Pruebas de Penetración e Intrusión

Castro, Carlos.
Arturocv_497@hotmail.com
Universidad Piloto de Colombia

***Resumen*— Este artículo pretende exponer algunas metodologías existentes para llevar a cabo pruebas de penetración e intrusión a través de la descripción de sus características, etapas y actividades que se llevan a cabo en cada una de ellas. Esto con el propósito de aproximar al lector al valor que, en la actualidad, la industria ha otorgado a esta actividad en aras de aportar al campo de la seguridad y la transformación digital, siendo desarrolladas y respaldadas por prestigiosas entidades y/o comunidades al punto de ser consideradas como un marco de referencia para llevar a cabo las pruebas de penetración y facilitar la adopción e implementación de su práctica en las organizaciones.**

***Palabras Claves*— Acceso, amenaza, confianza, contramedidas, explotación, pentester, pruebas de intrusión, seguridad, superficie de ataque, riesgo, visibilidad y vulnerabilidad.**

***Abstract* — This article pretends to expose some existing methodologies to develop penetration and intrusion tests through the description of their characteristics, stages and activities that are carried out in each one of them. The purpose is to the reader gets closer to the value that, currently, the industry has been granted to this activity in the field of security and digital publishing, being developed and supported by prestigious entities and/or communities to the point of being considered as a frame of reference to carry out a penetration tests and facilitate the adoption and implementation of their practice at the organizations.**

***Key words* — Access, threat, confidence, countermeasures, exploitation, pentester, intrusion tests, security, attack surface, risk, visibility and vulnerability.**

I. Introducción

Con el pasar de los años la información ha adquirido un valor relevante en las dinámicas sociales, posicionando el término “conectividad” como una de las necesidades más recurrentes entre las comunidades contemporáneas, más cuando esto se hace presente en la mayoría de contextos sociales a nivel mundial. Por esta razón, la seguridad informática ha adquirido un mayor reconocimiento, principalmente, para las empresas que tienen en la información uno de sus mayores activos. Este motivo impulsa a destinar un porcentaje significativo de su presupuesto en seguridad ya sea física, ambiental o lógica; sin embargo, como lo indican los expertos es imposible asegurar el 100% de la información del sistema, pues siempre habrá riesgos residuales que se deben asumir consecuencia de diversos factores externos. Para validar esto se pueden listar varios ataques que comprometieron los datos de importantes compañías en el último año:

Facebook (septiembre de 2018): Más de 50 millones de usuarios se vieron afectados por una filtración de datos detectada la última semana de ese mes. Los ciber delincuentes supieron explotar una vulnerabilidad en la función <<Ver como>> de la red social para robar tokens de acceso, que son unas claves que permiten iniciar la sesión de Facebook de manera automática y no tener que volver a escribir una contraseña cada vez que se quiere acceder; en la intrusión se comprometieron más de cincuenta millones de cuentas.

British Airway: Alrededor de 380.000 tarjetas de crédito de los clientes de la aerolínea quedaron expuestas ante un ciber ataque que sustrajo información personal de los viajeros. Según confirmó la propia compañía los datos fueron robados de la página web y de la aplicación móvil.

Ticketmaster (junio de 2018): Un software malicioso atacó un producto para soporte de clientes alojado por Inbenta Technologies, proveedor externo de la compañía y quedaron expuestos los datos de por lo menos 40.000 usuarios.

T-Mobile (agosto de 2018): Sufrió una filtración de datos que afectó a más de 2’000.000 de sus clientes; los datos potencialmente comprometidos, incluían los nombres de los usuarios, los códigos postales de facturación, los números de teléfono y las direcciones de correo electrónico, así como los números de cuenta y su tipo.

De acuerdo con estas cifras y a los avances tecnológicos que se registran día tras día, las empresas se están volcando a una transformación digital para mantener su posición en el mercado y/o seguir vigentes, máxime cuando el ecosistema digital cada vez es mayor, lo que representa un riesgo sobre los datos que se pretenden salvaguardar. Los ciberdelincuentes pueden explotar cualquier vulnerabilidad que surja, por tanto, es imprescindible que las organizaciones sigan esforzándose en establecer políticas de seguridad con el fin de mitigar el impacto que puede tener un ataque; además de concientizar a sus usuarios sobre el uso de sus plataformas.

En este marco, las pruebas de penetración o Penetration Testing (Pentest) en inglés constituyen una herramienta válida para evaluar o auditar sistemas; consisten en la realización de prácticas que ponen a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un posible atacante podría explotar.

Una definición más completa es la que sugiere Guillen (2017) donde menciona que un Pentest es "un ataque simulado y autorizado contra un sistema informático con el objetivo de evaluar la seguridad del sistema. Durante la prueba, se identifican las vulnerabilidades presentes en el sistema y se explotan tal como haría un atacante con fines maliciosos. Esto permite al pentester realizar una evaluación de riesgos en la actividad comercial del cliente basándose en los resultados de la prueba y sugerir un plan de medidas correctivas" [3].

II. Contextualización

Open Web Application Security Project (OWASP) y la fundación de Penetration Testing Execution Standard (PTES) surgieron como respuesta a la evolución de los sistemas de información y a la necesidad de establecer lineamientos específicos para llevar a cabo auditorías a los sistemas de información. Estos se enfocaron en estructurar y guiar de forma detallada el proceso de prueba de penetración desde el levantamiento de información hasta la presentación de los hallazgos encontrados en un reporte final. OWASP también enfatiza y orienta la seguridad a las aplicaciones web, dando una relevancia mayor al apartado técnico que conlleva cada proceso de prueba.

Ahora bien, cuando se hacen pruebas de penetración se pueden generar diversos escenarios, los cuales dependen de la información que se tenga acerca del objetivo que va a ser auditado; en el libro Kali Linux – Assuring Security by Penetration Testing, los autores definen dos de ellos, que denominan Black box testing y White box testing [1, 2].

Black box testing o pruebas de Caja negra: El auditor de seguridad evaluará la infraestructura de la red y no estará al tanto de ninguna tecnología interna implementada por la organización objetivo. Al emplear una serie de técnicas de hackers del mundo real y atravesar fases de pruebas organizadas, las vulnerabilidades pueden revelarse y potencialmente explotarse. Es importante que un pentester entienda, clasifique y priorice estas vulnerabilidades de acuerdo con su nivel de riesgo (bajo, medio o alto), el cual puede medirse según la amenaza impuesta por la vulnerabilidad en general.

