INTRUSION TEST AND OPEN SOURCE METHODOLOGIES

Article Information:

Received: October 16, 2013
Accepted: December 9, 2013

Keywords: Open source methodology, Penetration test, Security, Vulnerability assessment.

Abstract: Due to the growth of the attacks on the infrastructure of information technology and communications (TIC) which for 2012 was increased by 42% reaching, for example, in the case of the attacks on websites 190.370 daily attacks, according to information of Symantec Corporation (2013). The TI managers have seen the need to conduct periodic penetration testing in each of the important elements of your infrastructure, this kind of practice seeks to act proactively to shield the internal information and the customers information and also to prevent malicious staff can to appropriate of the information, taking economic advantage or causing damage in the data.

Therefore, this article presents a review and analysis of some sources of information about penetration testing and the main open methodologies that currently exist, in order to publicize the importance of implementing this kind of security assessments framed in a methodology that engages the needs of the company and it becomes a support to achieve their business goals.

PRUEBAS DE INTRUSIÓN Y METODOLOGÍAS ABIERTAS

Liliana Carolina Pinzón G.[1], Esp., MihdíBadí Talero M.[2], Esp., John A. Bohada[3], Ph.D.

Grupo de investigación MUISCA, Facultad de Ingeniería, Especialización en Seguridad de la Información, Fundación Universitaria Juan de Castellanos, Tunja, Colombia.

[1]lcarolinapinzon@gmail.com, [2]mihdibadi@gmail.com, [3]jbohada@jdc.edu.co

Información del artículo:

Recibido: 16 de octubre de 2013
Aceptado: 9 de diciembre de 2013

Palabras Claves: Metodología abierta, Prueba de intrusión, Seguridad, Análisis de vulnerabilidades.

Resumen: Debido al crecimiento de los ataques a las infraestructuras de las tecnologías de la información y comunicaciones (TIC), el cual para el año 2012 se incrementó en un 42% llegando, por ejemplo, en el caso de los ataques a sitios web, a 190.370 ataques diarios, según información de Symantec Corporation (2013). Los administradores de tecnología se han visto en la necesidad de realizar periódicamente pruebas de intrusión en cada uno de los elementos importantes que componen su infraestructura; este tipo de prácticas tienen como objetivo actuar proactivamente para blindar la información interna y de clientes, y también para evitar que personal malintencionado se apropie de ella sacando provecho económico o generando daño en la misma.

Por lo anterior, este artículo presenta la revisión y análisis de algunas fuentes de información acerca de las pruebas de intrusión y las principales metodologías abiertas que existen actualmente; con el fin de dar a conocer la importancia de ejecutar esta clase de evaluaciones de seguridad enmarcadas en una metodología que se acople a las necesidades de la empresa y que se convierta en un apoyo para lograr sus objetivos de negocio.

1. INTRODUCCIÓN

A pesar de que la mayoría de las empresas ha invertido considerablemente en productos y servicios para salvaguardar sus datos de la pérdida o destrucción intencionada o accidental, muchas de ellas no se dan a la tarea de comprobar el impacto real de un ataque en sus sistemas de información; razón por la cual, se hace necesario, efectuar periódicamente pruebas de intrusión, puesto que consisten en un modelo que reproduce intentos de acceso, a cualquier entorno informático desde diferentes puntos de entrada, tanto internos como externos [1] [2], lo que permite evaluar las repercusiones reales de cada una de las vulnerabilidades que existen en los sistemas y su impacto específico en la organización.

Si se quiere ser más efectivo en la seguridad, se deben conocer metodologías que permitan preparar escenarios donde se puedan poner a prueba todas las técnicas y habilidades de ataque [3]; es por esta razón, que el conocimiento de las metodologías abiertas es de gran utilidad, debido a que estas garantizan el libre derecho a ser usadas, modificadas y redistribuidas. Por lo anterior, esta investigación se basa en la recopilación y análisis de información referente a pruebas de intrusión y las principales metodologías abiertas que son utilizadas actualmente para este tipo de análisis de seguridad, con el fin de generar conocimiento acerca de la manera como se debe poner a prueba un sistema o red para determinar el grado de acceso que tendría un atacante con intenciones maliciosas a nuestros recursos [4].

