Acceso	▪ Locales ▪ Red Local ▪ Remotos
	Complejidad de Acceso	▪ Alta ... Baja
	Autenticación	▪ Simple ▪ Múltiple ▪ Ninguna
	Impacto en la Confidencialidad	▪ Alta ... Baja
	Impacto en la Integridad	▪ Alta ... Baja
	Impacto en la Disponibilidad	▪ Alta ... Baja
Métricas Temporales	Explotabilidad	▪ Explotable ▪ No Explotable
	Facilidad de Corrección	▪ Corrección Fácil ▪ Corrección Compleja ▪ No Existe Corrección
	Fiabilidad del Informe de Vulnerabilidad	▪ Identificada y Confirmada ▪ Identificada sin Confirmar ▪ Sin Fuentes
Métricas del Entorno	Daños Colaterales	▪ Alta ... Baja
	Distribución de Equipos Vulnerables	▪ Alta ... Baja
	Requisitos de Seguridad	▪ Alta ... Baja

Es necesario tener en cuenta que el nivel de criticidad de las vulnerabilidades depende en gran medida del contexto de la organización en particular, los controles compensatorios que existan y el nivel del riesgo que implica [4]

3. METODOLOGÍAS ABIERTAS

los test de penetración constan de 4 etapas y deben ser conocidas por el atacante para comprometer la seguridad del sistema de información [5]:

Figura 1. Fases de metodologías.



Una metodología define un conjunto de reglas prácticas y conocimientos que son ejecutados durante el procedimiento de evaluación de los programas de seguridad de la información [6]

A. OWASP (Open Web Application Security Project)

La guia de pruebas se divide en dos partes: una pasiva y otra activa. En la primera de ellas, el evaluador junta la información a través de múltiples herramientas a fin de encontrar la lógica de la aplicación, mientras que en la segunda, empieza a realizar las pruebas usando la metologia que se compone de subcategorías y se relacionan a continuación:

TABLA II
Subcategorías y actividades de la guía de pruebas OWASP [7]

Categoría	Actividades
Recopilación de información	Pruebas de firma digital de Aplicaciones Web
	Descubrimiento de aplicaciones
	Técnicas de spidering y googling
	Análisis de códigos de error
	Pruebas de gestión de configuración de la infraestructura
	Pruebas del receptor de escucha de la BBDD
	Pruebas de la gestión de configuración de la aplicación
	Pruebas de manejo de extensión de archivos
	Archivos antiguos, sin referencias y copias de seguridad
Comprobación de la lógica del negocio	Reglas de negocio: políticas del negocio
	Flujos de trabajo: tareas ordenadas de paso de documentos o datos de un elemento
	participante a otro
Pruebas de autenticación	Pruebas de diccionario sobre cuentas de usuario o cuentas por defecto
	Fuerza bruta
	Saltarse el sistema de autenticación
	Atravesar directorios/acceder a archivos adjuntos externos
	Sistemas de recordatorio/reset de contraseñas vulnerables
Pruebas de gestión de sesiones	Análisis del esquema de gestión de sesiones
	Manipulación de cookies y testigos de sesión
	Variables de sesión expuestas
	Abuso de sesión
	Exploit HTTP
	Pruebas de CSRF (Cross Site Request Forgery)
Pruebas de validación de datos	Cross Site Scripting
	Métodos HTTP y XST
	Inyección SQL
	Inyección LDAP
	Inyección ORM

	Inyección XML
	Inyección SSI
	Inyección Xpath
	Inyección IMAP/SMTP
	Inyección de código
	Inserción de comandos del sistema operativo
	Prueba de desbordamiento de Búfer
	Pruebas de vulnerabilidad incubada
Pruebas de denegación de servicio	Bloqueo de cuentas de usuario
	Desbordamiento de Búfer
	Reserva de objetos especificada por usuarios
	Pruebas de uso de entradas de usuario como bucle
	Pruebas de escritura de entradas suministradas por usuario a disco
	Fallos en la liberación de recursos
	Pruebas de almacenamiento excesivo en la sesión
Comprobación de servicios web	Pruebas estructurales de XML
	Comprobación de XML a nivel de contenido
	Comprobación de parámetros HTTP GET/REST (Representational State Transfer)
	Adjuntos SOAP maliciosos
	Pruebas de repetición
Pruebas de AJAX (este tipo de aplicaciones tienen mayor superficie de ataque debido a que se extienden entre el cliente y el servidor)	Inyección SQL
	Cross Site Scripting
	La explotación de XSS
	Inyección DOM (Modelo de Objeto de Documentos)
	Inyecciones JSON/XML/XSLT
	Cross Site Request Forgery (CSRF)
	Denegación de Servicio

B. NIST SP 800-115

Esta metodología propone 4 fases: planificación, descubrimiento, ejecución del ataque y presentación de informes.

Para determinar el nivel de acceso que puede tener un atacante, se deben llevar a cabo pruebas sobre multiples sistemas y tener retroalimentación entre la fase de ataque y descubrimiento.