Una prueba de intrusión ideal determinaría todos los vectores de ataque que podrían hacer que el objetivo se vea comprometido. Una vez que se ha completado el proceso de prueba, se genera un informe que contiene toda la información necesaria con respecto a la seguridad de los objetivos evaluados, además de la clasificación y su significado en un contexto de negocio.

White box testing o pruebas de caja blanca: El auditor involucrado debe conocer todas las tecnologías internas y subyacentes utilizadas por el entorno objetivo cuando realiza este tipo de prueba de penetración. Por lo tanto, abre una puerta para que un pentester vea y evalúe críticamente las vulnerabilidades de seguridad con el mínimo esfuerzo posible y la máxima precisión. Este proceso aporta más valor a la organización, en comparación con el enfoque de caja negra debido a que eliminará cualquier problema de seguridad interna que se encuentre en el entorno de la infraestructura de destino, lo que hace más difícil que un adversario malintencionado se infiltre desde el exterior.

El número de pasos involucrados en las pruebas de caja blanca es similar al de las pruebas de caja negra. Además, el enfoque de la caja blanca se puede integrar fácilmente en un ciclo de vida de desarrollo regular para erradicar cualquier posible problema de seguridad en una etapa temprana antes de que sean revelados y explotados por intrusos. El tiempo, costo y nivel de conocimiento requerido para encontrar y resolver las vulnerabilidades de seguridad es comparativamente menor que con el enfoque de caja negra.

En este mismo sentido OSSTMM define más matices dentro de las pruebas dando cabida a seis escenarios [5] como se muestra en la Fig. 1:

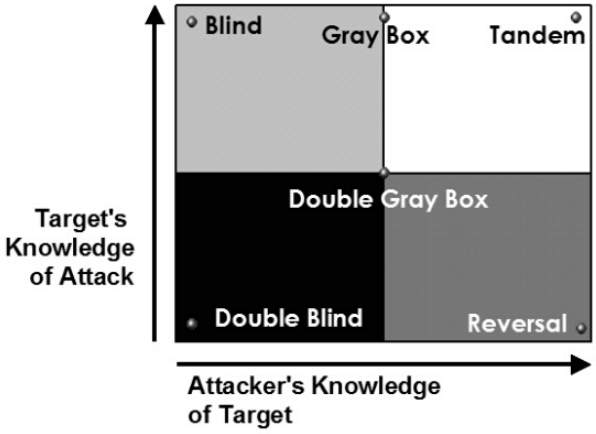

Fig. 1. Escenarios para pruebas de penetración e intrusión según la información que se tenga del objetivo. [5]

Blind: El analista se compromete con el objetivo sin conocimiento previo de sus defensas, activos o canales. El objetivo está preparado para la auditoría, sabiendo todos los detalles de la auditoría con antelación. Una auditoría ciega principalmente prueba las habilidades del analista. La amplitud y profundidad de una auditoría ciega solo puede ser tan amplia como lo permita el conocimiento y la eficiencia aplicables del analista.

Double Blind: El analista se compromete con el objetivo sin conocimiento previo de sus defensas, activos o canales. El objetivo no recibe una notificación con anticipación sobre el alcance de la auditoría, los canales probados o los vectores de prueba. Una auditoría a doble ciego pone a prueba las habilidades del analista y la preparación del objetivo ante variables desconocidas de agitación. La amplitud y profundidad de cualquier auditoría ciega solo puede ser tan amplia como lo permita el conocimiento y la eficiencia aplicables del Analista.

Gray Box: El analista se compromete con el objetivo teniendo un saber limitado de sus defensas y activos, pero si un conocimiento completo de los canales. El objetivo está preparado para la auditoría, sabiendo de antemano todos los detalles de esta. Una auditoría de caja gris pone a prueba las habilidades del analista. La naturaleza de la prueba es la eficiencia; la amplitud y profundidad dependen de la calidad de la información proporcionada al Analista antes de la prueba, así como de su conocimiento aplicable. Este tipo de prueba a menudo se denomina prueba de vulnerabilidad y la mayoría de las veces es iniciada por el objetivo como una autoevaluación.

Double Gray Box: El analista se compromete con el objetivo con un conocimiento limitado de sus defensas y activos y un conocimiento completo de los canales. El objetivo se notifica por adelantado del alcance y el marco de tiempo de la auditoría, pero no los canales probados o los vectores de prueba. Una auditoría de doble caja gris pone a prueba las habilidades del analista y la preparación del objetivo para variables desconocidas de agitación. La amplitud y profundidad dependen de la calidad de la información proporcionada al Analista y del objetivo antes de la prueba, así como del conocimiento aplicable del Analista.

Tandem: El analista y el objetivo están preparados para la auditoría, razón por la cual ambos conocen de antemano todos los detalles de esta. Una auditoría en tandem prueba la protección y los controles del objetivo. Sin embargo, no puede probar la preparación del objetivo ante variables desconocidas de agitación. La verdadera naturaleza de la prueba es la minuciosidad, ya que el analista tiene una visión completa de todas las pruebas y sus respuestas. La amplitud y profundidad dependen de la calidad de la información proporcionada al Analista antes de la prueba (transparencia), así como de su conocimiento aplicable. Esto a menudo se conoce como una auditoría interna o una prueba de Crystal Box, donde el analista con frecuencia forma parte del proceso de seguridad.

Reversal: El analista se compromete con el objetivo a partir del un amplio y basto conocimiento de sus procesos y seguridad operacional, aunque el objetivo no sabe qué, cómo o cuándo el analista realizará la prueba. La verdadera naturaleza de esta prueba es auditar la preparación del objetivo a variables desconocidas y vectores de agitación. La amplitud y profundidad dependen tanto de la calidad de la información proporcionada al analista como a su conocimiento y creatividad aplicables. Con frecuencia, este es un llamado a realizar un ejercicio del equipo rojo.

III. The Open Source Security Testing Methodology Manual 3 (OSSTMM 3)

Después de ver los escenarios en los que se pueden realizar diversas pruebas de penetración, se presentará la estructura que proponen algunas de las metodologías y/o framework disponibles en la actualidad como apoyo a la hora de realizar este tipo de pruebas. Se iniciará con el Open Source Security Testing Methodology Manual (OSSTMM 3) que es un marco de referencia flexible y ajustable a una variedad de auditorías que incluye pruebas de penetración, evaluaciones de seguridad, evaluaciones de vulnerabilidad, entre otras.

Esta metodología propone una mirada holística de la seguridad; sin embargo, al tener un alcance tan amplio utiliza como fundamento en su estructura una división de clases y canales, que representan las interacciones que puede tener un activo dentro de la organización; la metodología sugiere que se debe realizar pruebas de seguridad sobre cada canal.