2. PRUEBAS DE INTRUSIÓN

En primer lugar, es indispensable definir el término vulnerabilidad como cualquier situación que pueda desembocar en un problema de seguridad [5] o toda diferencia entre los parámetros recomendados por los estándares y las mejores prácticas profesionales en cuanto a seguridad informática [6]. Existen vulnerabilidades de diferentes tipos: físicas, naturales, de hardware, software, medios de almacenamiento, comunicación y humanas [7], que se pueden presentar por intrusión, por configuración o pueden ser propias del sistema [8].

Una prueba de intrusión es aquella en la que se simulan ataques reales para identificar los métodos a través de los cuales es posible eludir las medidas de seguridad [9]. Este tipo de pruebas permiten realizar un buen diseño de estrategias que aseguren la continuidad operativa [10] y son útiles para determinar aspectos como la capacidad de detectar y responder adecuadamente a los ataques, que pueden ser de tipo: modificación (compromete la confidencialidad y la integridad), fabricación (compromete la integridad), interceptación (compromete la confidencialidad), interrupción (compromete la disponibilidad) [11]. Así mismo, esta clase de pruebas son un complemento fundamental para la auditoría perimetral, en la cual se analiza el grado de seguridad de las entradas exteriores a la red de la empresa [12].

La evaluación de vulnerabilidades constituye la primera parte de una prueba de intrusión, en la cual se realiza, además, ataques de pruebas de concepto (POC) [13], por medio de la explotación de dichas vulnerabilidades, para confirmar su existencia y determinar los daños que puedan causar [14]. El objetivo fundamental de este tipo de pruebas es tratar de poner en peligro la seguridad del sistema “emulando un hacker” [15], con el fin de presenciar el potencial de un atacante malintencionado; bajo el concepto de que la mejor forma de detener a un criminal informático es pensar en la forma en que él piensa [16]; es decir, utilizar las herramientas y técnicas comúnmente empleadas por los piratas informáticos [17]; quienes además de estos conocimientos encuentran oportunidades (fallos en la seguridad) y motivos (diversión, lucro personal, entre otros), que los llevan a ejecutar los ataques [18].

Una vez son explotadas las vulnerabilidades evidenciadas, es preciso realizar una clasificación y cualificación de cada una de ellas, para llevar a

cabo este proceso, el Forum of Incident Response and Security Teams (FIRST), plantea un modelo tipológico basado en métricas cualitativas, temporales y del entorno, como se muestra en la siguiente tabla [19]:

Tabla 1. Tipología 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 [20]. El daño potencial causado por la acción directa de una amenaza debe ser estimado de manera objetiva con la participación del responsable de cada activo [21], debido a que hay que asociar de la manera más explícita posible las vulnerabilidades con las amenazas a los activos, para entender su interrelación y llevar a cabo un análisis de costo/beneficio [22].

Las pruebas de intrusión se enfocan principalmente en las siguientes perspectivas: externas, internas, con objetivo (buscan vulnerabilidades en partes específicas), sin objetivo (examinan la totalidad de los componentes informáticos), pruebas a ciegas (solo se emplea la información pública disponible sobre la organización) y pruebas informadas (utilizan la información privada, otorgada por la organización acerca de sus sistemas informáticos) [23].

Según las buenas prácticas de seguridad, las pruebas de intrusión deben ser ejecutadas al menos una vez al año y cada vez que se realiza una actualización o modificación importante en la infraestructura de TI, para asegurar que los controles establecidos continúan siendo eficaces [24] y dar a la empresa la oportunidad de cerciorarse de que sus sistemas sean seguros y sus políticas de respuesta a incidentes sean las adecuadas [25].

