UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster en Seguridad Informática

Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad

Trabajo Fin de Máster

Presentado por: Fuertes Maestro, Antonio

Director: Martínez Herraiz, José

Ciudad: Madrid
Fecha: 05/03/2014

Agradecimientos

Este trabajo culmina un duro año de estudio, que he compatibilizado con el trabajo, la familia y la amistad, pero que ha sido muy satisfactorio en cuanto a los conocimientos y los resultados obtenidos. Por tanto, en este apartado quería agradecer a las personas que han hecho posible este esfuerzo a través de su apoyo y comprensión.

Agradecer a mis padres, que me han dado el cariño, la educación, el compromiso y la ética que me ayuda en cada momento a tomar decisiones, y a ser lo que soy.

Agradecer a mis hermanas que me han dado la compañía, entendimiento y atención, para crecer como persona.

Agradecer a mi hija Noelia, que es la mayor maravilla que me ha dado la vida, que tanto disfruto con ella y que tantos ratos le he robado a cambio de estos estudios.

Agradecer a Alicia, que me ha apoyado en cada momento con su cariño, inteligencia, comprensión y buenos consejos, y que me aguanta cada día, y a la que espero pedir matrimonio un día de estos.

Agradecer también a mis amigos que por falta de tiempo no he podido compartir todo el tiempo que me gustaría, y a los compañeros de trabajo y superiores que gracias a su buena actitud, han conseguido motivarme y hacer que me supere cada día.

Agradecer de corazón a Fernando Luengo y a sus compañeros de Provide HMC People, que me han dado la oportunidad de realizar las prácticas en su empresa, y que me han tratado como un compañero mas, lastima no haber podido colaborar más profundamente con ellos.

No quería terminar sin agradecer a los buenos docentes que han impartido el máster, y de los que he aprendido tanto, para iniciar una nueva actividad laboral que tanto me gusta. En concreto quería agradecer a mi tutor, José Martínez, que aunque no le he conocido personalmente, si he sentido la cercanía y apoyo desinteresado tan necesario a la hora de afrontar un trabajo fin de máster online, donde la cercanía es un bien escaso.

Resumen

El presente trabajo está orientado a las líneas de trabajo de la auditoria de la seguridad y del análisis de vulnerabilidades, enfocada de manera directa a la auditoria técnica de seguridad, actividad que engloba conocimientos de *hacking* ético y de test de intrusión.

El objetivo principal de este trabajo es ubicar, diseñar y desarrollar una nueva metodología de test de intrusión dentro de la auditoría técnica de seguridad. Para ello, se estudiaran las principales guías y metodologías estándar de facto, como son la OSSTMM, ISSAF y OWASP. Una vez desarrollada la nueva metodología, deberá ser validada dentro de un entorno real a través de pruebas sobre una infraestructura de red, sistemas y elementos Web.

La aportación fundamental de esta metodología es por tanto una visión resumida y práctica de los test de intrusión orientada hacia los auditores noveles.

Palabras claves: Auditoria Técnica de Seguridad, Test de Intrusión, OSSTMM, ISSAF, OWASP

Abstract

This work is aimed at the working lines of security audit and vulnerability analysis focused directly to technical security audit, which activity encompasses knowledge of ethical hacking and penetration testing.

The main objective of this work is to situate, design and develop a new methodology of testing intrusion into technical security audit. For it, will be studied the main guidelines and methodologies de facto standard, such as OSSTMM, ISSAF and OWASP. Once developed the new methodology should be validated in a real environment through tests on a network infrastructure, systems and Web elements.

The main contribution of this methodology is therefore a summarized and practical viewpoint, oriented toward novice auditors.

Keywords: Technical Security Audit, Penetration Test, OSSTMM, ISSAF, OWASP

Contenido

1. Introducción …….....8

1.1. Objetivos……..... 9

1.2. Estructura del trabajo……... 9

2. Estado del arte de las metodologías……... 10

2.1. Metodologías de evaluación de seguridad…….....10

2.2. OSSTMM……..... 13

2.3. ISSAF……..……..……..... 22

2.4. OWASP……...……..…..... 29

2.5. Ubicación del test de intrusión dentro de la auditoria de seguridad…….....44

3. Desarrollo de nueva metodología de test de intrusión…..…….....52

3.1. Características generales de la metodología 52

3.2. Fases de la nueva metodología del test de intrusión 53

4. Validación de la metodología…….....78

4.1. Arquitectura y requisitos mínimos del prototipo de validación 78

5. Conclusiones y líneas futuras……..…….....79

Referencias bibliográficas……..…….....85

Relación de acrónimos

BSSID: Basic Service Set Identifier
CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart
COBIT: Control Objectives for Information and Related Technology
CSRF: Cross Site Request Forgery
DHCP: Dynamic Host Configuration Protocol
DNS: Domain Name System
DOM: Document Object Model
FTP: File Transfer Protocol
HTTP: Hypertext Transfer Protocol
ICMP: Internet Control Message Protocol
IDS: Intrusion Detection System
IPS: Intrusion Prevention System
IMAP: Internet Message Access Protocol
ITIL: Information Technology Infrastructure Library
LDAP: Lightweight Directory Access Protocol
LOPD: Ley Orgánica de Protección de Datos
LSSICE: Ley de Servicios de la Sociedad de Información y Comercio Electrónico
NetBIOS: Network Basic Input / Output System
NIST: National Institute of Standards and Technology
OML: Open Methodology License
RAV: Risk Assesment Values
SDLC Software Development Life Cycle
SMB: Server Message Block
SMTP: Simple Mail Transfer Protocol
SNMP: Simple Network Management Protocol
SQL: Structured Query Language
SSID: Service Set IDentifier
SSL: Secure Sockets Layer
URI: Uniform Resource Identifier
VPN: Virtual Private Network
XML: eXtensible Markup Language
XSS: Cross-site scripting
WEP: Wired Equivalent Privacy
WIFI: Wireless Fidelity
WPA: Wi-Fi Protected Access

Índice de figuras

2.1. Fases propuestas por la metodología OSSTMM 16
2.2. Orden de ejecución y relaciones de dependencia de OSSTMM 19
2.3. Ámbitos de aplicación de la metodología OSSTMM 20
2.4. Fases propuestas por la metodología ISSAF 24
2.5. Actividades realizadas en el ámbito de la auditoria de la seguridad 44
2.6. Conjunto de actividades que componen la auditoria de seguridad 47
2.7. Modelo de mejores prácticas propuesto por McGraw 48
2.8. Evolución del coste de corrección de fallos en el ciclo de vida de una aplicación 49
2.9. Ubicación de los tipos de pruebas de test de intrusión 51
3.1. Fases de la metodología propuesta en este trabajo 55
3.2. Tipos y ámbitos acordados sobre el alcance de las pruebas 60
3.3. Etapas que componen la recopilación de Información 62
3.4. Etapas que componen la recopilación de información pública 63
3.5. Etapas que componen la actividad *Fingerprinting* 67
3.6. Etapas que componen el análisis de vulnerabilidades 70
3.7. Etapas que componen la explotación de vulnerabilidades e intrusión 74
3.8. Procedimiento completo de la nueva metodología de test de intrusión 78
4.1. Esquema propuesto como prototipo de validación 80

