ANALISIS Y PRUEBAS DE NIVELES DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN LAS GUIAS DEL OSSTMM v3

Sierra Quintana, Gustavo Oswaldo
goro27@hotmail.com
Universidad Piloto de Colombia

***Resumen*— El documento consta de los pasos necesarios para realizar pruebas y validaciones de los niveles de seguridad a nivel operativo basado en la metodología encontrada en el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) en su tercera versión.**

***Abstract*— This document consists of steps to performs tests and validations of security levels based on the methodology found in Open Source Security Testing Methodology Manual (OSSTMM) in its third versión.**

***Índice de Términos*— OSSTMM, Pruebas de Seguridad, medición, metodología, auditoría**

I. INTRODUCCIÓN

Para una empresa, aplicación e incluso infraestructura es primordial conocer los niveles de seguridad a nivel operativo con los que cuenta y que mejor que con una metodología que a través del tiempo se ha vuelto un estándar de auditoría ya que ayuda a conocer que es lo que se debe probar, como se pueden realizar estas pruebas y cuando se hacen necesarias realizar dichas pruebas.

La metodología que mejor representa las necesidades explicadas anteriormente es la Metodología OSSTMM (Manual de Metodología de Pruebas de Seguridad de Código Abierto) la cual fue creada por ISECOM (Institute for Security and Open Methodologies) en el año 2001, bajo la licencia Creative Commons por lo que se permite su libre uso y distribución, como una manera distinta de probar e implementar la seguridad a un nivel operativo [1] y como un marco de trabajo de buenas prácticas hasta que en el año 2005 fue considerado como una metodología para asegurar la realización correcta de la seguridad a nivel operacional [2].

Lo que hace que esta metodología sea tan utilizada es que en ella se incluyen la totalidad de los canales de operación empresarial:

- Físico
- Humano
- Telecomunicaciones
- Redes de Datos

Ahora, si se habla de Seguridad en Sistemas de Información la metodología se divide en:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

Para todos estos aspectos se establecen una cantidad de pruebas específicas por área con las que se prueban las especificaciones de seguridad acompañadas de validaciones rutinarias.

II. MANUAL OSSTMM V3

Para su tercera versión, publicada el 14 de diciembre de 2010, ISECOM reescribió totalmente la metodología, cambió el orden del mapa de seguridad y dio la capacidad de ordenar de manera mas eficiente los datos de los RAV (Valores de Evaluación de Riesgo) al explicarlos de una manera mas clara y brindando una mayor importancia a su valoración.

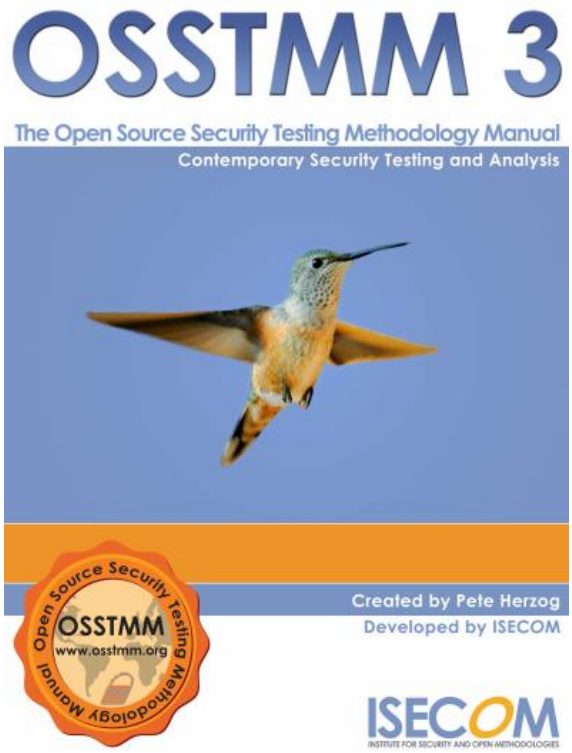

Fig. 1. Portada OSSTMMv3

III. CAPITULO 1. QUE SE NECESITA SABER

Como primer capítulo, el manual define seguridad operacional como la combinación de separación y controles, separación completa entre las amenazas y los activos de información y controles aplicados en los activos que permitan reducir el impacto de una amenaza materializada al mínimo nivel posible, además el capítulo establece lo que es necesario conocer en los ámbitos de:

a) Seguridad

Se define como la separación entre los activos y las amenazas, separación que se puede realizar de 3 maneras lógicas y proactivas:

- Crear barreras lógicas o físicas entre los activos y las amenazas
- Cambiar las amenazas a un estado 'inofensivo'
- Destruir la amenaza

b) Controles

Cuando la amenaza esta en el entorno circundante es necesario aplicar controles que provean seguridad en las operaciones, los controles se definen como caminos que logren apaciguar el impacto de las amenazas y sus efectos cuando su activación es requerida.