El nivel de criticidad y confidencialidad de los datos administrados por los sistemas de información de una empresa [26], hace evidente la necesidad de realizar pruebas de intrusión debido a la preocupación de que ésta no esté protegida adecuadamente de un número exponencial de amenazas [27] que pueden generar daño en la reputación, pérdida financiera, perjuicio a las personas por la divulgación de sus datos personales, entre otros [28]. De igual forma, la ejecución de estas pruebas no supone el cumplimiento de las legislaciones existentes en cada país, pero puede aportar información sobre aspectos de incumplimiento de las mismas [29].

Los componentes de la infraestructura tecnológica han ofrecido un sinnúmero de oportunidades para las pruebas de intrusión a través de los años [30], puesto que contienen información estratégica de la compañía entre la que se puede encontrar: información acerca de los mercados sensitivos, información financiera, secretos industriales, procesos de aprovechamiento tecnológico, información del personal, de clientes, de productos, información interna y de seguridad [31].

Vale la pena destacar que las incidencias y ataques pueden convertirse en oportunidades para el negocio, si desde la dirección de la empresa se plantean como un reto a la política de seguridad corporativa y se utilizan para mejorar los aspectos deficientes [32]; por lo anterior, un proceso de gestión de incidentes es un instructivo fundamen-

tal en este tipo de análisis de seguridad; puesto que no solo revela vulnerabilidades sino también consecuencias reales fruto de las mismas [33]. De la misma manera, algunos aspectos como los acontecimientos históricos y los informes de auditoría pueden proporcionar información adicional que debe tenerse en cuenta [34].

Los hackers éticos que realizan pruebas de intrusión utilizan los siguientes modelos:

- Modelo de caja blanca: cuando la organización facilita información detallada acerca de los sistemas de información que utiliza [35]. El propósito de este modelo es simular un ataque perpetrado por un usuario interno autorizado [36].
- Modelo de caja negra: en caso de que la administración no divulgue al personal que se están llevando a cabo pruebas de penetración, ni suministre información concerniente a la tecnología utilizada [35]. El objetivo es emular un ataque externo, realizado por un pirata informático que no tiene relación con la empresa [36].
- Modelo de caja gris: en este modelo, la compañía brinda sólo información parcial [35]. La intención es fingir un ataque perpetrado por un usuario interno no-autorizado, ya sea un empleado de la empresa o un asesor externo que tiene acceso físico a la red de la organización [36].

3. METODOLOGÍAS ABIERTAS

Es importante mencionar que cada día se generan nuevos riesgos en los sistemas de información de una organización [37]; razón por la cual, la adopción de cualquier metodología debe ser un proceso aplicado de manera iterativa y reiterada en el tiempo[38], con el fin de descubrir los puntos débiles de la seguridad que pueden provocar que los datos y/o los equipos se vean afectados en mayor o menor medida por ataques [39] pasivos (escuchar los datos transmitidos sin modificarlos) y/o activos (modificación o alteración de la información que ha sido interceptada, con el fin de hacer daño) [40]. Para comprometer la seguridad de cualquier sistema de información, el atacante debe tener conocimiento de las cuatro etapas que se detallan en la figura 1 para realizar un test de penetración [41]:

Figura 1. Etapas de un test de Penetración.

Fuente: D. Monrroy, Análisis inicial de la anatomía de un ataque a un sistema informático, disponible en http://www.segu-info.com.ar/tesis/, 2009

Una metodología define un conjunto de reglas prácticas y procedimientos que son ejecutados durante el curso de evaluación de cualquier programa de seguridad de la información [42] y permite ordenar y estandarizar este proceso [43]. Para el caso específico de las pruebas de intrusión, existen múltiples metodologías que pueden ser propietarias o abiertas. Las metodologías abiertas (Open Source), serán el objeto de estudio de este artículo, debido a su naturaleza, ya que son creadas sin ánimo de lucro y se encuentran disponibles al público para ser descargadas, leídas y mejoradas [44].