Las clases presentadas para entender la seguridad de la organización son la seguridad física (PHYSSEC), seguridad de espectro inalámbrico (SPECSEC) y seguridad de comunicaciones (COMSEC); cada una de ellas se asocia a unos canales específicos dependiendo de su naturaleza.

Hay dos (2) canales asociados a la seguridad física. El canal humano donde la interacción es de tipo presencial o psicológica, mientras que en el físico se requiere una transmisión de energía que no sea del tipo electrónico para manipular un elemento; de otro lado, el canal inalámbrico corresponde a la seguridad de espectro y comprende todas las emisiones de señal, frecuencias y comunicaciones electrónicas que están sobre el espectro. Por último, la clase de seguridad de comunicaciones tiene el canal de telecomunicaciones y el canal datos de red, el primero agrupa todas las telecomunicaciones análogas y digitales, mientras que el segundo representa todos los sistemas electrónicos y las redes de datos.

El flujo de trabajo para realizar una auditoría se plantea a través de un ciclo completo que inicia conociendo los requisitos de la operación y termina con la revisión de los resultados de la auditoría; para ayudar al auditor a realizar correctamente este ciclo se maneja una jerarquía:

1. Canal
2. Modulo
3. Tarea

El canal, como ya se mencionó previamente, es el medio de interacción; los módulos son las propiedades que aplican al canal y que son comunes para todos ellos, aunque cada uno puede tener un enfoque diferente; mientras que las tareas son las acciones que se realizan para cada módulo.

Antes de continuar es importante tener claro los siguientes conceptos:

Visibilidad: Hace referencia a los activos que se pueden identificar dentro de un ámbito; esta característica permite calcular el riesgo de oportunidad. Si un objetivo no es visible no tiene posibilidad de ser atacado.

Acceso: Se refiere a los puntos de interacción que tiene un objetivo; se debe distinguir entre seguridad física y seguridad

de comunicaciones. En el primer caso, la interacción se refiere a entradas a una oficina o centro de cómputo mientras que, para la seguridad de comunicaciones, la interacciones se realizan a través de los puertos, en particular, a los servicios que estén activos en esos puertos.

Confianza: Es la relación que existe entre dos objetivos donde se admite la interacción libre entre ellos.

Con estos conceptos claros, continuamos con el flujo de trabajo definido en la metodología, la cual establece cuatro (4) fases a través de las cuales se evalúan los diecisiete (17) módulos, como se observa en la Fig. 2.

Fase de inducción: En esta etapa el analista establece un marco de la situación que se va a desarrollar durante la auditoría, comprendiendo los requisitos, el alcance y las restricciones que tiene. Para llevar a cabo la auditoría se debe tener en cuenta la cultura, normas, reglamentos, legislación y políticas que son aplicables al objetivo; además, se debe determinar la forma de medición y la fiabilidad con el fin de establecer la precisión que tendrán los resultados. Los módulos evaluados en esta etapa son:

- A.1 Revisión de la postura
- A.2 Logística
- A.3 Verificación de detección activa

Fase de interacción: Esta etapa busca entender el sistema donde se va a realizar la auditoría; se definen los objetivos, la visibilidad que tienen, los puntos de acceso, la confianza y las interacciones entre los objetivos que se encuentren en el mismo ámbito; también, se identifican los controles. Los módulos revisados en esta etapa son:

- B.4 Auditoría de visibilidad
- B.5 Verificación de acceso
- B.6 Verificación de confianza
- B.7 Verificación de control

Fase de indagación o investigación: En esta etapa se valida la interacción y las respuestas generadas por el objetivo en un estado normal; con esto se busca comprender sus interacciones y las posibles fallas que se puedan explotar. También se pretende determinar la existencia de los controles y su eficacia; se hace una búsqueda de información libre que permita afectar a otros objetivos directa o indirectamente. Los módulos que contiene esta etapa son:

- C.8 Verificación de procesos.
- C.9 Verificación de configuración/ verificación de capacitación.
- C.10 Validación de propiedad.
- C.11 Revisión de segregación.
- C.12 Verificación de la exposición.
- C.13 Inteligencia competitiva de exploración.

Fase de intervención: Esta fase se centra en los recursos definidos en el alcance de la prueba, y los recursos pueden ser alterados, modificados o sobrecargados con el fin de lograr una interrupción del servicio o acceso al recurso mismo; frecuentemente esta es la fase final de una prueba de seguridad. La mayoría de las pruebas de seguridad que no incluyen esta fase pueden necesitar una revisión final desde la perspectiva de los objetivos y los activos para aclarar cualquier anomalía. Los módulos que pertenecen a esta etapa son:

- D.14 Verificación de garantía.
- D.15 Privilegios de auditoría.
- D.16 Continuidad del servicio.
- D.17 Revisión de alertas y registros/ Encuesta final

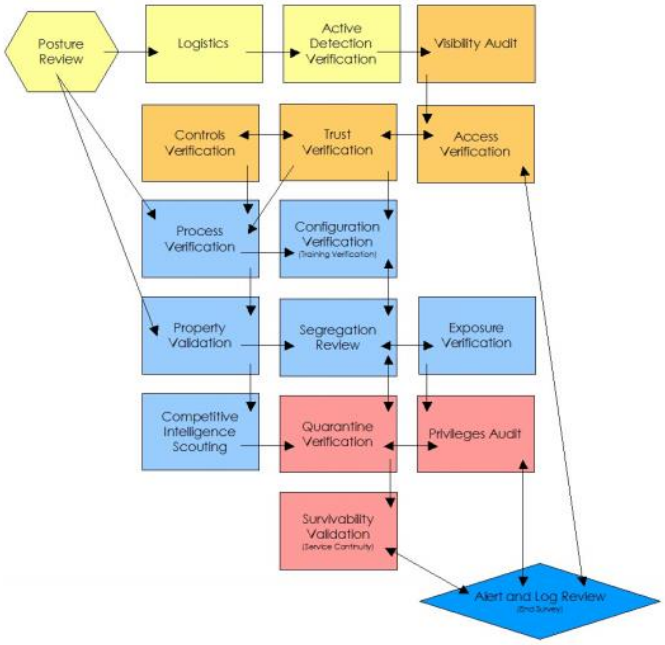

Fig. 2. Módulos propuestos por OSSTMM para realizar las pruebas en cada uno de los canales. [5]

Las auditorías de seguridad buscan establecer el estado actual en el que se encuentra la seguridad de una organización para definir cómo actuar frente a las amenazas encontradas. OSSTMM incluye en su última versión un nuevo concepto Risk Assessment Values (RAV), el cual permite identificar el estado actual de seguridad con base en la superficie de ataque. RAV es una métrica operativa, es decir, una medida constante que posibilita tener una estadística y realizar seguimiento del comportamiento que ha tenido la seguridad de la organización a través del tiempo.