Índice de tablas

2.1. Descripción de ámbitos cubiertos por OSSTMM 21
2.2. Tipos de pruebas en los test de intrusión 50

Capítulo 1: Introducción

A día de hoy cualquier organización independientemente del tamaño y del sector de su actividad, utilizan de manera habitual las TIC para realizar su proceso de negocio. Los sistemas de información (SI) por tanto son una parte fundamental para el desarrollo de la actividad. Es necesario proteger estos sistemas debidamente para asegurar la confidencialidad de la información, mantener la integridad de la información, garantizar la disponibilidad de la información y salvaguardar la propiedad de la información. Por lo tanto, la seguridad de los SI es uno de los aspectos que más preocupan actualmente a todas las organizaciones. En contraposición a esto, surge la figura del coste asociado para asegurar un sistema. En la mayoría de las ocasiones esta inversión se reduce drásticamente, de manera que no se puede cubrir adecuadamente las medidas de seguridad que necesitan las organizaciones.

La seguridad de los SI dentro de una organización varía a lo largo del tiempo y depende directamente de los procesos de negocio. La adquisición de un alto nivel de protección en el momento actual, no implica la obtención de una seguridad total de manera ilimitada. Los sistemas e infraestructuras que soportan las actividades de la organización varían, adaptándose al modelo de negocio o de actividad de la organización. De forma similar, la seguridad de los procesos llevados a cabo también lo hace. Por lo tanto, la seguridad es un proceso continuo, vivo y adaptativo a los cambios realizados en la organización.

Para llevar a cabo el proceso continuo de la seguridad de los SI es necesaria la creación de políticas de seguridad que planifiquen de forma eficaz y eficiente los diferentes procedimientos y controles, y la implantación de los estándares. Estas políticas serán gestionadas desde el gobierno de las TIC, para ser alineadas con los objetivos estratégicos de la organización. Esto conlleva la necesidad de realizar las auditorias informáticas como pieza fundamental en la verificación del cumplimiento de las políticas.

Dentro de la auditoria informática se encuentra la auditoria de seguridad de los SI, que es donde se ubica este trabajo fin de máster. Los test de intrusión se sitúan dentro de la auditoria técnica de seguridad.

Un test de intrusión puede definirse como la evaluación de la seguridad de los SI presentes en la organización (infraestructura de red, sistemas, servidores Web, etc.) mediante la simulación de un ataque, usando para ello diferentes técnicas y herramientas de software. La realización de las auditorias técnicas de manera periódica dentro de la política de seguridad de las organizaciones, permitirá controlar el cumplimiento de las políticas, y evaluar y mitigar los riesgos en entornos con constantes cambios.

1.1 Objetivos

La principal aportación de este trabajo es la elaboración de una nueva metodología a la hora de realizar un test de intrusión dentro de una auditoria de seguridad informática. Esta nueva metodología está fundamentada en el estudio de las metodologías más utilizadas actualmente. También es importante ubicar las pruebas de intrusión dentro de la auditoria de seguridad, aclarando el ámbito, alcance y tipología de estas pruebas.

En cuanto a los objetivos específicos de este trabajo, pueden enumerarse los siguientes:

- Obtención de una visión actual y global de las metodologías de evaluación de seguridad. Estas metodologías se ubican dentro de las actividades de la auditoria de la seguridad informática.
- Adquisición de los conocimientos de las principales metodologías de evaluación de seguridad, como son OSSTMM, ISSAF y OWASP. Se extraerán los aspectos más significativos y los procedimientos principales de las fases de pruebas. Esto servirá para valorar y adquirir unos conocimientos previos enfocados a la elaboración de la nueva metodología.
- Diseño y desarrollo de una nueva metodología de test de intrusión basada en el estudio de las metodologías anteriores. Esta metodología debe aportar un punto de vista eminentemente práctico y resumido de los test de intrusión. Debe servir como guía rápida de buenas técnicas y métodos, para la orientación y concreción de los test de intrusión por parte de auditores noveles.
- Propuesta de los requisitos mínimos de un prototipo que simule un entorno de pruebas real permitiese la validación de la metodología.
- Obtención de las correspondientes conclusiones y exposición de las posibles líneas futuras que pueden realizarse sobre la misma.

1.2 Estructura del trabajo

La estructura del presente trabajo es la siguiente:

En el **Capítulo 2** se expondrá la situación actual en cuanto al estado del arte de las metodologías que cubren las pruebas de intrusión. Se estudia y extrae las características más importantes de las metodologías: OSSTMM, ISSAF, OWASP, en concreto las distintas fases, técnicas y ámbitos que componen las pruebas de intrusión. Estas pruebas ofrecen

diferentes puntos de vista y diferentes aspectos que proporcionan las bases para el desarrollo de la nueva metodología. Además, se expone la ubicación de las pruebas de intrusión dentro del ámbito de la seguridad informática para poder acotar el alcance de la nueva metodología.

En el **Capítulo 3** se propone una nueva metodología de test de intrusión, partiendo de los conocimientos adquiridos en el estudio de las metodologías de referencia del capítulo 2. Para ello se diseña y se desarrolla el procedimiento de pruebas de intrusión que se aporta en este trabajo.

En el **Capítulo 4** se propondrá un pequeño prototipo con los requisitos mínimos a nivel de arquitectura y de tecnología, que permitiría validar la metodología propuesta en el capítulo 3. El prototipo debería permitir pruebas sobre un sistema real o virtual, compuesto por una infraestructura de red, sistemas servidores, estaciones de trabajo y aplicaciones y servicios habituales en una organización, para de esta forma simular un escenario real.

En el **Capítulo 5** se concluye el trabajo presentando las conclusiones extraídas a lo largo de la elaboración de la metodología, y se detallaran posibles líneas futuras que pueden realizarse sobre la nueva metodología.

Por último, se recoge las **Referencias bibliográficas** necesarias para alcanzar los conocimientos sobre los temas aquí tratados, que han sido utilizados y que se han referenciado a lo largo del presente trabajo.

Capitulo 2: Estado del arte de las metodologías

Las metodologías para la evaluación de seguridad dentro de una auditoria de seguridad informática ayudan a los especialistas del sector a evaluar de una forma metódica y repetible los test de intrusión. De esta forma las pruebas pueden ser realizadas por diferentes auditores y un método común, obteniendo resultados al menos equiparables.