En ese punto, el manual tiene una frase bastante interesante que es: "*El hecho de que algo no pueda ser controlado directamente no significa que no se pueda controlar. Si controlas el entorno controlas todo lo que hay en él.*"

Teniendo como objetivo la frase anterior, se establecen 2 tipos de Controles:

- Controles Interactivos
  - Autenticación
  - Indemnización
  - Resistencia
  - Subyugación
  - Continuidad
- Controles de Proceso
  - No repudio
  - Confidencialidad
  - Privacidad
  - Integridad
  - Alarma

c) Objetivos de Aseguramiento de la Información

Se habla de cómo los controles operativos pueden ser integrados y separados para lograr los 3 objetivos de la Seguridad de la Información, Confidencialidad, Integridad y Disponibilidad.

d) Limitaciones

En este punto se habla de cómo la inhabilidad de los mecanismos de protección pueden ser las limitaciones para lograr dichos objetivos, y se clasifican:

- Vulnerabilidad
- Debilidad
- Preocupación
- Exposición
- Anomalía

e) Seguridad Actual

Se define seguridad actual como la captura de un momento especifico de lo que sería un ataque a un entorno operativo, una representación de los controles, limitaciones y seguridad operativa en un momento particular, esto para poder entender mejor como funciona la seguridad y donde se pueden integrar y administrar controles para su mejor funcionamiento.

f) Conformidad

En el manual se establece que la conformidad no va de la mano con la seguridad, ya que puede que algo que logre la conformidad de la alta gerencia no sea seguro como que algo que sea muy seguro no logre los niveles de conformidad de la alta gerencia, por lo que se requiere documentación de versionamiento y actualizaciones, documentación que pueda ser accedida por auditores internos y externos.

IV. CAPITULO 2: QUE SE NECESITA HACER

Ya en el capitulo dos el manual especifica que es necesario hacer, por donde se puede empezar, como distribuir y administrar cualquier complejidad que surja por lo que necesario:

a) Definir las pruebas de seguridad

Para lograr definir correctamente una prueba de seguridad es necesario seguir 7 pasos

1. Definir lo que se desea proteger, es decir los activos de información.
2. Identificar el contexto de los activos entre estos los mecanismos de protección, procesos y servicios, es decir la zona de compromiso.
3. Definir los elementos sobre los cuales no se puede influir directamente y los elementos que mantienen la infraestructura operacional como procesos, protocolos y recursos continuos, lo que concluye que en este paso se define el alcance de prueba.
4. Se define como el alcance interactúa con el exterior y dentro de sí mismo, es decir, definir los vectores.
5. Se identifican los equipos necesarios para cada prueba ya que en cada vector pueden ocurrir interacciones a distintos niveles y estos son clasificados en 5 canales: humanos, físicos, inalámbricos, de telecomunicaciones y redes de datos.
6. Determine si se están probando interacción con los activos o respuesta a medidas de seguridad, cada prueba debe definirse de manera individual y existen 6 tipos de pruebas: ciego, doble ciego, caja gris, doble caja gris, tándem y reversión.
7. Se debe asegurar que las pruebas de seguridad que se definieron cumplen con reglas de compromiso que son guías para asegurar que el proceso para cada prueba de seguridad es el adecuado evitando malentendidos, conceptos erróneos o falsas expectativas.

b) Alcance

Se define como alcance el entorno total de seguridad operativa posible para cualquier interacción con cualquier activo que pueda incluir también los componentes físicos de las medidas de seguridad. El alcance se compone de tres canales:

- Canal de seguridad de redes de datos y telecomunicaciones de la clase COMSEC.
- Canal de seguridad física y humana de la clase PHYSSEC.
- Canal de seguridad inalámbrico de espectro completo de la clase SPECSEC.

c) Tipos de pruebas comunes

Se definen 6 tipos de pruebas comunes que se diferencian según la cantidad de información que el evaluador sabe de sus objetivos, lo que el objetivo sabe sobre el probador o lo que espera de la prueba y la legitimidad de la prueba:

1. Ciego
2. Doble ciego
3. Caja gris
4. Doble caja gris
5. Tándem
6. Reversión

d) Reglas de Compromiso

Estas reglas definen los lineamientos operativos de prácticas aceptables en mercadeo y venta de pruebas, la realización de trabajos de prueba y manejando los resultados de los trabajos de prueba.