Para que el uso de esta métrica sea útil, se debe evitar datos imprecisos y relativos a través del reduccionismo, proceso que pretende encontrar los componentes mínimos requeridos. El RAV estandariza qué superficie de ataque se evalúa a partir de tres (3) elementos: porosidad, controles y limitaciones. Además, el RAV como cualquier métrica operacional, debe ser aplicado correctamente para que sea útil y así la finalización de

pruebas de seguridad arroje datos precisos que validen los datos de seguridad actual.

El RAV es una medida en escala de la superficie de ataque expuesta que es un cálculo cuantitativo que busca el balance entre operaciones, limitaciones y controles. El equilibrio se identifica dentro de la escala como 100, si la evaluación del RAV arroja un valor inferior muestra falta de controles y mayor superficie de explotación; por el contrario, si es mayor señala que se tienen controles innecesarios que dan cobertura a la superficie de ataque.

El RAV no mide el riesgo de una superficie de ataque o si se atacará un objetivo particular, lo que si puede establecer es la superficie de ataque expuesta, es decir, dónde pueden atacar a un objetivo; además, establece contra qué ataques se puede defender exitosamente, así como la profundidad y el daño que puede llegar a causar un atacante.

La superficie expuesta es la combinación de diferentes cálculos que miden la porosidad, controles o limitaciones y se muestra de 2 formas prácticas para su análisis. La primera, es el cálculo de DELTA, un número positivo o negativo que describe la exposición específica de un objetivo. Cuando es positivo, se puede interpretar como el gasto excesivo en controles. Por otro lado, si es negativo indica qué tan lejos el objetivo está de una seguridad perfecta o en equilibrio. La segunda forma muestra la superficie de ataque dando a conocer un panorama general de la organización, teniendo esto claro se puede evaluar el riesgo, determinar qué está expuesto, qué no tiene control y está expuesto ante las amenazas, dando herramientas para un análisis de riesgo preciso como se presenta en la Fig. 3 [5]

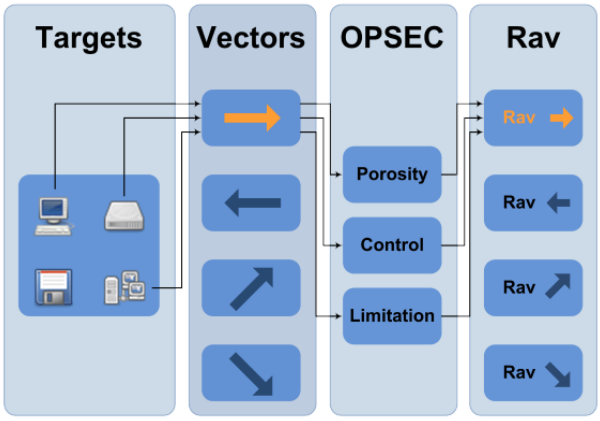

Fig. 3. Elaboración de un RAV a partir de las pruebas de seguridad. [5]

IV. Penetracion Testing Excecution Estandar (PTES)

Penetration Testing Excecution Standar (PTES) es otro de los estándares que se abordará en este artículo; éste brinda a las empresas y a los proveedores de servicios de seguridad un marco y alcance común para realizar las pruebas de penetración, se divide en siete (7) grandes segmentos como se muestra en la Fig. 4. y que a continuación se describen [6]:

Pre-engagement Interactions o Interacción previa: Esta etapa pretende establecer las reglas sobre el trabajo que se va a llevar a cabo; se busca dejar total claridad en el alcance, lo cual implica definir el objetivo, la infraestructura que ingresa dentro de las pruebas de penetración, aplicaciones web, rango de IP's dominio, el tiempo que va a tomar la ejecución de las pruebas de penetración, la tarifa del servicio, tarifa por hora, fechas de inicio y fin de las pruebas de penetración. Además, se define hasta dónde se van a tener en cuenta los proveedores de servicios, las líneas de comunicación, contacto de emergencia y frecuencia de entrega de reportes. Por último, la metodología plantea un cuestionario que le permitirá entender aspectos sobre la empresa donde se llevarán a cabo las pruebas de penetración. Este proceso resulta importante a la hora de establecer las expectativas del cliente y así entender cuáles son los resultados esperados.

Intelligence Gathering o recolección de información: En PTES se plantean tres (3) tipos de niveles de recolección de información: Nivel 1. La recolección más simple que se puede hacer de forma automática con las herramientas que se encuentran en el mercado; Nivel 2. Una recolección que requiere mayor esfuerzo ya que demanda un análisis profundo, a pesar de que gran parte de la información se puede obtener de manera automática. Asimismo, requiere un conocimiento básico del negocio, las relaciones comerciales y la estructura de la organización; Nivel 3. Es el más complejo, pues además de contemplar los niveles 1 y 2, demanda conocer el negocio en su totalidad, por lo que es necesario cultivar nuevas relaciones.

Una vez definidos estos niveles, se puede decir que el objetivo de esta fase es recolectar tanta información como sea posible para usarla en la evaluación de vulnerabilidades y la fase de explotación cuando se esté realizando la penetración al objetivo. Esta fase se lleva a cabo para determinar los puntos de entrada del atacante, porque muchas empresas comparten información al público que sin saberlo puede ser usada para ser atacados. En esta etapa es importante tener en cuenta las reglas para la recolección de información planteadas por el cliente y el objetivo final; de este modo, se evita perder tiempo y dinero examinando sistemas que están fuera del alcance.

Open Source Intelligence (OSINT) hace referencia a tres formas de recolectar información: pasiva, semi-pasiva y activa.

Pasiva: Estas pruebas no son muy comunes y suelen ejecutarse cuando es claro que la recolección activa no permitirá encontrar ningún tipo de información, acá solo se va a usar información almacenada o archivada. En este escenario no se va a lanzar tráfico hacia el objetivo.

Semi-pasiva: El objetivo de este método es crear un perfil con el tráfico de internet y su comportamiento, solo se consultan los servidores expuestos públicamente, pero sin intentar hacer un escaneo de puertos o ataques de fuerza bruta sobre el DNS.

Activa: En este punto se buscará todo tipo de información haciendo uso de diversas técnicas como escaneo de puertos, escaneo de servicios o mapeo de la infraestructura de la red. También, se explorarán archivos, directorios o servidores inéditos.