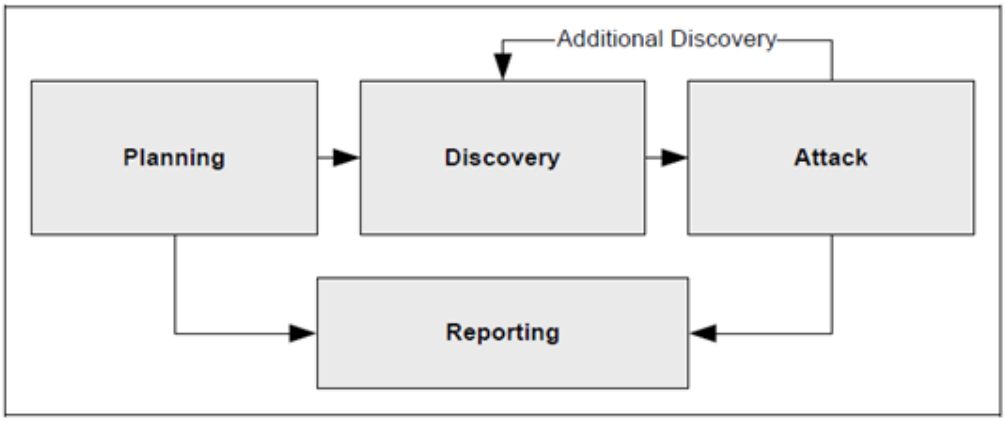
3.1 Publicación NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)

Como se muestra en la figura 2, este estándar plantea cuatro fases: planificación (aprobación de la Gerencia, identificación del alcance y los objetivos de la prueba), descubrimiento (recopilación de información y análisis de vulnerabilidades), ejecución del ataque (explotación de vulnerabilidades) y presentación de informes (informe final

que describe las vulnerabilidades identificadas y las recomendaciones pertinentes para mitigarlas, así como la valoración del grado de riesgo que representa cada una de ellas) [45].

Entre la fase de ataque y el descubrimiento se representa un bucle de retroalimentación, lo que significa que deben llevarse a cabo las pruebas y análisis sobre múltiples sistemas para determinar el nivel de acceso que puede tener un atacante [46].

Figura 2. Metodología NIST SP 800-115



Fuente: National Institute of Standards and Technology (NIST), Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, 2008.

3.2 Guía de pruebas OWASP (Open Web Application Security Project)

La guía de pruebas para OWASP se divide en 2 modos: modo pasivo y modo activo. En el modo pasivo, el evaluador recopila información a través de diferentes herramientas, intentando comprender la lógica de la aplicación, previo a la segunda fase. Por otro lado, en el modo activo el evaluador empieza a realizar las pruebas usando la siguiente metodología que se compone de las subcategorías que se muestran en la tabla 2:

Tabla 2. Subcategorías y actividades de ejecución de la Guía de pruebas OWASP

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

Categoría	Actividades
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	Pruebas de gestión del Caché de Navegación y de salida de sesión
	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
	Bloqueo de cuentas de usuario
Pruebas de denegación de servicio	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

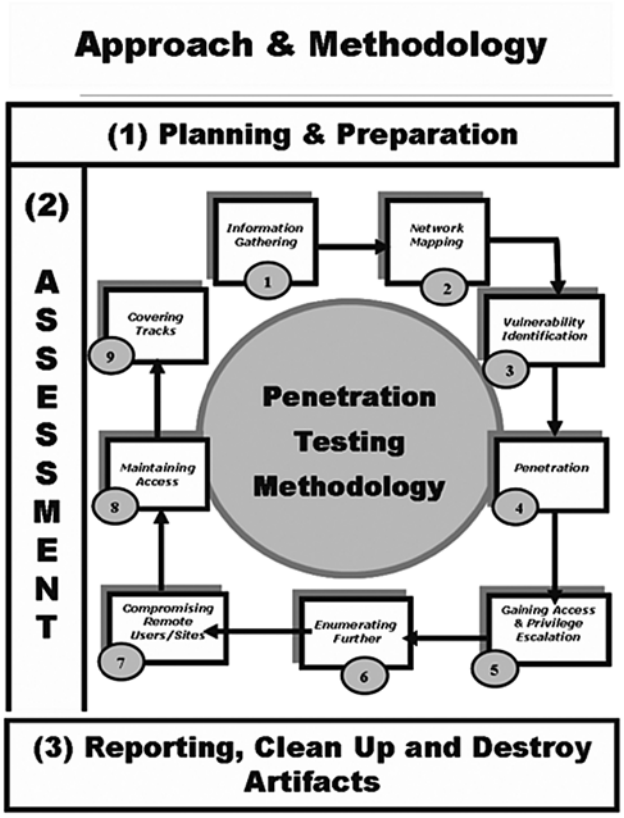
Finalmente, se debe emitir un informe que describa detalladamente la valoración de los riesgos reales como resultado de la evaluación de seguridad [47].