En este capítulo se van a exponer las metodologías de evaluación de seguridad más utilizadas en este sector. Se centrara el estudio en los aspectos más destacados de las fases de test de intrusión de las metodologías, área en la que se desarrolla este trabajo.

Cabe reseñar que a fecha de redacción de este trabajo, no hay ninguna metodología que haya sido desarrollada como norma ISO, de forma que aun no están estandarizados los test de intrusión. Quizá un factor importante en la realización de los test de intrusión, es que no es una ciencia exacta, ya que depende de muchos factores, tales como la diversidad de objetivos y entornos donde se desarrolla esta actividad. Sin embargo, es necesaria la elección de una metodología de evaluación, que normalmente se adaptara por parte del auditor en función del entorno real de trabajo.

2.1 Metodologías de evaluación de seguridad

La decisión a la hora de elegir una de las metodologías explicadas en este capítulo es siempre difícil, y dependerá del ámbito, pericia y objetivo de la evaluación. Cada una de ellas aporta diferentes aspectos que serán ventajosas en determinados casos, por lo que no es una decisión simple, y deber ser estudiada y adaptada para cada caso. Es importante remarcar que no hay una metodología mejor o peor que otra, sino que son guías que aportan diferentes puntos de vista de cara a la evaluación de seguridad y que sirven como manual de referencia a la hora de realizar esta actividad.

En esta introducción se enumeraran las metodologías que van a ser explicadas a lo largo del capítulo. Se explicaran los aspectos y características más importantes de cada una de ellas, que sirvan como base para el diseño y creación de una nueva. Un punto destacable que tienen en común estas metodologías es el tipo de licencia con el que se han creado, que permite su utilización de forma libre.

Las metodologías que se van a explicar en este capítulo son:

- OSSTMM [1].
- ISSAF [2].
- OWASP [3].

Los aspectos más significativos orientados a los test de intrusión de cada metodología son los siguientes:

Ámbito y alcance

El ámbito de aplicación delimitara las pruebas a realizar. Dependerá del tipo de organización, marco de la actividad general, profesionales que la implantan y áreas donde se desarrollen. Este aspecto acota y clasifica cada una de las metodologías en cuanto al alcance y posibilidades que ofrecen.

Meticulosidad

Este aspecto tiene en cuenta la minuciosidad y exactitud que aporta cada metodología. El nivel de profundidad que utilice la metodología en el desarrollo de las pruebas, mostrara el nivel de detalle con el que extrae información de los sistemas a testear. La mayoría de los problemas de seguridad son debidos la suma de pequeñas vulnerabilidades, que individualmente no suponen un riesgo alto, pero su acumulación deriva en un problema grave. Es por tanto un aspecto muy valioso dentro de las pruebas de intrusión.

Usabilidad y uso

La usabilidad de estas metodologías podría definirse como la facilidad a la hora de utilizar las metodologías para alcanzar los objetivos marcados de una forma efectiva, eficiente y con una satisfacción subjetiva. En cuanto al uso o utilización de las mismas en los entornos de auditorías de seguridad, se investigara la popularidad de las metodologías de forma genérica.

Métricas

La obtención de una medición de forma objetiva y repetible es una característica importante en las metodologías. Permite la clasificación del las vulnerabilidades encontradas, y por ende el riesgo y el impacto que tendrían su explotación. Cabe reseñar que no todas las metodologías cubre este aspecto, y que la nueva metodología no lo cubrirá, dado que se sale de los objetivos básicos que propone este trabajo.

Fases de la metodología

Cada metodología aporta diferentes puntos de vista a la hora de realizar la planificación y desarrollo de las pruebas. En este punto se expondrán las fases que utiliza cada metodología para la obtención de los objetivos. Este aspecto es primordial en el desarrollo del trabajo, dado que servirá de base de conocimiento en el diseño de la nueva metodología, extrayendo las mejores prácticas y técnicas aquí expuestas.

Ventajas

Evidentemente cada metodología ofrece una serie de ventajas que es necesario reseñar. Esto facilita la obtención de una visión global de lo que aporta cada metodología a las evaluaciones de seguridad. Este punto muestra las ventajas que tiene cada metodología de forma genérica, ayudando a la obtención de las mejores prácticas en el desarrollo de la nueva metodología. Además permitirá evaluar la utilización de las mismas en el caso de tener que elegir una de ellas en un proyecto real.

Limitaciones

Como se indicaba en la introducción de este capítulo, no hay una metodología mejor o peor que otra. Al igual que se destacan las ventajas de cada metodología es necesario exponer sus limitaciones. Este punto por tanto aportara una visión crítica de cada metodología, orientando en la elección de la metodología en función del tipo de proyecto a realizar. Este aspecto también debe ser reflejado en la nueva metodología, para obtener así un punto crítico en las conclusiones del trabajo.

2.2 OSSTMM

OSSTMM (*Open Source Security Testing Methodology Manual*) es una metodología de evaluación de seguridad y de métrica, definida por la asociación ISECOM. ISECOM (*Institute for Security and Open Methodology*) es una organización internacional sin ánimo de lucro. Fue creada en el año 2000, para el desarrollo de metodologías en áreas tales como la verificación de la seguridad, verificación del software, y programación segura.

Su primera versión apareció en 2001, fecha hasta la cual no se había publicado aun un documento formal que verificase sistemas de forma abierta y estandarizada. Actualmente, la última versión de la metodología OSSTMM es la versión 3 [1], que fue publicada en 2007. Es imprescindible señalar que esta valoración no es compatible con versiones anteriores, por lo que debe ser considerada como una versión completamente nueva.

Ámbito y alcance

El ámbito de aplicación de OSSTMM está orientado hacia cualquier tipo organización, independientemente del tamaño, tecnología o medidas de seguridad. La aplicabilidad de la metodología engloba cualquier entorno donde se requieran aspectos de seguridad, ya sea la seguridad física, la de los procesos, la de las comunicaciones y la del espectro electromagnético.

Es conveniente destacar que OSSTMM no solo alcanza el ámbito técnico y tradicional de la seguridad, sino que introduce aspectos tales como:

- Estandarización a nivel de acreditación, presentando cinco certificaciones.
- Comercialización de los servicios ejecutados por los profesionales.
- Formalización de los resultados según las normas éticas y legales a cumplir.
- Planificación mostrando la trazabilidad y tiempos requeridos en cada una de las fases.

Meticulosidad

Esta metodología es muy exhaustiva y minuciosa en la realización del test de intrusión. Se basa en la búsqueda y examen de forma detallada de los diferentes sistemas para descubrir fallos de seguridad. Se hace hincapié en los pequeños detalles, que por sí solo no representan mucho riesgo, pero cuya acumulación pueden suponer fallos de seguridad graves.

Usabilidad y uso

La usabilidad que presenta esta metodología se puede considerar de nivel medio. Requiere un alto entrenamiento y pericia, que son habitualmente cubiertas con las certificaciones que propone la metodología.