Threat Modeling o modelamiento de amenazas: La metodología no define un modelo específico para esta etapa, aun así, el más usado debe ser coherente en términos de representación de amenazas, y poder aplicarse de forma repetida obteniendo los mismos resultados. La metodología se enfoca, principalmente, en dos aspectos del modelamiento de amenazas por parte del atacante y sus capacidades.

Claro está que también se debe tener en cuenta el valor de los activos y el costo de adquisición; como un modelo complementario, se debe tener un modelo de impacto para la organización con el propósito de tener una visión más objetiva de los posibles escenarios en los que se materialice una amenaza. En consecuencia, se debe tener claro el contexto de cada uno de los activos identificados y su valor neto, intrínseco y cualquier costo que tenga relación directa o indirecta con su perdida.

Esta fase tiene gran importancia dentro del proceso tanto para la organización como para los pentester porque permite priorizar los activos de la organización, dando al pentester una base para probar procesos, procedimientos y controles más destacados.

Vulnerability Analysis o análisis de vulnerabilidades: Esta fase consiste en detectar las vulnerabilidades del sistemas o aplicaciones que un atacante puede usar para acceder. Este tipo de fallas pueden ser desde configuración de servidores y servicios hasta el desarrollo de aplicaciones sin tener estándar de desarrollo seguro. Para realizar esta actividad el analista debe establecer un alcance claro razón por la cual se determina la profundidad y amplitud de la prueba.

Esta etapa se puede evaluar en dos fases activa y pasiva; la activa se refiere a la interacción directa con el componente o servicio que se está evaluando; este puede estar en la capa de trasporte o en la capa de aplicación, esta interacción se puede realizar de forma manual o automática; la pasiva es la exploración de los metadatos en los archivos expuestos al público, en estos metadatos se puede encontrar información que pueda servir a un atacante para realizar recolección de información.

Al terminar esta fase se debe contar con una lista de objetivos de alto valor que serán el insumo para la siguiente etapa.

Exploitation o explotación: Consiste únicamente en determinar el acceso a un sistema, por tanto, es fundamental haber realizado correctamente el análisis de vulnerabilidades para tener claro el punto de entrada y reconocer los activos de alto valor. En esta fase lo ideal es tener enumeradas las contramedidas que pueda tener la organización, entendiendo contramedida como una herramienta tecnológica o de control que tiene la víctima para evitar una intrusión exitosa, algunas de estas herramientas pueden ser firewall, Web Application Server (WAF), Intrusion detection system (IDS), entre otros.

Cuando se encuentra con alguna de estas contramedidas se debe tener un método de explotación alternativo; es importante resaltar que los vectores de ataque y código malicioso son herramientas genéricas. Para que esta etapa sea exitosa se debe personalizar el ataque, es decir, el exploit se debe modificar con base en la tecnología e infraestructura propia de la organización.

Post Exploitation o Post explotación: Se busca valorar la máquina comprometida; esta valoración se da en función de la información almacenada, privilegios que tenga, otras máquinas a las que se pueda acceder o la utilidad para comprometer la red.

En esta etapa es de vital importancia precisar con el cliente los roles y responsabilidades establecidos en las primeras fases, y de forma contractual; para proteger la organización, como regla general, se debe demostrar que cada cambio en la configuración o el exploit usado tenía como objetivo mostrar como un atacante podría escalar privilegios, tener acceso a datos, denegar servicios etc.; claro está que este proceso se hace sin llevar a cabo ninguna actividad injustificada que ponga en riesgo a la organización. Ahora bien, la configuración modificada como parte de la prueba de penetración se debe restablecer y los datos o información sensible se debe entregar al cliente; por otra parte, para realizar este tipo de pruebas se debe tener el consentimiento del cliente, y dejar en claro qué y cómo se va a hacer, con el fin de evitar problemas legales al acceder a un sistema sin autorización.

Reporting o presentación de reporte: esta metodología no proporciona un formato para presentar un reporte de pruebas de penetración, pero si da una guía de los puntos que se deben exponer. Se debe presentar el contexto en el que se realizaron las pruebas, mostrar los lineamientos sobre los cuales se hizo y los objetivos alcanzados, manifestar los riesgos clasificándolos por su criticidad, presentar los hallazgos encontrados y las recomendaciones, que son las actividades que debe realizar para resolver los riesgos encontrados.

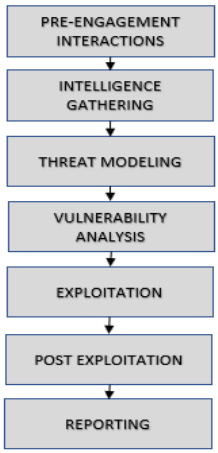

Fig. 4. Etapas de la metodología PTES.

V. Testing Guide

The Open Web Application Security Project (OWASP) es un proyecto que como su nombre lo indica está enfocado en la seguridad de las aplicaciones web; sin embargo, al igual que las otras metodologías que ya se han presentado, ofrece un marco de referencia para llevar a cabo unas pruebas de penetración, pero alineadas al ciclo de vida del software. La guía explica los costos que un software inseguro genera en una organización.

Asimismo, la guía en cada una de sus etapas presenta las actividades, técnicas y tareas que se deben aplicar, caracterizando de forma detallada los aspectos técnicos sobre cómo se realiza la prueba, aunque esto no hace parte del objetivo y alcance de este documento, por tanto, solo se mencionaran algunas de las actividades. A continuación, se muestra en las Fig. 5 y se describirá más adelante cada una de las etapas que propone la guía de OWASP [7].

Fig. 5. Flujo de trabajo del marco de pruebas OWASP. [7]

Antes del desarrollo: Se debe tener definido un ciclo de vida del desarrollo, en el cual la seguridad esté presente. En cada una de las etapas se debe confirmar que existan estándares y documentación para el desarrollo; la documentación es un factor importante porque da los lineamientos al equipo.

En esta etapa se deben establecer las métricas con las que se medirá el producto; éstas deben ser proporcionales al tamaño y complejidad del desarrollo. Es esencial que estas métricas estén antes de iniciar el desarrollo con el fin de hacer las modificaciones pertinentes y evitar reprocesos en etapas posteriores.

Durante la definición y diseño: Uno de los elementos que se debe tener en cuenta en esta etapa es la revisión de requisitos de seguridad, y es parte fundamental probarlos; en este contexto, probar hace referencia a verificar los supuestos que se hacen en los requisitos y las pruebas para validar si hay diferencias. Con esto se pretende evitar ambigüedades y así tener claridad en los requerimientos. Al definir o evaluar los requisitos de seguridad se deben considerar mecanismos como autenticación, autorización, administración de usuarios, integridad, etc.