- Ventas y Mercadeo
- Evaluación / Estimación de Entrega
- Contratos y Negociaciones
- Definición del Alcance
- Plan de Pruebas
- Procesos de Prueba
- Reportes

e) El proceso en las pruebas de seguridad operacional

Este proceso es necesario ya que todo se basa en los resultados, y para ello es necesario realizar pruebas de las operaciones, por lo que se estará realizando una secuencia cronológica de pruebas en un sistema que cambia y no siempre da la misma salida para la entrada proporcionada. El objetivo es un sistema, una colección de procesos interactivos y codependientes que también está influenciado por el entorno estocástico en el que existe, por lo tanto, una prueba de seguridad operacional requiere una comprensión profunda del proceso de prueba, elegir el tipo correcto de prueba, reconocer los canales y vectores de prueba, definir el alcance de acuerdo con el índice correcto y aplicar la metodología adecuadamente.

f) Proceso de 4 puntos

Se define en el manual como el proceso de cuatro puntos (4PP) como una prueba completa de principio a fin, también se deja claro que, aunque no necesita ser exhaustivo en la documentación explicando paso a paso, pero si dejar claro como se llega de un paso a otro y que se debe esperar en los resultados para que quien siga este proceso sepa que va por buen camino.

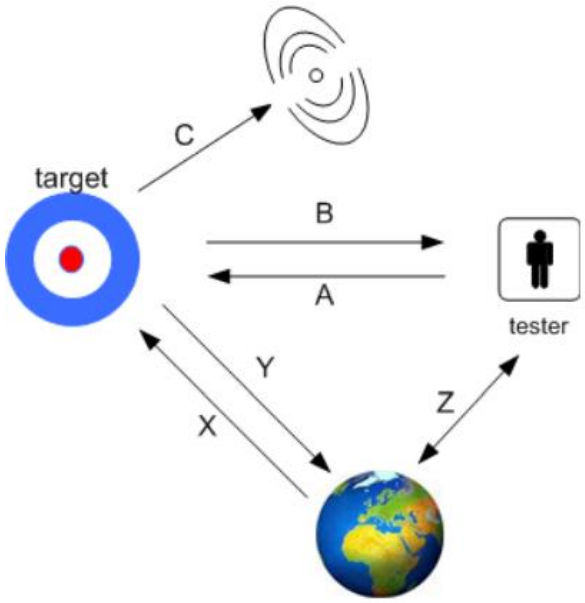

Fig. 2. Proceso de 4 puntos

En la figura 2 se especifica el proceso de 4 puntos en los que:
(Z) Inducción
(C) Encuesta
(A/B) Interacción
(X/Y/Z) Intervención

g) La trifecta

En este punto, se hace un símil de la metodología de seguridad con una orquesta, donde la metodología es la partitura que decide las pruebas necesarias, pero el analista controla el orden, la duración y la ejecución ya que el analista crea una única ruta a través de la metodología basada en el objetivo, el tipo de prueba, el tiempo asignado para la auditoría y los recursos aplicados a la prueba.
Por lo tanto, una metodología que se invoca de manera diferente para cada auditoría y por cada analista aún puede tener el mismo resultado final si el analista completa la metodología. Por esta razón, uno de los fundamentos del OSSTMM es registrar con precisión lo que no se probó. Al comparar lo que se probó y la profundidad de la prueba con otras pruebas, es posible medir la seguridad operativa (OpSec) en función de los resultados de la prueba. Al aplicar esta metodología, el objetivo del Analista será responder las siguientes tres preguntas que conforman el análisis:

- ¿Cómo funcionan las operaciones actuales?
- ¿Qué tan diferentes funcionan estas operaciones a como la gerencia piensa que funcionan?
- ¿Cómo necesitan trabajar las operaciones?

h) Manejo de Errores

El manejo de errores se distribuirá entre:

- Falso Positivo
- Falso Negativo
- Gris Positivo
- Gris Negativo
- Espectro
- Indiscreción
- Error de Entropía
- Falsificación
- Error de Muestra
- Restricción
- Propagación
- Error Humano

i) Revelación

Durante una prueba de seguridad, pueden surgir limitaciones de seguridad previamente desconocidas o no publicadas.