OSSTMM es uno de los estándares de facto más utilizados por los profesionales dedicados a la revisión de la seguridad de sistemas, proporcionando una referencia imprescindible dentro de este sector. La metodología está bajo licencia *Creative Commons* y OML (*Open Methodology License*), que permite su libre utilización, revisión pública y el empleo de herramientas de código abierto.

Métricas

Esta metodología aporta mediciones objetivas que son necesarias para la valoración de riesgos desde un punto de vista práctico. Esto es muy demandado para la justificación de resultados y más palpable que los análisis de riesgos mas teóricos. Por tanto, se basa en mediciones técnicas realizadas durante las pruebas, que son verificables y concluyentes, y que indican un factor de riesgo en el sistema comparable a posteriori.

Utiliza el concepto de valores de evaluación de riesgos o RAV (*Risk Assesment Values*). RAV son definidos en cada uno de los módulos y su objetivo primordial es la medición de la degradación de la seguridad respecto al eje de tiempo. De esta forma se obtiene una valoración más longeva que la “instantánea” de seguridad tomada sobre el sistema en el momento de su ejecución. RAV utiliza factores de ajuste tales como seguridad operacional,

limitaciones y controles de pérdidas para la obtención de un resultado final en forma porcentual.

Fases de la metodología

OSSTMM presenta una metodología de prueba de intrusión dividida en cuatro fases. Cada una de estas fases aporta una diferente profundidad a la auditoria de seguridad, por lo que no hay ninguna fase más o menos importante dentro de esta metodología. Estas fases se muestran de forma de esquemática en la figura 2.1. Cada fase está compuesta a su vez de diferentes módulos. Las cuatro fases que componen las pruebas de intrusión son los siguientes:

- Fase de preparación.
- Fase de interacción.
- Fase de investigación.
- Fase de intervención.

Figura 2.1. Fases propuestas por la metodología OSSTMM

A continuación se expondrán las cuatro fases de las pruebas de intrusión que proponen la metodología OSSTMM, que se realizaran en 17 módulos:

A. Fase de preparación (*Induction Phase*)

Esta fase es donde comienza la auditoria, para ello es necesario comprender los requisitos, el alcance y las restricciones de este alcance. Frecuentemente, el tipo de prueba a realizar (caja blanca, caja negra, etc.) se determinara después de esta fase.

A1. Revisión de la situación (*Posture Review*)

En este estudio inicial se revisan la cultura, reglas, normas, reglamentos, legislación y las políticas aplicables al objetivo. Este módulo permite conocer el alcance y que pruebas deben ser realizadas. Se requerirá si la fase C es realizada adecuadamente.

A2. Logística (*Logistics*)

Se recogen las medidas de las restricciones de interacción tales como la distancia, velocidad y facilidad, determinando los márgenes de exactitud dentro de los resultados. Este módulo permite conocer las limitaciones de la propia auditoria, reducir el error y mejorar la eficiencia.

A3. Verificación de la detección activa (*Active Detection Verification*)

Se verificarán las actividades prácticas y la amplitud de las mismas, a la hora de detectar la interacción, la respuesta y la previsibilidad de la respuesta. Este módulo permite conocer las restricciones impuestas sobre los test interactivos. Esto es necesario para realizar adecuadamente las fases B y D.

B. Fase de interacción (*Interaction Phase*)

Esta fase es el núcleo de las pruebas de seguridad, por lo que es necesario conocer el alcance de las interacciones de los objetivos sobre los activos. Esta fase definirá el alcance de las pruebas.

B4. Auditoria de la visibilidad (*Visibility Audit*)

Se determinarán los objetivos que serán testeados dentro del alcance. La visibilidad se considera como la presencia en el sistema, que permite conocer que objetivos existen y cómo interactúan dentro del alcance. Un objetivo muerto o desaparecido es un objetivo sin respuesta, sin embargo los objetivos sin respuesta no son necesariamente objetivos desaparecidos.

B5. Verificación de accesos (*Access Verification*)

Se verificarán los puntos de acceso interactivos a través de las medidas de la amplitud y de la profundidad dentro de los objetivos y la autenticación requerida. El punto de acceso es el punto principal de cualquier interacción. Por lo tanto, verificar un punto de acceso existente es una parte determinante de este propósito. La verificación completa requiera el conocimiento completo del punto de acceso.

B6. Verificación de confianza (*Trust Verification*)

Se determinarán las relaciones de confianza desde los objetivos, y entre ellos. Una relación de confianza existe siempre que los objetivos acepten interacciones entre ellos dentro del alcance. A menudo, la confianza para los nuevos procesos es muy limitada

respecto a procesos más antiguos que tienen una evolución aparentemente caótica de cara al exterior. Conocer las relaciones de confianza entre los objetivos mostrara la edad o el valor de interacción.

B7. Verificación de control (*Control Verification*)

Se verificarán los procesos basados en la pérdida de control a través de la medición del uso y eficacia. Estos procesos son: no repudio, confidencialidad, privacidad e integridad. La mayoría de los procesos son definidos en respuesta a una interacción necesaria, de forma que algún proceso permanece mucho tiempo después de que la interacción se detenga o haya cambiado. Conocer que procesos de control están en su lugar correcto, es un tipo de arqueología de la seguridad.

C. Fase de investigación (*Inquest Phase*)

Esta fase ocupa gran parte de la auditoria de seguridad, ya que se trata de la información que el analista descubre. En esta fase, los diferentes tipos de activos de información que están mal situados o mal administrados, son sacados a la luz.

C8. Verificación de los procesos (*Process Verification*)

Se determinará la existencia y eficacia del registro, el mantenimiento de los niveles de seguridad reales, las diligencias definidas en la revisión de la situación (A1) y los controles de indemnización. La mayoría de los procesos tendrán un conjunto de reglas definidas, por lo que es necesario conocerlas.

C9. Verificación de la configuración / Verificación de capacitación *(Configuration Verification / Training Verification)*

Este modulo explorará las condiciones por defecto bajo las cuales los objetivos operan regularmente para comprender el propósito, justificación de negocio y el razonamiento de los objetivos. Se determinarán problemas subyacentes fuera del contexto de la aplicación de pruebas de estrés de seguridad. Además muchas de las regulaciones requieren información sobre como algo es planeado para trabajar, y esto no siempre es evidente en la ejecución de ese trabajo.

C10. Validación de la propiedad (*Property Validation*)

Se validará el uso de propiedad intelectual o aplicaciones ilegales o sin licencia dentro del objetivo, a través de la medición de la amplitud y la profundidad. Es necesario conocer el estatus de los derechos de propiedad.