3.3 Penetration Testing Framework (PTF) - ISSAF (Information Systems Security Assessment Framework)

Como se muestra en la figura 3, esta metodología incluye tres fases en las cuales, los pasos de ejecución son cíclicos e iterativos [48]:

- Fase I: Planificación y preparación. Previo a la ejecución de las pruebas, se debe planear los aspectos relevantes de las pruebas que se van a realizar y se debe firmar un acuerdo formal donde se detallen los mismos.
- Fase II: Evaluación. Esta fase presenta un enfoque por capas, como se muestra en la figura 3, en el que cada una de ellas representa un mayor nivel de acceso a los activos de información.
- Fase III: Informes, limpieza y destrucción de información. Una vez se han culminado todos los casos de prueba definidos en el alcance del trabajo, se debe generar un informe escrito que describe los resultados detallados y las recomendaciones pertinentes para mejorar la seguridad; no obstante, en caso de identificar un punto crítico durante la ejecución de las pruebas, se debe informar de inmediato. Adicionalmente, toda la información que se crea y/o almacena en los sistemas de prueba debe ser eliminada; si por alguna razón esto no es posible, todos los archivos (con su localización) deben ser mencionados en el informe técnico para que sean eliminados posteriormente [49].

Figura 3. Metodología para pruebas de intrusión - ISSAF.



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

3.4 OSSTMM 3 – Manual de metodología abierta para pruebas de seguridad (ISECOM)

Esta metodología divide la totalidad de una infraestructura en cinco canales: humano, físico, redes inalámbricas, telecomunicaciones y redes de datos para su estudio [50]. Como se observa en la tabla 3, está constituida por cuatro fases y éstas a su vez por diecisiete módulos, que tienen sus correspondientes tareas y procedimientos, los cuales varían dependiendo del canal que se está evaluando [51].

Tabla 3. Fases y Módulos de la Metodología OSSTMM

Fases	Módulos	Descripción
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.
	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.
Fase de Interacción	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.

Fases	Módulos	Descripción
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.

Fases	Módulos	Descripción
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.

Finalmente, es imprescindible destacar, que todas las metodologías tienen sus debilidades y fortalezas, su elección se debe hacer dependiendo del alcance del proyecto, los conocimientos de los miembros del equipo y la complejidad de la red o el sistema que se va a evaluar [52].

4. CONCLUSIONES

- Una prueba de intrusión es una evaluación de las medidas de protección de una organización que debe realizarse periódicamente como parte de las tareas de seguridad de la información, estableciendo métricas que permitan evaluar el nivel de criticidad e impacto de las vulnerabilidades detectadas y llevar a cabo un análisis de costo/beneficio que permita concientizar a las organizaciones de su importancia como apoyo para la toma de decisiones y el cumplimiento de sus objetivos de negocio.
- Las metodologías estudiadas se complementan entre sí y aportan a la verificación del nivel de resistencia a ataques informáticos en una empresa desde sus diferentes enfoques; haciendo que el proceso de evaluación sea organizado y estandarizado de manera que puedan realizarse comparaciones del grado de continuo mejoramiento de la seguridad de una empresa a través del tiempo.
- La metodología del NIST indica el proceso general de cómo llevar a cabo una prueba de intrusión y trata de cubrir todos los aspectos informáticos y humanos que tienen contacto con la información de las organizaciones.
- La metodología OWASP tiene como objetivo crear un marco de trabajo para el desarrollo

de pruebas de seguridad en aplicaciones web, mostrando una colección de diferentes tipos de vulnerabilidades a las cuales están expuestas este tipo de aplicaciones.