- Derechos de Divulgación
- Responsabilidades

V. CAPÍTULO 3: ANÁLISIS DE SEGURIDAD

Después, en el capítulo 3, el manual indica que es necesario un análisis de seguridad que es definido como la habilidad de convertir la información en inteligencia de seguridad, lo que se logra entendiendo el origen de la información, cuando y como fue recolectada y cual posible restricción surgió durante su recolección. Ya teniendo lo anterior el siguiente paso es crear lo que denominan inteligencia accionable que es información procesada que puede ser usada para tomar decisiones.

a) Pensamiento Crítico de Seguridad

El pensamiento crítico de seguridad es usado como una mezcla de la lógica y los hechos para formar una idea sobre la seguridad requerida, que puede ser una respuesta, una conclusión o una caracterización para que las pruebas de verificación estén claramente definidas, es decir el pensamiento critico de seguridad le proporcionará mas sentido a la seguridad operativa.

b) Reconocer el modelo de Seguridad Operativa

Al realizar el reconocimiento del nivel de seguridad operativa se pueden encontrar dos problemas, que la tecnología puede estar por delante de la capacidad de los analistas y estos no logran comprender el núcleo del negocio y que al momento de querer fragmentar un proceso para entender su funcionamiento se puede incurrir en irregularidades empresariales que no sean del agrado de los dueños de los procesos, por lo que el proceso que se define en este paso en el manual es que para cada vector y canal analizado, un analista colocará una superposición del modelo de Seguridad Operativa sobre los objetivos. Para aplicar el modelo es necesario contar los controles para cada punto interactivo de acceso o confianza, así como el descubrimiento de oportunidades en forma de visibilidad.

c) Búsqueda de coincidencia de patrones como señal de errores

En este punto se buscan coincidencias de patrones que muchas veces son obviados por considerar que sus resultados son obvios ya que son habilidades que los analistas desarrollan con el tiempo evitando la afectación de la calidad de las pruebas de verificación y el análisis.

d) Caracterización de los resultados

En una prueba de seguridad se realiza una hipótesis al realizar una verificación en un punto especifico del alcance, el analista recolecta los datos empíricos de esta prueba y considera si las pruebas verifican la hipótesis planteada.

e) Búsqueda de signos de intuición

A medida que avanzan las pruebas de seguridad, un evaluador puede usar la intuición para suponer que alguna prueba es necesaria o no y un analista debe prestar atención a estas pruebas y buscar signos de intuición en los que realizan las pruebas.

f) Informes Transparentes

Al momento de informar los resultados de unas pruebas, que dependerán de la superficie y nivel de seguridad operativa, un analista debe informar lo que se ha encontrado con total certeza y no posibles o probables escenarios de resultados, no puede haber lugar a adivinanzas.

VI. Capítulo 4: Métricas de Seguridad Operacional

Esta metodología define las métricas de seguridad operacional como una medida constante que informa un recuento de hechos en relación con el entorno físico al momento de realizar pruebas de seguridad operativa.

a) Conociendo el Rav

Se define al Rav como una medida de escala de la superficie de ataque, la cantidad de interacciones no controladas con algún objetivo que es calculada a través del equilibrio entre controles, limitaciones y operaciones, lo que logra entender cual es la cantidad expuesta de la superficie de ataque en la cual 100 Rav es la representación del equilibrio total, menos de esta cantidad muestra un control muy limitado y una superficie de ataque mayor y mas de 100 Rav indica que se están utilizando mas controles de los necesarios, lo que indica una complejidad innecesaria en el proceso.