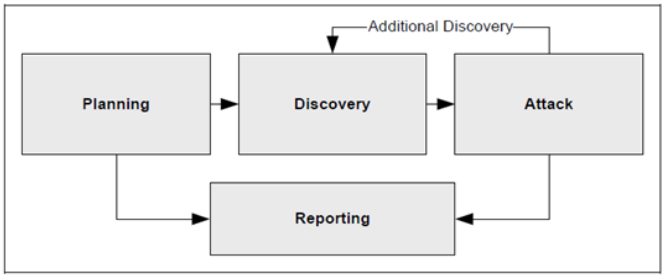


Figura 2. Metodología NIST SP 800-115

C. OSSTMM 3 (ISE-COM)

Representa un estándar de referencia imprescindible para llevar a cabo un test de seguridad de forma ordenada y con calidad profesional.

Se divide en cinco canales: humano, físico, redes inalámbricas, telecomunicaciones y redes de datos [8].

Consta de 4 fases y diecisiete módulos, que tienen cada uno sus tareas y procedimientos, dependiendo del canal que se está evaluando. [9]

TABLA III
Fases y Módulos de la Metodología OSSTMM

FASE	MÓDULOS	DESCRIPCION
Fase de Inducción	Revisión de Postura	La revisión de la cultura, reglas, normas, reglamentos, leyes y políticas aplicables al objetivo. Define el alcance y qué pruebas deben hacerse. Requerido para realizar de manera correcta la Fase C.
	Logística	La medición de las limitaciones de interacciones tales como: la distancia, velocidad, y la falibilidad de determinar los márgenes de exactitud en los resultados.
	Verificación de la Detección Activa	La verificación de la práctica y la amplitud de detección de interacciones, y la previsibilidad de respuesta. Para conocer las restricciones impuestas a las pruebas interactivas y llevar adecuadamente las Fases B y D.
Fase de Interacción	Auditoría de la Visibilidad	La determinación de los objetivos que van a ser probados dentro del ámbito. La visibilidad es considerada como "presencia" y no se limita a la vista humana.
	Verificación de Acceso	La medición de la amplitud y profundidad de los puntos de acceso interactivos dentro del objetivo y la autenticación necesaria
	Verificación de la Confianza	La determinación de las relaciones de confianza de y entre los objetivos. Una relación de confianza existe donde quiera que el objetivo acepta la interacción entre los objetivos en el ámbito de aplicación.
	Verificación de los Controles	La medición de la utilización y eficacia de los controles de pérdida basados en procesos: el no repudio, confidencialidad, privacidad e integridad. El control de alarma se verifica al final de la metodología.
Fase de Investigación	Verificación de los Procesos	La determinación de la existencia y eficacia del registro y mantenimiento de los actuales niveles de seguridad se define por la revisión de la postura y los controles de indemnización. La mayoría de los procesos tienen definidos un conjunto de reglas; sin embargo, las operaciones reales no reflejan ninguna eficiencia, por lo tanto, es necesario redefinir las reglas establecidas.
	Verificación de Configuración/ Verificación de la Capacitación	La investigación del estado estable (funcionamiento normal) de los objetivos tal como han sido diseñados para funcionar en condiciones normales para determinar problemas de fondo fuera de la aplicación de pruebas de stress de seguridad.
	Validación de Propiedad	La medición de la amplitud y profundidad en el uso de la propiedad intelectual ilegales o sin licencia o aplicaciones dentro del objetivo
	Revisión de la Segregación	La determinación de los niveles de identificación de información personal definido por la revisión de la postura. Sabemos cuáles son los derechos de privacidad que se aplican y en qué medida la información detectada como personal puede ser clasificados con base en estos requisitos.
	Verificación de la Exposición	La búsqueda de información libremente disponible que describe la visibilidad indirecta de los objetivos o los activos en el canal elegido por el alcance.
	Exploración de Inteligencia Competitiva	La búsqueda de información libremente disponible, directa o indirectamente, que podría perjudicar o afectar negativamente al propietario del objetivo a través de medios externos. Descubrir información que por sí sola o en conjunto puede influir en las decisiones de negocios.
Fase de Intervención	Verificación de la Cuarentena	La determinación y la medición del uso eficaz de la cuarentena para todos los accesos hacia y dentro del objetivo. Determinar la

		efectividad de los controles de autenticación y el sometimiento en términos de cuarentena de listas blancas y negras.
	Auditoría de Privilegios	El mapeo y la medición del impacto del mal uso de los controles de sometimiento, las credenciales y los privilegios o la escalada no autorizada de privilegios. Determinar la eficacia de la autorización en los controles de autenticación, la indemnización, y el sometimiento en términos de profundidad y roles.
	Validación de la Supervivencia/ Continuidad del Servicio	La determinación y la medición de la resistencia del objetivo a los cambios excesivos o adversos (Denegación de Servicios) en los controles de continuidad y la capacidad de recuperación que se verían afectados.
	Revisión de Alertas y Registros/Estudio Final	Una revisión de las actividades de auditoría realizadas con la verdadera profundidad de las actividades según lo registrado por el objetivo o por un tercero como control de alarma. Se pretende saber que partes de la auditoría dejó un rastro útil confiable.