C11. Revisión de la segregación (*Segregation Review*)

Se determinarán los niveles de información de la identificación personal definidos por en revisión de la situación (A1). Es necesario conocer qué derechos de privacidad aplicar y

en qué medida la información de la identificación personal descubierta puede ser clasificada**.**

C12. Verificación de la exposición (*Exposure Verification*)

Se verificará la visibilidad de los objetivos o activos dentro del canal seleccionado del alcance. Es necesario el descubrimiento de la información expuesta sobre los objetivos y activos desde fuentes públicas, incluyendo la de los objetivos en sí mismos.

C13. Exploración de inteligencia competitiva (*Competitive Intelligence Scouting*)

Se buscará la información disponible, directa o indirectamente, que podría perjudicar o afectar negativamente al propietario de los objetivos a través del exterior. Podría ocurrir que se obtuviese información de más valor de los procesos y objetivos que de los activos que son protegidos. Por lo tanto, descubrir información por sí mismo o en conjunto puede influir en las decisiones que son competencia del negocio.

D. Fase de intervención (*Intervention Phase*)

Esta fase de pruebas está enfocada a los recursos que los objetivos requieren en el alcance. Esos recursos pueden ser permutados, cambiados, sobrecargados o muertos por inanición, a causa de la intrusión o interrupción. Esta es la fase final del test de seguridad, asegurando que las interrupciones no afectan a las respuestas de las pruebas menos invasivas, dado que la información obtenida aquí no puede ser conocida hasta que las otras fases se han llevado a cabo.

El modulo final D.17 de alerta y revisión de registros, es necesario para verificar pruebas prioritarias que no suministran un retorno interactivo al analista. La mayoría de pruebas de seguridad que aun podrían necesitar la ejecución y revisión final desde la perspectiva de los objetivos y activos para aclarar cualquier anomalía.

D14. Verificación de la cuarentena (*Quarantine Verification)*

Se determinará y medirá el uso eficaz de la cuarentena para todos los accesos hacia y dentro del objetivo. Es necesario determinar la eficacia de la autenticación y controles de sometimiento en términos de cuarentena de listas blancas y listas negras.

D15. Auditoria de los privilegios (*Privileges Audit)*

Se realizará el esquema del sistema en cuanto a privilegios y se medida el impacto del mal uso de los controles de sometimiento, credenciales y privilegios o escalado no autorizado de privilegios. Es necesario determinar la eficacia de la autorización sobre la autenticación, indemnización y controles de sometimiento en términos de profundidad y de roles.

D16. Validación de supervivencia / Continuidad del servicio (*Survivability Validation / Service Continuity)*

Se determinará y medirá la resiliencia del objetivo ante cambios excesivos y adversos, donde la continuidad y controles de capacidad de recuperación podrían ser impactados. Es necesario determinar la eficacia en cuanto a la continuidad y control de la capacidad de recuperación, a través de la evaluación de la denegación de servicios y de la denegación de la interactividad.

D17 Revisión de alertas y de reportes/ Evaluación final (*Alert and Log Review / End Survey)*

Se realizará la revisión de las actividades de auditoría ejecutadas con la verdadera profundidad de estas, como son la información registrada a través del objetivo o desde una tercera parte en el control de alarmas. Es necesario conocer que partes de la auditoria dejaron una pista utilizable y confiable.

Una vez explicadas cada una de las fases y los módulos que componen estas fases de la metodología, se muestra en la figura 2.2, el orden de ejecución y las relaciones de dependencia entre cada uno de los 17 módulos que componen la metodología.

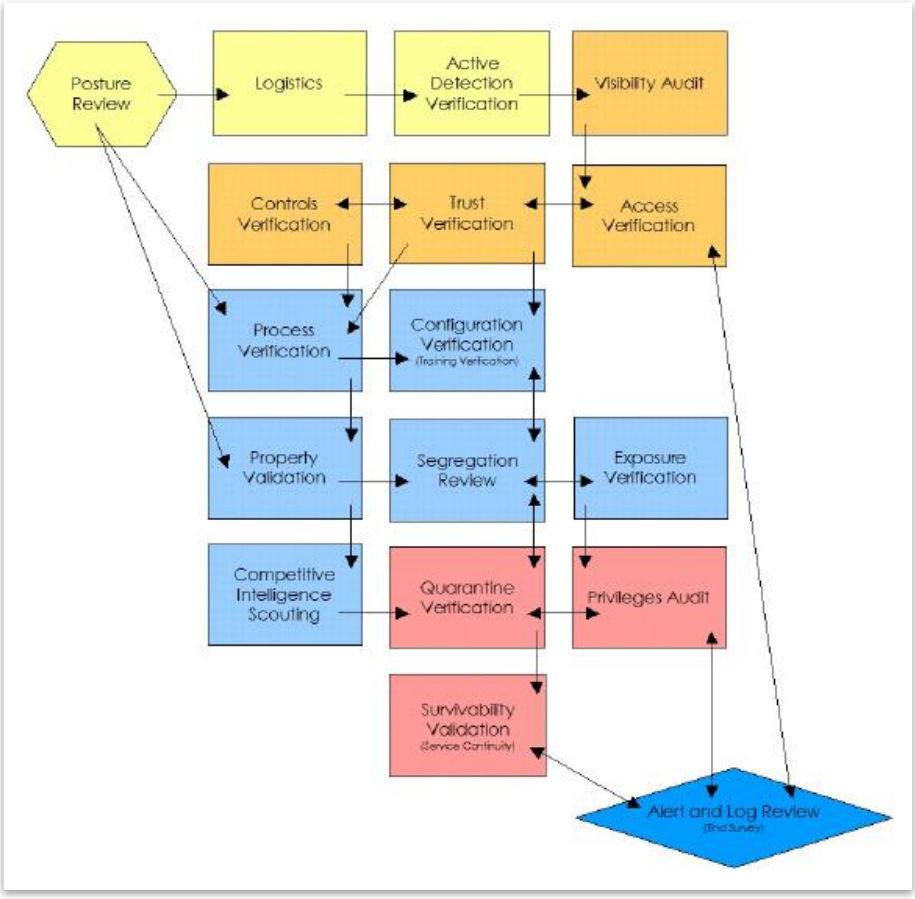

Figura 2.2. Orden de ejecución y relaciones de dependencia de OSSTMM

La metodología de prueba de intrusión debe aplicarse a los diferentes ámbitos que permitan la consecución de los objetivos dentro del alcance pactado. Estos ámbitos permiten la realización exhaustiva de pruebas. Se dividen en tres canales distintos, como son la seguridad de comunicaciones (COMSEC), la seguridad física y seguridad espectral. A su vez estos canales se subdividen en cinco secciones diferentes que utilizaran de forma minuciosa la metodología explicada anteriormente, pero concretando los detalles sobre el ámbito ejecutado. De esta manera se extraerá la información más significativa de cada una de las pruebas realizadas.

El ámbito de aplicación de las pruebas de intrusión se muestra de manera muy grafica en la figura 2.3 [4]. En la misma se observa cómo se cubre gran parte del ámbito de la seguridad de la información que deberá ser acotado en el alcance de las pruebas.