En esta etapa se debe definir el diseño y arquitectura de la aplicación tomando en consideración los factores de seguridad asociados, que debe ser documentado en texto, diagramas y/o artefactos. De igual manera, la definición debe estar alineada con los requisitos definidos previamente por lo que debe validarse. Esta es una etapa donde identificar errores en diseño o arquitectura no sólo es eficiente a nivel de presupuesto sino también a la hora de realizar modificaciones a la aplicación.

El siguiente paso es realizar diagramas UML donde se evidencie el comportamiento de la aplicación, para comprobar que el equipo de diseño y desarrollo tienen el mismo entendimiento de cómo funciona la aplicación. Para finalizar esta etapa se realiza un diagrama de amenazas que consiste en construir escenarios realistas de las posibles amenazas y garantizar que se hayan tomado las acciones necesarias para mitigar, aceptar o transferir el riesgo.

Durante el desarrollo: En principio se codifica el diseño definido con antelación. Esto no aplica del todo en el contexto laboral, pues si se realizó un buen diseño, solo se definirán algunos detalles que eran muy dispendiosos de especificar al documentar el diseño. De lo contrario, es decir, en caso de haber hecho un mal diseño o no contarse con políticas o estándares adecuados, el desarrollador deberá tomar diversas decisiones que pueden extralimitar sus funciones.

En esta etapa se debe realizar una labor conjunta entre el equipo se seguridad y el de desarrollo donde éste último muestra el código al personal de seguridad explicando la lógica y el flujo del código escrito. El propósito de este paso no es hacer una auditoría del código sino tener una comprensión de

alto nivel sobre la lógica, diseño y estructura del código. Una vez la persona de seguridad tiene un entendimiento profundo de la aplicación, se procede a realizar una revisión en busca de posibles fallos de seguridad.

Durante la implementación: Para esta etapa se deben considerar diversos aspectos de seguridad, como garantía adicional se pueden realizar unas pruebas de penetración después de la implementación. En estas pruebas no sólo se debe tener en cuenta la aplicación sino la infraestructura sobre la que fue montada para encontrar vulnerabilidades en configuraciones o servicios.

Mantenimiento y operaciones: Se debe haber generado y establecido un procedimiento para realizar la evaluación periódica de los sistemas y aplicaciones, en el cual se describa las actividades de verificación después de realizar la implementación de un cambio.

Para finalizar la guía, OWASP plantea la estructura de una prueba de seguridad de una aplicación web, esta se divide en dos: pasiva y activa. Pasiva hace referencia a interacción con la aplicación directamente en busca de entender lógica, entradas y salidas. En la activa con el conocimiento adquirido en las pruebas pasivas se intenta vulnerar la aplicación, para las pruebas de seguridad activas OWASP propone once (11) categorías y noventa y un (91) controles.

1. Recopilación de información
2. Pruebas de gestión de configuración e implementación
3. Pruebas de gestión de identidad
4. Pruebas de autenticación
5. Pruebas de autorización
6. Pruebas de gestión de sesión
7. Pruebas de validación de ingreso
8. Manejo de errores
9. Criptografía
10. Pruebas de lógica del negocio
11. Pruebas del punto de vista del cliente

VI. Information System Security Assesment Framework (ISSAF)

Es una metodología propuesta por Open Information Systems Security Group que permite evaluar los controles establecidos para la red, sistemas y aplicaciones. Esta metodología está segmentada en tres etapas con nueve pasos para su evaluación [8] como se detalla en la Fig. 6.

A.1 Fase-I: Planeación y preparación. En esta etapa inician las pruebas de penetración y se plantean los lineamientos para realizar la auditoría, se elabora un contrato explicando la responsabilidad de ambas partes proporcionando protección legal mutua. Se sugiere realizar las siguientes actividades durante esta etapa:

- Reunión inicial del proyecto donde se define el alcance, el enfoque y la metodología de trabajo.
- Identificar contacto y definir ruta de escalamiento de ambas partes.
- Aceptar casos de prueba propuestos.

A.2 Fase-II: Evaluación. En esta fase se centra el mayor esfuerzo de la auditoría. La metodología sugiere nuevas capas para evaluar la organización como se expone a continuación [8]:

A.2.1 Information gathering o recolección de información consiste especialmente en buscar la mayor cantidad de información del objetivo a través de herramientas técnicas o navegadores; en esta capa inicia cualquier auditoría informática y se busca ser lo más recursivo posible explorando la mayor cantidad de vías con el fin de entender mejor la entidad que se quiere atacar. En esta etapa cualquier información se puede volver relevante iniciando con folletos, tarjetas de presentación, anuncios en periódicos, etc. Para llevar a cabo estas tareas no se requiere contacto directo con el sistema objetivo, la información usualmente se obtiene de fuentes públicas en internet.

A.2.2 Network mapping o mapeo de red tiene como propósito modelar la posible topología que tiene el objetivo, host vulnerables, puertos y servicios, mapeo de red perimetral, identificación de servicios críticos e impresión de huellas de sistemas operativos para ello el auditor pasa a un aspecto más técnico por lo que se apoya en un sin número de herramientas.

A.2.3 Vulnerability identification o identificación de vulnerabilidades, para esta sección el auditor con base en la información recolectada hasta el momento y su experticia se decanta por probar puntos específicos. Para llevar a cabo esta labor se deben conocer los servicios vulnerables, por lo que se puede apoyar de las vulnerabilidades conocidas y publicadas por los fabricantes o la comunidad como puede ser los CVE o CERT.

A.2.4 Penetration o penetración, se intenta ingresar evadiendo los controles que tenga el objetivo y obteniendo el máximo nivel de acceso. En casos particulares, el auditor puede diseñar e implementar sus propias herramientas o script, evaluando el costo/beneficio; además de realizar pruebas de concepto que una vez validadas y aplicadas sobre el objetivo permitirán tener certeza de las vulnerabilidades existentes. Esto se plasmará en la documentación, explicando en detalle las acciones ejecutadas para llevar a cabo la explotación de sistemas y el impacto que tiene sobre la organización.

A.2.5 Gaining access and privilege escalation u obtener acceso y escalar privilegios. Esta tarea se puede realizar de varias formas: usando ataques de fuerza bruta, ataques de diccionario, aprovechando perfiles sin contraseña, configuraciones preestablecidas por los fabricantes y/o servicios expuestos públicamente que permitan ejecutar

comandos sobre el sistema. Usualmente para poder comprometer el objetivo es necesario evadir contramedidas intermedias como puede ser firewall, IDS entre otros. Una vez se tenga el acceso se debe buscar la forma de tener privilegios administrativos dentro del sistema que sería el objetivo final de esta etapa, la dificultad de esta tarea depende del aseguramiento que tenga el objetivo.