D. PTF – ISSAF

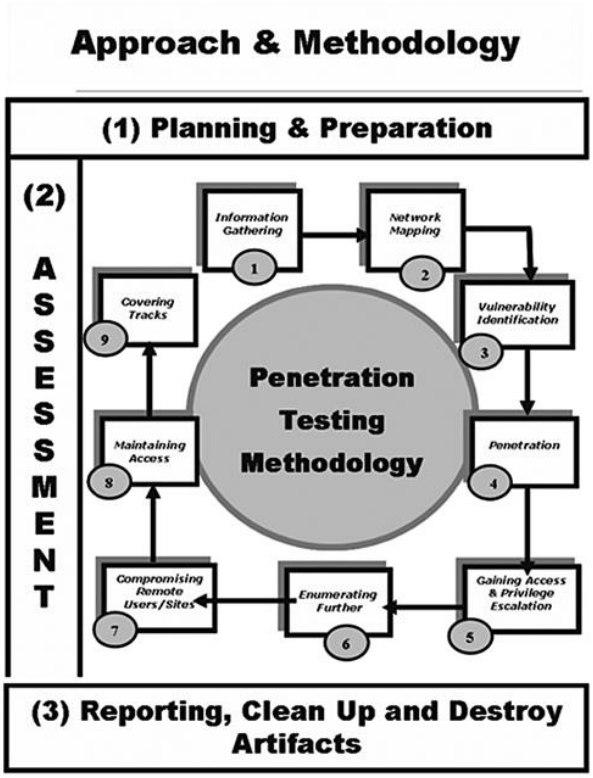
Esta metodología consta de 3 fases en las cuales, los pasos de ejecución son cíclicos e iterativos [10]:

Fase 1: Planificación y preparación: en esta fase se planean los aspectos relevantes de las pruebas que se consideran realizar y se debe firmar un acuerdo formal donde se detallen los mismos.

Fase 2: Evaluación: Presenta un enfoque por capas en el que cada una, representa un mayor nivel de acceso a la información.

Fase 3: Informe, limpieza y destrucción de información: Una vez culminadas todas las pruebas programadas, se debe generar un informe que contenga el resumen de los resultados, detallando cada punto y generando recomendaciones. Además, si se encuentran falencias en la seguridad se debe informar de forma inmediata y, al finalizar, destruir todos los archivos generados para evitar futuros inconvenientes.

Figura 2. Metodología ISSAF



Fuente: OISSG, Information System Security Assessment Framework (ISSAF), Penetration Testing Framework (PTF), 2006.

4. Reconocimientos

De acuerdo a las problemáticas presentadas en la compañía SO Solutions, implementar una de las técnicas presentadas anteriormente es el primer paso para aumentar el nivel de seguridad de la información.

La metodología NIST SP 800-115, podría ser, en comienzo, una buena forma de proceder, pues, contiene pasos importantes que las demás también, pero contiene una retroalimentación, punto favorable a la hora de solucionar huecos en seguridad.

5. Referencias

[1] J. Rivera, Ciclo de vida de una prueba de intrusión física, Universidad San Carlos de Guatemala, Guatemala, 2011.
[2] Sofisrtic, Test de Intrusión, [on line] Disponible en https://www.sofistic.com/auditoria/test-de-intrusion/.
[3] P. Mell, K. Scarfone, S. Romanosky, A Complete Guide to the Common Vulnerability Scoring System, 2007.
[4] H. Jara, F. Pacheco, Ethical hacking 2.0, Fox Andina, Buenos Aires.
[5] D. Monrroy, Análisis inicial de la anatomía de un ataque a un sistema informático. [Online]. Disponible en http://www.segu-info.com.ar/tesis/.
[6] J. Bolívar, C. Villarroel, Propuesta de Best Practice para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red del laboratorio de sistemas, Escuela Superior Politécnica de Chimborazo, Riobamba, 2012.
[7] Slideshare, Guia de pruebas OWASP, [online] Disponible en: https://es.slideshare.net/ragazome/gua-de-pruebas-owasp-v20
[8] ISECOM, OSSTMM 3 – The Open Source Security Testing Methodology Manual, 2009
[9] OSSTMM 3, the Open source security testing methodology manual. Herzog. [online] Disponible en http://www.isecom.org/mirror/OSSTMM.3.pdf
[10] OISSG, Information System Security Assessment Framework (ISSAF), Penetration Testing Framework (PTF), 2006
[11] Pruebas de Intrusion y metodologías abiertas. Pinzon, L. Octubre 2013. Revista ciencia, innovación y tecnología.