- La metodología OSSTMM tiene un enfoque en el cual se toma como base las políticas de seguridad y se contemplan algunas características que no cubren otras metodologías como la existencia de los controles de seguridad y la indemnización de los activos de información.
- La metodología ISSAF está orientada principalmente en cubrir los procesos de seguridad y la evaluación de los mismos para así obtener un panorama completo de las vulnerabilidades existentes.

REFERENCIAS

[1] Symantec Corporation, Internet Security Threat Report, 2013, pp. 10.

[2] E. Cruz, D. Rodríguez, Modelo de seguridad para la medición de vulnerabilidades y reducción de riesgos de datos, Instituto Politécnico Nacional, México, 2010.

[3] J. Rivera, Ciclo de vida de una prueba de intrusión física, Universidad San Carlos de Guatemala, Guatemala, 2011.

[4] Sec Track, Test de Intrusión, (2013, noviembre). [On line]. Disponible en http://www.sec-track.com/test-de-penetracion.

[5] A. Villalon, Seguridad en Linux y redes, GNU, Free Documentation License. [On line]. Disponible en http://www.rediris.es / cert/doc/ unixsec/unixsec.pdf.

[6] M. Bisogno, Metodología para el Aseguramiento de Entornos Informatizados – MAEI, Universidad de Buenos Aires, Buenos Aires, 2004.

[7] C. Barón, Metodología de análisis de vulnerabilidades para la red de datos en la dirección de telemática de la Policía Nacional, Universidad Militar Nueva Granada, Bogotá, 2010.

[8] M. Coello, Procedimiento Formal de Ethical Hacking para la Infraestructura tecnológica de los servidores por internet de la banca Ecuatoriana, Escuela Politécnica Nacional, Quito, 2012.

[9] M. Bishop, About Penetration Testing, Security & Privacy, IEEE, California Vol. 5, 2007.

[10] MJ. Ochoa, Seguridad física, prevención y detección, Universidad Autónoma de Nuevo León, México, 2013.

[11] A. Carvajal, Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático, Global Tek Security: tecnologías globales para la seguridad de la información, Colombia, 2007.

[12] W. Mejía, Auditoría Forense, Revista de Información, Tecnología y Sociedad, Universidad Mayor de San Andrés, 2009.

[13] P. Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Elsevier Inc., USA, 2011.

[14] J. Bertolín, A. Bertolín, Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red, España, 2009.

[15] F. Pacheco, H. Jara, Hackers al descubierto, Fox Andina, Buenos Aires, 2010.

[16] K. Wyk, (2013, mayo), Adapting Penetration Testing for Software Development Purposes, Build Security In, [On line]. Available: https://build securityin.uscert.gov/articles/best-practices/security-testing/adapting-penetration-testing-software-development-purposes.

[17] S. Umrao, M. Kaur, G. Gupta, Vulnerability assessment and penetration testing, International Journal of Computer & Communication Technology, 2012.

[18] A. Vieites, Enciclopedia de la Seguridad Informática, México, Alfaomega, 2007.

[19] P. Mell, K. Scarfone, S. Romanosky, A Complete Guide to the Common Vulnerability Scoring System, 2007.

[20] H. Jara, F. Pacheco, Ethical hacking 2.0, Fox Andina, Buenos Aires.

[21] L. Flores, G. Hernández, Pruebas de Hacking ético en un laboratorio de la Facultad de Ingeniería de la UNAM, 2012.

[22] V. Baena, La seguridad de Tecnología de la Información (TI) como una variable de la cultura organizacional, Universidad EAFIT, Medellín, 2009.

[23] L. Sandoval, A. Vaca, Implantación de técnicas y administración de laboratorio para investigación de ethical hacking, Escuela Politécnica del ejercito, Sangolquí, 2013.

[24] A. Basta, W. Halton, computer security and penetration testing, Cengage Learning, Estados Unidos, 2007.