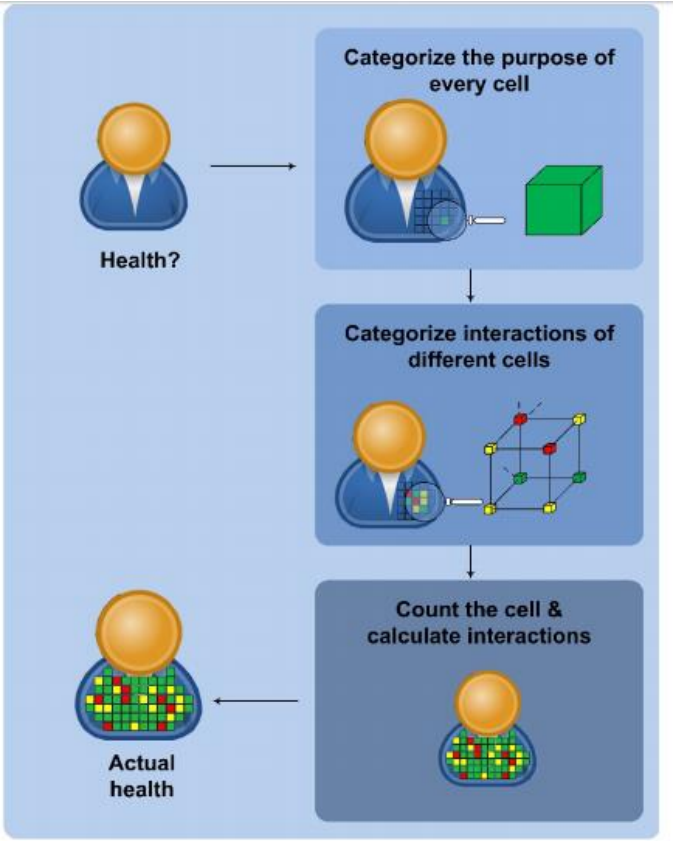

Fig. 3. Estructura Rav

b) Como hacer un Rav

Para realiza un Rav es necesaria una prueba de seguridad, se puede utilizar cualquier prueba de seguridad, pero cuanto mas profunda y precisa sea una prueba sus resultados serán más concluyentes.
Aunque el Rav fue diseñado al principio para pruebas operativas, los resultados de las pruebas realizadas lograron establecer que el Rav puede ser aplicado en pruebas no operativas como el análisis de código estático para determinar el nivel de seguridad y complejidad del software o en auditorías de listas de verificación de seguridad física para determinar el nivel de protección que proporcionará un espacio físico.

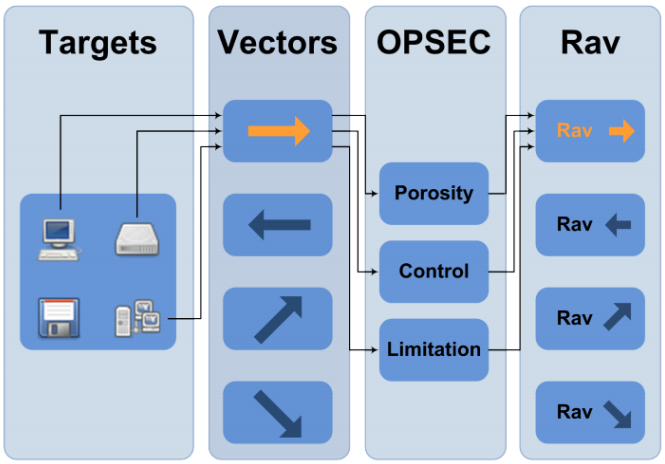

Fig. 4. Estructura Rav

c) Transformar los resultados de la prueba en una medición de ataque de superficie

Para la medición de una superficie de ataque se requieren mediciones de visibilidad, confianza y acceso en relación con el alcance y a medida que se determina la visibilidad, su valor representa el número de objetivos en el alcance.
También se requieren controles los cuales se pueden medir por autenticación, continuidad, resistencia entre otros. Y por último se requieren las limitaciones presentadas que se pueden expresar en vulnerabilidad, debilidad, exposición, anomalía etc.

d) La fórmula de la Seguridad Operacional

Definiendo las tres categorías que componen el Rav, se debe agregar y asociar la información de entrada en las categorías pertinentes para cada variable de entrada. Para esta ecuación Rav se requiere que a cada una de las categorías se les asigne un valor base para poder escalar los factores de seguridad dependiendo del alcance.

e) La fórmula de los controles

Ya habiendo asociado la información a las categorías pertinentes el siguiente paso es definir los Controles de Perdida que son los mecanismos de seguridad establecidos para proteger las operaciones y es dado por la suma de las 10 categorías de control.

f) La fórmula de las limitaciones

Como siguiente paso, se establecen las limitaciones de manera individual mediante la relación entre la suma de los resultados de las pruebas de seguridad operativa, los controles de perdida, y las posibles exposiciones o anomalías que no plantean problemas por si solas a no ser que se le sume una vulnerabilidad o debilidad.

g) La fórmula de la Seguridad Actual

Como parte final, se muestra la formula que utiliza los cálculos anteriormente hechos de tres maneras diferentes:

- Delta de Seguridad Real, la cual sirve para comparar soluciones y productos estimando el cambio (delta) que este realizaría en el alcance
- Protección Real, que puede ser usada para la cobertura optima de un ámbito donde 100 establece una relación optima entre controles, limitaciones y posibles espacios o vacíos que se encuentren.
- Seguridad Real, que mide el estado actual de las operaciones empresariales con los controles aplicados y las limitaciones descubiertas. En conclusión, el valor de seguridad que combina los valores de seguridad operacional, controles y limitaciones que logran mostrar el estado real de la seguridad.