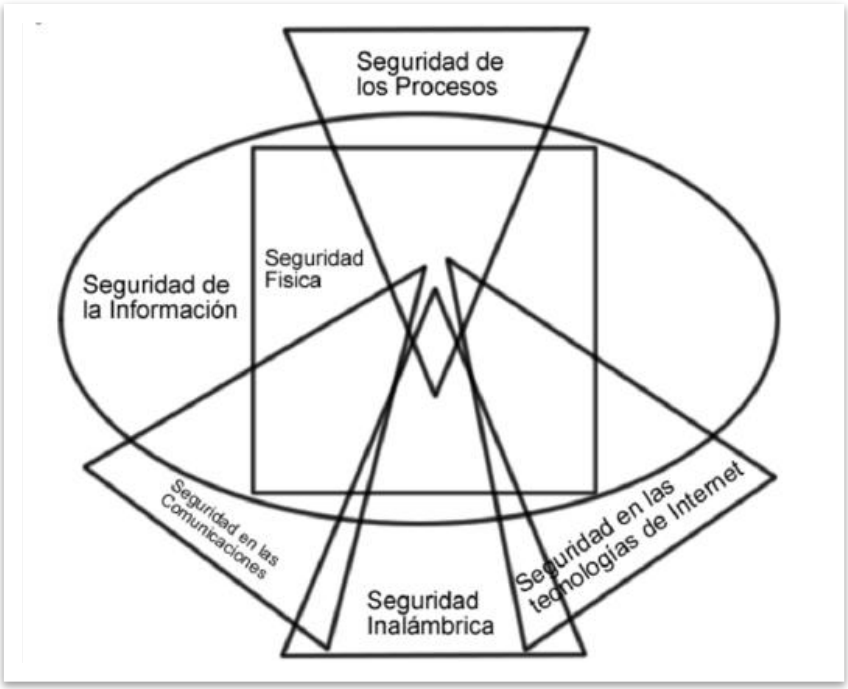

Figura 2.3. Ámbitos de aplicación de la metodología OSSTMM

En la tabla 2.1 se realiza una descripción genérica de los canales, y la subdivisión en secciones que cubren los aspectos más importantes de la seguridad de la información, tal y como se indicaba en la figura 2.3.

Canal	Sección	Descripción
Seguridad en el entorno físico PHYSEC	Humano	Engloba el elemento humano de comunicación que comprometa la organización, Esta interacción puede ser tanto física como psicológica
	Físico	Consiste en las pruebas de seguridad físicas, definiendo físico como elementos tangibles de la organización.
Seguridad en el espectro electromagnético SPECSEC	Comunicación Inalámbrica	ELSEC (comunicaciones electrónicas) SIGSEC (Señales) EMSEC (Emanaciones no encadenadas por cable)
Seguridad de las comunicaciones COMSEC	Redes de datos	Consta de todos los sistemas y redes de datos cableadas que interactúan en la organización.
	Telecomunicaciones	Engloban todas las comunicaciones digitales o analógicas empleadas sobre las redes para completar las comunicaciones.

Tabla 2.1. Descripción de ámbitos cubiertos por OSSTMM

Ventajas

Las ventajas que presenta esta metodología pueden resumirse en los diferentes puntos:

- Aporta escalabilidad, ya que se trata de una metodología abierta, pública y revisable. OSSTMM es una de las metodologías más actualizadas de las estudiadas.

- Cumple las leyes establecidas vigentes (en España tales como LOPD Ley Orgánica 15/1999, LSSICE 31/2002, la Firma Electrónica RD 14/1999 y el Reglamento de desarrollo de la LOPD 1720/2007). También cumple y complementa los estándares internacionales ISO de seguridad de la información ISO 27001 y las guías de mejores prácticas como las establecidas en el NIST e ITIL.

- Permite medir la evolución de la seguridad a lo largo del tiempo, obteniendo una valoración cuantificable de los resultados de las pruebas y la calidad del servicio prestado. Estas medidas además se basan en las pruebas realizadas y los resultados obtenidos, y no en un estudio teórico del riego.

- Metodología aceptada mundialmente como referencia estándar en la realización de pruebas de intrusión sin importar el tamaño de la organización, la tecnología o las defensas utilizadas.
- Análisis secuencial desarrollado de forma muy ordenada, exhaustiva y con calidad profesional permitiendo la ejecución de las tareas de forma sistemática.
- La metodología es presentada desde un punto de vista de alto nivel, indicando las tareas a realizar pero de manera independiente a la tecnología. Esto aporta mayor longevidad en la metodología, dotándola de flexibilidad.

Limitaciones

Las limitaciones que presenta esta metodología pueden resumirse en los diferentes puntos:

- OSSTMM 3, no es compatible con la versión 2, de forma que es necesaria la lectura e interpretación completa, como si de una nueva metodología se tratase.
- Dado que no recomienda herramientas, es necesario que el auditor complemente el trabajo con un conjunto de aplicaciones en las que tenga experiencia.
- Se basa mucho en la creatividad y experiencia del auditor, por lo que no es una metodología sencilla de utilizar para auditores noveles.
- Es una metodología muy intrusiva, por lo que es necesario cerrar adecuadamente el alcance de la misma en la relación contractual con el cliente.
- La complementación de la metodología OSSTMM con otras metodologías puede ser complicada, ya que existen partes donde armonizarlas puedan ralentizar ese proceso. Esto se justifica dado que OSSTMM no permite la separación entre la recolección de datos activos y la verificación a través del efecto de la alteración. Tampoco diferencia entre pruebas activas y pasivas.

2.3 ISSAF

ISSAF (*Information Systems Security Assessment Framework*) es una metodología estructurada de análisis de seguridad, diseñada para la evaluación de los elementos principales de los sistemas informáticos y sus comunicaciones. Es un proyecto de OISSG (*Open Information System Security Group*) presentado formalmente a principios del año 2005 y que no ha sido actualizada desde el año 2006, con la versión 0.2.1. [2]. La licencia es del tipo GNU GPL por lo que puede ser utilizada de manera libre.

Ámbito y alcance

El ámbito de aplicación de ISSAF es muy amplio, ya que cubre el análisis de seguridad en casi todos los dominios de cualquier organización, independientemente de su tamaño. La aplicación de esta metodología permite el análisis de sistemas tales como la infraestructura de red, sistemas operativos, aplicaciones y sistemas de gestión de bases de datos. La metodología se organiza a través del los "Criterios de Evaluación" donde se describen aspectos tales como los objetivos, pre-requisitos, evaluación, contramedidas recomendadas y referencias a documentación externa.

Otro factor importante que aporta es el cumplimiento de las normas de buenas prácticas y los requisitos reglamentarios. Al igual que otras metodologías presenta cinco certificaciones, una de ellas dedicada al test de intrusión: *Penetration Testing Expert* (I-PTE). Además ISSAF puede utilizarse como referencia para nuevas implementaciones relacionadas con la seguridad de la información.