[25] T. J. Klevinsky, S. Laliberte, A. Gupta, Hack I.T.: Security Through Penetration Testing, Pearson Education Inc., Indianapolis, 2004.

[26] J. Ramírez, Desarrollo de un esquema de análisis de vulnerabilidades y pruebas de penetración en sistemas operativos para una organización de la administración pública federal, Escuela Superior de Ingeniería Mecánica y Eléctrica, México, 2009.

[27] A. Whitaker, D. Newman, Penetration Testing and Network Defense, Cisco Press, Indianapolis, 2006.

[28] E. Nabbus, Penetration Testing A Vital System Security Assessment Method, Electrosoft, 2007.

[29] A. Verdesoto, Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular, comunicaciones y representaciones, Escuela Politécnica Nacional, Quito, 2007.

[30] K. Xynos, SUTHERLAND Iain & READ Huw, Penetration testing and vulnerability assessments: A professional approach, University of Glamorgan, United Kingdom, 2010.

[31] D. Parker, The Strategic Values of Information Security in Business. Computers & Security, Vol. 16, 1997.

[32] E. Quispe, Asegurándose contra delitos informáticos, Universidad Mayor de San Andrés, Bolivia, 1997.

[33] G. Baker, A. Vulnerability Assessment Methodology for Critical Infrastructure Facilities, James Madison University, Estados Unidos, 2005.

[34] Risk Assessment Special Interest Group (SIG), PCI Security Standards Council, PCI Data Security Standard *(PCI DSS)*, versión 2.0, 2012.

[35] M. Simpson, K. Backman, J. Corley, Hands-on ethical hacking and network defense, 2nd Edition, Cengage Learning, 2010.

[36] G. Chicaiza, Hacking ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos, Universidad Técnica de Ambato, Ambato, 2012.

[37] J. Triviño, Detección de intrusos en redes de telecomunicaciones IP usando modelos ocultos de Markov, Universidad Nacional de Colombia, Bogotá, 2009.

[38] D. Garzón, J. Gómez, A. Vergara, Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala, Pontificia Universidad Javeriana, Bogotá, 2013.

[39] VeriSing, Libro Blanco, Introducción a las pruebas de vulnerabilidad de red. [On line]. Disponible en www.verisign.es.

[40] A. Espinosa, Análisis de Vulnerabilidades de la Red LAN de la UTPL, Universidad Técnica Particular de Loja, Loja, 2010.

[41] D. Monrroy, Análisis inicial de la anatomía de un ataque a un sistema informático. [On line]. Disponible en http://www.segu-info.com.ar/tesis/.

[42] 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.

[43] K. Byeong-Ho, About Effective Penetration Testing Methodology, Instituto de Investigación en Ingeniería de Seguridad, Journal of Security Engineering. Vol. 5, 2008.

[44] L. Navas Leydy, Análisis, diseño e implementación de la metodología OSSTMM para aplicar penetration test y ethical hacking en la unidad administrativa de sistemas de información de la Universidad Técnica de Machala, Universidad Técnica de Machala, Ecuador, 2010.

[45] M. Prandini, M. Ramilli, Towards a practical and effective security testing methodology, IEEE Simposio sobre Computadores y Comunicaciones (ISCC), Italia, junio 22-25, 2010.

[46] National Institute of Standards and Technology (NIST), Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, 2008.

[47] OWASP Fundation, OWASP TESTING GUIDE V3.0, 2008.

[48] OISSG, Information System Security Assessment Framework (ISSAF), Penetration Testing Framework (PTF), 2006.

[49] O. Acosta, Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaría nacional de gestión de riesgos utilizando metodologías de ethical hacking, Escuela Politécnica Nacional, Quito, 2013.

[50] ISECOM, OSSTMM 3 – The Open Source Security Testing Methodology Manual, 2009.

[51] A. López, Estudio de metodologías para pruebas de intrusión a sistemas informáticos, Instituto Politécnico Nacional, México, 2011.

[52] T. Wilhelm Thomas, Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Elsevier Inc., USA, 2010.