VII. Análisis de Confianza

En el manual se sigue con un análisis de confianza, que es definida como una interacción a controlar y se diferencia del acceso, que es otra forma de interacción, en como la confianza se relaciona con otros objetivos dentro del alcance ya que la confianza es medida como las interacciones entre objetivos dentro del alcance.

a) Entendiendo la Confianza

Partiendo del hecho que la confianza es una decisión, la metodología establece la capacidad de cuantificar la confianza aplicando un proceso lógico aplicando dichos valores de confianza a procesos y objetos, así como a personas, lo que ayuda a los analistas a descartar o restarle valor a la información que proviene de fuentes no confiables o no autorizadas.

b) Fallas en la Confianza

Esta metodología define dos puntos erróneos importantes de confianza que son la composibilidad y la transitividad, dos propiedades usadas comúnmente para la toma de decisiones de confianza sobre lo desconocido.

Se define la composibilidad como cuando una persona hace una elección de confianza basada en la opinión que tenga una cierta cantidad de personas sobre el tema en cuestión.

También definen transitividad como la cadena de confianza, que es cuando una persona acepta la decisión de confianza de una persona para sí misma.

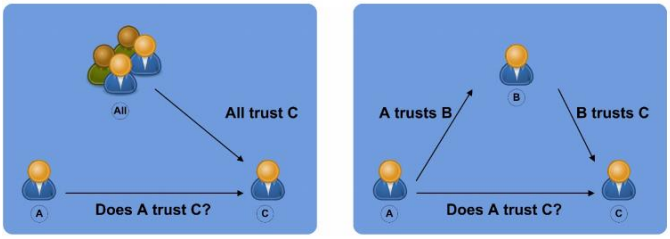

Fig. 5. Funcionamiento Confianza basado en primero composibilidad y segundo transitividad

c) Propiedades de la Confianza

Se establecen 10 propiedades de la confianza:

- Tamaño
- Simetría
- Visibilidad
- Subyugación
- Consistencia
- Integridad
- Compensaciones
- Valor
- Componentes
- Porosidad

d) Reglas de Confianza

Ya establecidas las propiedades de la confianza, es necesario convertirlas en reglas de confianza, lo que se logra formulando preguntas donde las respuestas sean números imparciales que lograran una comprensión mas sencilla con calificadores comunes como casi, a veces, siempre y nunca. Estas reglas de confianza deben ser creadas para un objetivo especifico y pueden crearse unas reglas por defecto específicamente para cada tema.

e) Aplicación de Reglas de Confianza en Pruebas de Seguridad

Las pruebas de seguridad logran verificar los niveles de confianza operativa existentes, pero se requieren las reglas de confianza para establecer si dichas pruebas debieran existir, por lo que una política de seguridad definirá lo que se define como confiable o no y que será permitido o no.

VIII. FLUJO DE TRABAJO

Para la metodología OSSTMM un flujo de trabajo empieza con una revisión del objetivo como son su cultura, reglas, normas, contratos, legislación y políticas que es lo que define el objetivo y termina con la comparación de resultados con las alertas, informes o registros de accesos, el primer paso es conocer los requisitos operativos y el último paso es la revisión de los registros lo que se simplifica para un análisis como: saber lo que se hace, hacerlo para luego verificar lo que se ha hecho.

Lo anterior la metodología lo separa en el formato:

1. Canal
2. Modulo
3. Tarea

Que es aplicado a los 5 canales, 17 módulos que son usados en todos los canales y difieren en distintas tareas. Cada modulo tiene una entrada y una salida, como entrada se usa la información de cada tarea realizada y como salida se define el resultado de las tareas completadas y la salida de un módulo puede servir o no como entrada para otro u otros módulos.

a) Flujo de la Metodología

La metodología no logra diferenciar entre pruebas activas y pasivas donde las pruebas activas requieren interacción con el objetivo y las pruebas pasivas son los registros y análisis de las emanaciones del objetivo. Además, cualquier evento externo que se incluya puede cambiar la naturaleza de las operaciones del objetivo y disminuir la calidad de una prueba sobre la seguridad operacional.

b) Módulos de Prueba

Para poder elegir el tipo de prueba apropiado es necesario entender como están diseñados los módulos. Por lo anterior se definen cuatro fases en esta metodología:

- Fase de Inducción
  Donde se empieza la auditoria con un entendimiento de los requisitos de auditoria, el alcance y las restricciones para la auditoria de un alcance.
- Fase de Interacción
  Donde se define el alcance, relacionado con las interacciones con los objetivos y con los activos.
- Fase de Investigación
  Donde se revelan los tipos de valor o devaluación de la información mal posicionada y mal administrada como activo.
- Fase de Intervención
  Donde se asegura que las interrupciones no afecten las respuestas de las pruebas ya que las pruebas se centran en los recursos que los objetivos requieren en el alcance.

c) Una Metodología

Al juntar todos los módulos se logra un conjunto establecido para conocer y trabajar conocido cono Una Metodología la cual es aplicable a todos los tipos de pruebas de seguridad ya sea que el objetivo sea un sistema, una ubicación, persona, proceso o la mezcla de estos ya que esta metodología asegurara pruebas mas completas, exhaustivas y eficientes posibles.