A.2.6 Enumerating further o enumeración, en esta sección se busca encontrar las vulnerabilidades que tiene el sistema. Para esto, el auditor puede apoyarse en múltiples técnicas, obtener contraseñas cifradas o en texto plano, capturar y analizar tráfico de red, recolectar correos electrónicos y/o cookies de sesión.

A.2.7 Compromise remote user/sites o comprometer usuarios/sitios remotos, cualquier vacío en la seguridad puede permitir a un atacante ingresar a un sistema; aunque, no es una garantía total que una organización use canales seguros para la comunicación evitando que la información sea alterada en el medio. El auditor puede comprometer los accesos o sitios remotos que por sus características pueden dar privilegios dentro del sistema.

A.2.8 Maintaining access o mantener acceso, con la explotación de sistema el siguiente objetivo es dejar un acceso abierto. Esto es lo que se conoce como un back door, el cual será usado para instalar exploit, script, rootkits etc. Esta tarea generalmente no se realiza dentro de la auditoría por la amenaza que genera para una organización si un atacante ingresa por estos accesos.

A.2.9 Cover the tracks o cubrir huellas. En este punto la metodología muestra de manera informativa cómo en un proceso de auditoría se debe ser lo más transparente posible con el cliente, por lo que no es necesario quitar la evidencia de la actividad que se realizó a menos de que la auditoría tenga como alcance esta etapa; en ese caso se deben ocultar los archivos usados durante la intrusión, limpiar logs, regenerar firmas en el servidor (este aspecto depende de los aplicativos usados para asegurar el sistema) y activar el antivirus si en la intrusión se desactivó.

En ISSAF hay un punto adicional a los nueve puntos ya descritos; éste hace referencia a la revisión de la auditoría del sistema, que puede brindar mucha más información que las pruebas de penetración en sí mismas. Se recomienda hacer esta revisión una vez las pruebas de penetración hayan terminado para establecer servicios en ejecución, conexiones, puertos y registro remoto de acuerdo con la lista de verificación que se tenga para cada sistema en particular.

A.3 Fase-III: Reporte, limpieza y destrucción de artefactos. Como en las otras auditorías, esta es la etapa en la que se presenta al cliente los avances, hallazgos encontrados y la evidencia del trabajo realizado.

A la hora de reportar incidentes, ISSAF establece que se debe informar de inmediato de forma verbal, discutir cómo impacta este incidente a las pruebas y qué medidas se tomarán para solucionar el inconveniente.

Una vez culminados todos los casos de prueba dentro de la auditoría es hora de presentar el informe final al cliente; en éste se deben describir las actividades realizadas y los resultados obtenidos. También, debe contener las recomendaciones para mejorar la seguridad de los hallazgos encontrados, ISSAF [8] propone la siguiente estructura para un buen informe:

- Resumen administrativo
- Alcance del proyecto (y temas fuera del alcance)
- Herramientas usadas
- Fechas y horas del sistema en las que se realizaron las pruebas.
- El resultado de cada actividad realizada, en este punto se puede excluir el informe de exploración de vulnerabilidades este puede ir como adjunto.
- La lista de todas las vulnerabilidades encontradas con las acciones que indiquen como sanear esos hallazgos.
- Lista de acciones, acá se da una priorización del orden en que se deben ejecutar las acciones propuestas.

La limpieza y destrucción de artefactos constituye el último paso dentro de esta etapa y hace referencia a borrar la información creada y/o almacenada que se usó en la auditoría, restablecer las configuraciones, desconectar conexiones, entre otras. En caso de no poder realizar esta actividad, se deben hacer explícitas las tareas a realizar dentro del informe técnico para que el departamento de sistemas de la empresa se encargue de restablecer el sistema.

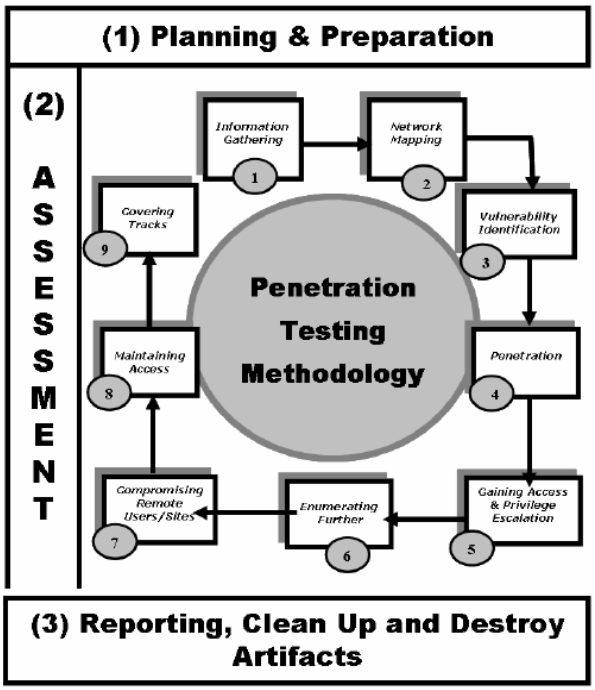

Fig. 6. Etapas y pasos de evaluación para la metodología ISSAF. [8]

La metodología es muy concreta en sus tres etapas. La segunda fase como ya se mostró tiene nueve aspectos a evaluar y ésta requiere un alto conocimiento técnico para que las pruebas sean lo más efectivas posibles y los datos arrojados sean confiables. Para apoyar esta labor ISSAF entrega un apartado en el que explica cómo se realiza cada una de las nueve fases de evaluación que exige la fase II, acá se encontrará una explicación más detallada; por ejemplo, para el primer punto a evaluar que es la recolección de información, plantea los dos escenarios: recolección pasiva y activa, detallando para cada uno de estos cuáles son las estrategias, sugerencias y herramientas que debe usar.

Y así lo hace con los ocho aspectos restantes, indicando el método que se va a usar, dando una descripción de lo que se va a hacer, un ejemplo y los resultados que a alcanzar, cómo analizar los resultados obtenidos y las contramedidas que se pueden tomar para que un atacante real no use estas herramientas para tener información del sistema que quiere atacar.

VII. Herramientas

Con la necesidad de hacer más eficiente las pruebas de penetración han surgido herramientas como open source o de pago, que automatizan algunas de las tareas de las pruebas de penetración, permitiendo al pentester enfocarse en analizar la información. A continuación, se listan algunos de los recursos que pueden ser usados dentro de las pruebas de penetración.