Meticulosidad

ISSAF es una metodología muy detallada, quizá en exceso. Los criterios de evaluación abarcan diversos dominios, yendo desde los muy generales hasta muy específicos.

Cada uno de los procedimientos los explica en profundidad, asociando cada actividad incluso a aplicaciones *Open Source*. Esta especificación tan exhaustiva a diferencia de metodologías mas generalistas, supone que este Framework debe ser actualizado de forma constante, dado que las técnicas de evaluación de productos o tecnologías pueden quedarse obsoletas en poco tiempo.

Usabilidad y uso

Presenta una usabilidad muy alta, pudiéndose ejecutar con unos conocimientos medios. La fase de test de intrusión cubre todas las etapas necesarias, y aportan mucho nivel de detalle. Por lo tanto es una metodología fácil de utilizar y muy útil para auditores noveles.

En cuanto al uso de la misma, ISSAF es una metodología muy utilizada en Norteamérica, ya que respeta los modelos marcados por el NIST (*National Institute of Standards and Technology*) cuestión muy valorada en dicho entorno. Además la metodología esta bajo la licencia GNU GPL por lo que permite un uso libre de la misma y el uso de herramientas *Open Source.*

Métricas

ISSAF propone una metodología para la valoración del riesgo en un sentido más teórico que practico. La evaluación del riesgo se basa en el estudio de tres factores significativos como son el valor del activo (tanto cuantitativo como cualitativo), las amenazas que son eventos que pueden conducir a daños (valor cualitativo de posibilidad) y la vulnerabilidad que es la

debilidad que puede ser explotada por la materialización de la amenaza (valor cualitativo) puede afectar al activo estudiado. Para ello se utiliza la siguiente fórmula:

Riesgo = Valor activo * Amenaza * Vulnerabilidad

Se analizará y valorarán estos riesgos para tomar decisiones a la hora de afrontarlos en función de la criticidad del mismo dentro del sistema en caso de ocurrencia. Esta forma de realizar la evaluación del riesgo es muy similar al estándar ISO 27001 y a la mayoría de guías de buenas prácticas (SPICE, CMMi, COBIT).

Fases de la metodología

ISSAF propone un enfoque concreto para la realización de la prueba de penetración que se lleva a cabo en tres fases. La figura 2.4 muestra de forma esquemática las tres fases a realizar en la metodología. La fase de evaluación se indica de una manera explícita, cíclica e iterativa los pasos a realizar.

Las tres fases que componen las pruebas de intrusión son las siguientes:

- Planificación y preparación.
- Evaluación (impactos, riesgos, etc.)
- Presentación de informes, limpieza (borrado de pistas) y destrucción de artefactos.

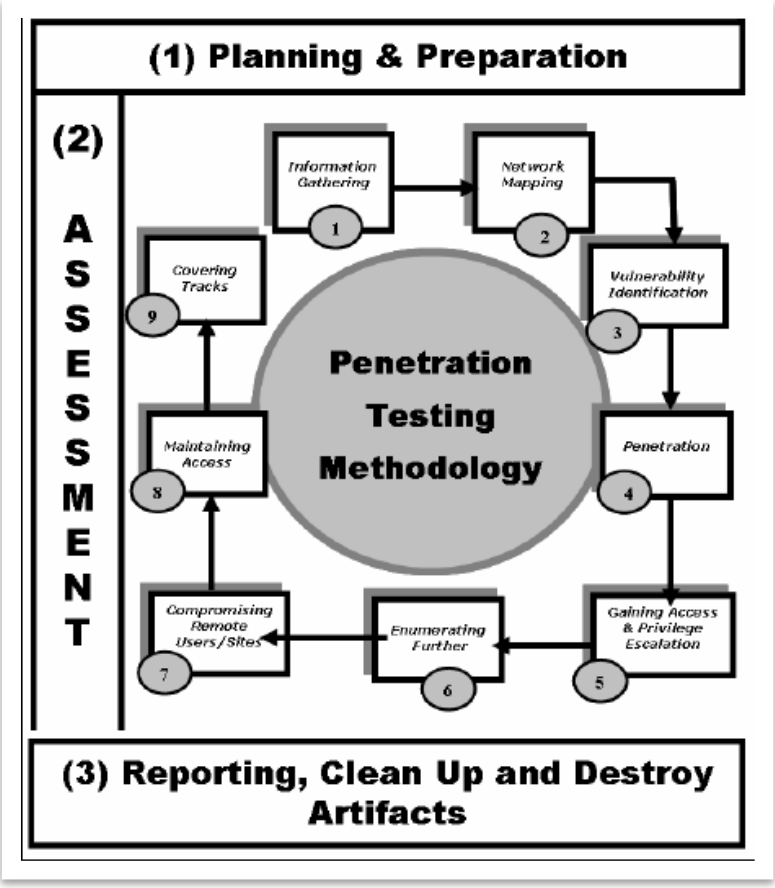

Figura 2.4. Fases propuestas por la metodología ISSAF

A continuación se expondrán las tres fases de las pruebas de intrusión que proponen la metodología ISSAF:

Fase I: Planificación y preparación

Esta es la fase inicial de la metodología, donde se prepara el escenario para la realización del test de intrusión. El aspecto más importante es la firma del acuerdo de evaluación, donde se delimitan tanto las funciones como las responsabilidades, creando una protección legal mutua y especificaciones de plazos, alcance, enfoque y limites. Este contrato debe ser firmado por las dos partes.

Fase II: Evaluación

Esta fase es donde realmente se lleva a cabo el test de intrusión. Se utilizara un enfoque orientado a las distintas capas del sistema, obteniendo acceso a niveles superiores a través de los pasos indicados en la figura, hasta su cumplimiento. Esta fase está dividida en 9 pasos.

1. **Recolección de información (*Information Gathering*)**

   Permite obtener la mayor cantidad de información acerca de las posibles formas de acceso al sistema. Se realizará tanto por medios externos como internos. La obtención de información para comprometer el sistema se obtendrá a través de cualquier medio, ya sea desde Internet (técnicas de DNS/WHOIS, presencia Web, búsqueda activa, teléfonos, email, etc.) o a través de la ingeniería social (empleados, *partners*, etc.).
   La recolección de esta información es muy importante en la consecución del test y deber obtenerse de la forma más cauta y sigilosa posible.

2. **Sondeo de la red (*Network Mapping*)**

   Permite la obtención de información desde un enfoque más técnico, tomado las huellas (*footprinting*) de la red y los recursos de los objetivos en cuestión. Con la información obtenida en la fase anterior y con la obtenida en esta, se ampliara la información con el fin de crear una posible topología de red del objetivo a evaluar. Antes de sondear la red es necesaria una planificación adecuada, teniendo en cuenta los siguientes tres aspectos básicos: punto de vulnerabilidad, puntos más críticos, y la consideración de los datos recolectados en el punto anterior.