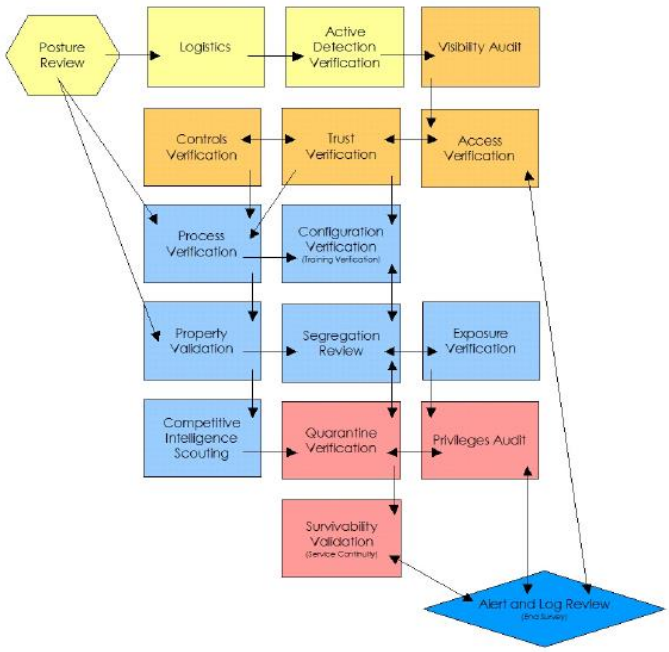

Fig. 6. Mapa de flujo de metodología OSSTMM

Después de esto, la metodología establece los tipos de pruebas en los canales Humano, Físico, Inalámbrico, de telecomunicaciones y de redes de datos.

La seguridad humana requiere la interacción con personas en los puestos de control de activos de información, también incluye la participación de personal principalmente operativo dentro del marco que se ha establecido como objetivo ya que el objetivo principal del cumplimiento de estas pruebas de seguridad es la prueba de conciencia de seguridad del personal y la medición de brechas según el estándar de seguridad requerido descrito en la política de la empresa, las regulaciones de la industria o la legislación regional.

Las pruebas de seguridad física empiezan con una clasificación de la seguridad material dentro del ámbito físico y su interacción con las barreras y controles, así como con el personal en las posiciones de control de los activos ya que el objetivo del cumplimiento de estas pruebas es la prueba de barreras físicas y lógicas y la medición de brechas con el estándar de seguridad requerido como se describe en la política de la empresa, las regulaciones de la industria o la legislación regional.

La seguridad inalámbrica se valida en pruebas que deniegan el acceso no autorizado a la información debido a la interceptación y análisis de radiaciones electromagnéticas ya que el objetivo del cumplimiento de estas pruebas es validar barreras físicas y lógicas y la medición de brechas según el estándar de seguridad requerido descrito en la política de la empresa, los reglamentos de la industria o la legislación regional.
Las pruebas seguridad de telecomunicaciones empiezan con una clasificación de la seguridad a nivel de seguridad electrónica dentro del objetivo estudiado ya que su principal funcionalidad con su cumplimiento es probar barreras lógicas y la medición de brechas con respecto a la norma de seguridad requerida, tal como se describe en la política de la empresa, los reglamentos de la industria o la legislación regional.
Para las pruebas de seguridad en redes de datos se requieren interacciones con las validaciones operativas de la red de comunicación de datos existentes utilizados para controlar el acceso a la información ya que el propósito de cumplir estas pruebas es la interacción del sistema y las pruebas de calidad operativa con mediciones de brechas según el estándar de seguridad requerido descrito en la política de la empresa, las regulaciones de la industria o la legislación regional.