Maltengo: Es una herramienta que permite recolectar información de internet de personas u organizaciones, permitiendo cruzar información para obtener cuentas de redes sociales y correos electrónicos. Maltengo tiene dos tipos de módulos de servidor, profesional y básica, la diferencia principal son los módulos a los que tiene acceso cada versión. Para terminar Maltengo cuenta con una interfaz gráfica muy intuitiva, su licencia es propietaria teniendo versiones de pago y libre.

Nessus: Es una solución de evaluación de vulnerabilidad estándar de la industria que ayuda a identificar vulnerabilidades, incluyendo fallas de software, parches faltantes, malware y configuraciones erróneas, en una variedad de sistemas operativos, dispositivos y aplicaciones. Tiene una licencia propietaria de pago.

OpenVas: Software de escaneo de vulnerabilidades muy completo, optimizado para pruebas a gran escala, dentro de sus características están: realizar pruebas no autenticadas y pruebas autenticadas; además, cuenta con su propio lenguaje para implementar cualquier tipo de prueba de vulnerabilidad. Su licenciamiento es GNU GPL.

Kali: Es una distribución basada en Linux, su antecesor se puede decir que es BackTrack. Este sistema operativo está enfocado en la auditoría y la seguridad informática en general, trae preinstalado muchas herramientas para diferentes actividades como escaneo de puertos, sniffer, crakeo de contraseñas, pruebas de seguridad inalámbrica, entre otras. Su licencia es GPL.

Foca: Es una herramienta para encontrar metadatos e información oculta en documentos de texto y hojas de cálculo, etc. Realiza una revisión completa de los ficheros para obtener datos relevantes de una empresa. Es una herramienta que se emplea de forma recurrente durante la etapa de recolección de información.

Cain: También conocido como Cain y Abel, es una herramienta para la recuperación de contraseñas bajo diferentes métodos como fuerza bruta, diccionario de datos o criptoanálisis; entre sus características se destaca crakeo web, aceleración de captura de paquetes, calculadora de hashes y ARP Spoofing. Su licencia es de software libre.

Nmap: Utilidad multi plataforma de código abierto con licencia GNU para descubrimiento de redes y auditoría de seguridad. Emplea paquetes de IP sin procesar para determinar si un host está disponible en la red, los servicios activos, el sistema operativo y los filtros que tiene el firewall; dentro de sus atributos están su flexibilidad, portabilidad, soporte por parte de una comunidad activa y la buena documentación que lo acompaña.

Metasploit: Framework con licencia BDS. Permite desarrollar y ejecutar exploit contra máquinas remotas. Se construyó inicialmente en leguaje Perl, pero fue reescrito en Ruby; está orientado al desarrollo y ejecución de exploit contra máquinas remotas. La versión no paga tiene soporte de la comunidad y la versión paga conocida como Metasploit pro está soportada por Rapid 7.

Zenmap: Se puede decir que es un cliente de Nmap que brida una interfaz gráfica para simplificar su uso sin perder su poder. Usada para escaneo, detección y explotación de vulnerabilidades. Su licenciamiento es de software libre.

VIII. Conclusiones

Las metodologías presentadas buscan dar una estructura para realizar las pruebas de vulnerabilidad, sin embargo, cada una de ellas tiene un enfoque particular, el cual se debe tener en cuenta a la hora de realizar su implementación en una empresa de acuerdo con los resultados que se estén esperando.

A pesar de las diferencias evidenciadas todas siguen una estructura general que consiste en entender el contexto en el que se va a realizar las pruebas de penetración e intrusión, hacer un acercamiento al objetivos interactuando y conociendo el sistema en busca de vulnerabilidades, la explotación de esas vulnerabilidades y finaliza con la elaboración y presentación de un informe donde se muestra el procesos realizado, hasta dónde se puede llegar si se explotan las vulnerabilidades y lo

más importante las recomendaciones para cerrar esas brechas de seguridad que ponen en riesgo a la organización.

Las metodologías presentadas constituyen un marco de referencia y como tal no requieren un seguimiento estricto para su uso; por el contrario, cada auditor y organización puede implementarlas según el objetivo que esté buscando o la orientación que quiera darle a las pruebas; de hecho, puede utilizar los lineamientos propuestos por las diferentes metodologías y definir una estructura propia para realizar las pruebas de penetración e intrusión.

Las pruebas de penetración permiten entender los riesgos a los cuales está expuesta una organización, evaluando cada uno de los elementos que hacen parte de la operación de la empresa, sin limitarse exclusivamente a componentes tecnológicos, sino involucrando todos los eslabones que participan en los procesos que permiten la operación diaria de una empresa como pueden ser el factor humano y/o políticas de seguridad, con el fin de entender los diferentes vectores de ataque por el que un intruso puede explotar las vulnerabilidades presentes en la organización.

RERERENCIAS

[1] L. Allen, T. Heriyanto, S. Ali, "Penetration testing methodology," en Kali Linux – Assuring Security by Penetration Testing, 2da edición, Birmingham: Pack Publishing, 2014.

[2] A. A Ramos, C. A. Barbero, R. Martínez, A. G. García, J. M. González, "Introducción al pentest web," en Hacking y seguridad de páginas web, Bogotá: Ra-Ma, 2015.

[3] J. L. Guillen, "Introducción al pentesting", Tesis de grado, Depto. Matemáticas e informática, Universidad de Barcelona, Barcelona, 2017.

[4] K. Rodríguez. Metodologías para la auditoría de seguridad. (2017). Disponible [en línea] https://www.linkedin.com/pulse/metodolog%C3%ADas-para-la-auditoría-de-seguridad-kevin-rodriguez-lago

[5] ISECOM. OSSTMM 3 – The Open Source Security Testing Methodology Manual. (2010). Disponible [en línea] http://www.isecom.org/mirror/OSSTMM.3.pdf

[6] PTES technical guidelines. "High Level Organization of the Standard". (2014). Disponible [en línea] http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

[7] OWASP Guide 4.0 (2014). "El Framework Referencial de Pruebas OWASP". Disponible [en línea] https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml

[8] Information system security Assesment Framework -ISSAF- (2006). "Penetration Testing Methodology". Disponible [en línea] https://untrustednetwork.net/files/issaf0.2.1.pdf

Carlos A. Castro. Nació en agosto de 1988 en la ciudad de Bogotá D.C., Colombia. Recibió el título de Ingeniero de Sistemas e Informática de la Universidad Libre de Colombia. Se ha desempeñado como Ingeniero de proyectos desde el año 2012 en diferentes entidades de carácter privado. Actualmente, opta por el título de especialista en Seguridad Informática en la Universidad Piloto de Colombia.