Para todas estas pruebas se siguen los siguientes pasos:

- Revisión de la postura
- Logística
- Verificación de detección activa
- Auditoria de visibilidad
- Verificación de acceso
- Verificación de confianza
- Verificación de controles
- Proceso de verificación
- Verificación de la configuración
- Validación de propiedad
- Revisión de segregación
- Verificación de la exposición
- Inteligencia competitiva de exploración
- Verificación de cuarentena
- Auditoria de privilegios
- Validación de la supervivencia
- Revisión de alertas y registros

Llevando a cabo las pruebas anteriormente descritas, el manual establece los parámetros de cumplimiento como la alineación con un conjunto de políticas generales, donde el tipo de cumplimiento requerido depende de la región y del gobierno actual, los tipos de industria y negocios, y la legislación de respaldo. El cumplimiento es obligatorio; sin embargo, al igual que con cualquier otra amenaza, se debe realizar una evaluación de riesgo para invertir o no en cualquier tipo de cumplimiento y se reconocen 3 tipos de cumplimiento:
1. Legislativo. El cumplimiento de la legislación está de acuerdo con la región donde se puede hacer cumplir la legislación. La fuerza y el compromiso con la legislación provienen de argumentos legales previamente exitosos y de medidas de aplicación justas y bien establecidas. El incumplimiento de la legislación puede dar lugar a cargos penales. Algunos ejemplos son Sarbanes-Oxley, HIPAA y las diversas leyes de Protección de Datos y Privacidad.

2. Contractual. El cumplimiento de los requisitos contractuales está de acuerdo con la industria o dentro del grupo que requiere el contrato y puede tomar medidas para hacer cumplir el cumplimiento. El incumplimiento de los requisitos contractuales a menudo conlleva el despido del grupo, la pérdida de privilegios, la pérdida de reputación, los cargos civiles y, en algunos casos, cuando existe legislación para respaldar al organismo regulador, los cargos penales.
Un ejemplo es el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) promovido y requerido por VISA y MasterCard.

3. Basados en estándares. El cumplimiento de las normas se realiza de acuerdo con la empresa u organización donde el cumplimiento de las normas se aplica como política. El incumplimiento de las normas a menudo conlleva el despido de la organización, la pérdida de privilegios, la pérdida de reputación o la confianza de la marca, los cargos

civiles y, en algunos casos, cuando existe legislación para respaldar a los responsables políticos, los cargos penales. Ejemplos son los
OSSTMM, ISO 27001/5, e ITIL.

Por ultimo el manual establece lo que se obtiene al llevar a cabo la implementación de las métricas dadas y lo que se obtendrá al utilizar OSSTMM es realmente acerca de tener una comprensión profunda de la interconexión de las cosas. Las personas, los procesos, los sistemas y el software tienen algún tipo de relación. Esta interconexión requiere interacciones. Algunas interacciones son pasivas y otras no. Algunas interacciones son simbióticas, mientras que otras son parasitarias. Algunas interacciones están controladas por un lado de la relación, mientras que otras están controladas por ambos. Luego, algunos controles son defectuosos o superfluos, lo que es perjudicial para al menos un lado de la relación, si no ambos. Otros controles se equilibran perfectamente con las interacciones. Independientemente de lo que ocurra con la interconexión, sin embargo, las interacciones ocurren, sin embargo, si se controlan, son las operaciones las que hacen posible la supervivencia. Cuando se prueban las operaciones, se logra obtener una visión general de las relaciones existentes y se logra ver la interconexión de las operaciones en detalle.

IX. CONCLUSIONES

- El Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) en su tercera versión ofrece un marco de trabajo con los pasos necesarios para realizar pruebas de niveles de seguridad y dichas pruebas pueden ser parte de una auditoria.
- Esta metodología es supremamente útil al momento de querer realizar pruebas de penetración, ya que logran indicar superficies de ataque, vectores de confianza y resultados medibles para la presentación de resultados puntuales.
- El manual esta tan completo y estructurado que cuenta con un numero de pruebas incluidas y formatos de ejemplo para la presentación de resultados que ya son tan ampliamente usados que se convirtieron en un referente a nivel global para las pruebas de seguridad operativa.
- El manual se basa, a diferencia de lo que se pueda pensar, en el factor humano, ya que está presente en la mayoría de canales, procesos y servicios que presta una organización lo que ofrece un plus al momento de realizar pruebas de seguridad operativa.
- En algunos apartes esta metodología intenta probar que al lograr predecir que es lo que se necesita probar, como se tienen que realizar las pruebas y en que momento es necesario ejecutarlas se puede lograr una seguridad operativa completa o al 100% bajo la frase *“El hecho de que algo no pueda ser controlado directamente no significa que no se pueda controlar. Si controlas el entorno controlas todo lo que hay en él.”*.

REFERENCIAS

[1] http://www.isecom.org/home.html
[2] http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual
[3] https://colombiadigital.net/actualidad/noticias/item/10005-entrevistas-colombia-digital-seguridad-informatica-el-valor-de-la-informacion-y-el-rol-de-las-empresas.html