   En este punto se utilizaran herramientas y aplicaciones de carácter muy técnico. Estas herramientas ayudaran al descubrimiento de la información de los *host* y elementos de red involucrados en la evaluación. Durante la actividad se realizaran acciones tales como búsqueda de *host* activos, escaneo de puertos y servicios, sondeo del perímetro

de la red (*routers*, *firewall*), identificación de servicios críticos, identificación de los S.O., identificación de *routers* usando MBI (*Management Information Base*).

3. Identificación de vulnerabilidades (*Vulnerability Identification*)

A priori, deben fijarse lo puntos específicos de evaluación y la forma en la que se realizara la identificación, profundizando en el conocimiento de los sistemas objetivos. Esto permitirá refinar en lo posible el futuro ataque de una manera planificada.

Las actividades a realizar incluyen la identificación de la vulnerabilidad de los servicios usando *banners*, escaneo de vulnerabilidades para conocidas (bases de datos publicas), verificación de falsos positivos y negativos, enumeración de las vulnerabilidades encontradas, estimación del impacto para el cliente, identificación las rutas de ataque y los escenarios para su explotación.

4.* Intrusión *(penetración)

Esta acción tiene como objetivo la obtención del acceso no autorizado al sistema. Para ello se eludirán las medidas de seguridad utilizadas y se tratara de llegar al mayor nivel de acceso posible. Para realizarlo, se ejecutan actividades tales como encontrar pruebas de concepto de código y herramientas para el testeo de las vulnerabilidades, desarrollar herramientas, evaluar los resultados de las pruebas de concepto de código, verificar o refutar las existencia de vulnerabilidades y documentar los descubrimientos. Se realizara un informe detallado con las explicaciones, las vías de explotación, evaluación del impacto y evidencias de la existencia de vulnerabilidad.

5. Ganar acceso y escalonado de privilegios (*Gaining Access & Privilege Escalation*)

La finalidad de este paso es la obtención de privilegios de administrador sobre el sistema, confirmando y documentando las intrusiones logradas, y automatizando las acciones para lograrla. Para la consecución del objetivo, se intentara en primer lugar ganar acceso con unos privilegios mínimos a través diferentes métodos tales como el descubrimiento de las combinaciones de nombre de usuario y *password*, *password* en blanco o por defecto, configuración predeterminadas, etc. Por lo tanto, se debe ganar privilegios en los dispositivos de manera perseverante y detallada, hasta la obtención de privilegios de administrador, asegurando el control y el compromiso de los sistemas.

6. Enumeración extra o adicional (*Enumerating Further*)

Pretende la obtención de información adicional, utilizando técnicas más intrusivas y mas especializadas, tales como ataques para obtener *password* cifradas, esnifar y analizar tráfico de red, recopilación de *cookies*, direcciones de correo, etc.

7. Comprometer usuarios y sitios remotos (*Compromise Remote Users/Sites*)

Una vez que se ha obtenido el acceso con altos privilegios a algún dispositivo del sistema interno, es necesario comprometer a usuarios y sistemas remotos al mismo, demostrando que el entorno está comprometido y obteniendo accesos privilegiados a la red interna.

8. Mantenimiento del acceso (*Maintaining Access*)

ISSAFF resalta que este punto normalmente no suele realizarse en una evaluación de seguridad, ya que implica un alto riesgo que podría ser aprovechado por verdaderos atacantes. Las actividades consisten en el mantenimiento del acceso al sistema a través de canales ocultos (túneles de acceso remoto, *backdoors),* instalación de *rootkits (*programas de *kernel* que permiten un acceso remoto con control total) y la ocultación de todas las actividades.

9. Cubrir las huellas (*Covering Tracks*)

ISSAFF indica que este paso es una práctica habitual, para actuar de la manera más abierta y generar información y registros detallados de todas las actividades realizadas.

El objeto de este paso es el ocultamiento de las huellas de la intrusión, realizando tareas de eliminación de evidencias y de actividades ejecutadas. Estas tareas consisten en la limpieza de archivos de registro, ocultación de ficheros, superación de pruebas de integridad de sistema, desactivación o engaño a sistemas antivirus, etc. Por lo tanto esta actividad se utiliza para el almacenamiento de la información obtenida, sin levantar ninguna alarma sobre los administradores del sistema.

FASE III: Informe, limpieza y destrucción de artefactos (*Reporting, Clean Up & Destroy Artifacts*)

La fase final de la metodología incluye la presentación de dos informes:

- Informe verbal, solo en el caso de descubrir una vulnerabilidad grave. Debe ser reportada de inmediato para que la organización sea consciente de ello.
- Un informe final por escrito, una vez finalizadas las pruebas definidas en el alcance de trabajo, donde se detallan al máximo los resultados obtenidos y las conclusiones de la misma, con las recomendaciones para la mejora.

  Este informe deberá presentar la siguiente estructura:

  - Resumen de gestión.
  - Alcance global del proyecto, incluyendo también las partes que no han sido consideradas.
  - Herramientas utilizadas (incluyendo *exploits*).

- Registro de las horas y las fechas en las que se han realizado las pruebas sobre los sistemas.
- Resultados de las pruebas realizadas.
- Listado de las vulnerabilidades detectadas, incluyendo las recomendaciones para solventarlas.
- Listado de los puntos de acción para el mantenimiento de seguridad en el sistema.

Por último, toda la información que se creó o almacenó durante la evaluación de los sistemas debe ser eliminada. Si no fuese posible desde el sistema remoto, es necesario informar al personal técnico para que realice estas acciones.

Profundizando en la metodología ISSAF se propone una metodología extendida de la fase II, donde se añaden especificaciones y herramientas utilizadas para concretar el test y ejemplos de cómo realizarlo, a modo de tutorial guiado.

Después de esta concreción de la fase II, se realiza una clasificación en cuatro áreas diferenciadas donde se explica de modo detallado cada una ellas. Estas áreas son las siguientes:

- Seguridad de redes.
- Seguridad de clientes de red.
- Seguridad de aplicaciones
- Seguridad de las bases de datos.

Ventajas

Las ventajas que aporta esta metodología se resumen en los diferentes puntos:

- El diseño se ha realizado a partir de cero, aportando un gran compendio de conocimiento con independencia y neutralidad de los productos existentes en el mercado. Al tratarse de una herramienta abierta, puede ser utilizada libremente y el personal de seguridad puede certificarse por parte de la entidad que la ha redactado.

- Presenta una fase de evaluación conocida y probada en el ámbito de la seguridad informática, que es utilizada de manera frecuente, sobre todo en Norteamérica. Esto reduce costes significativos en la inversión para implantarla en los organismos donde se requiera.

- Alta usabilidad, al tener unos pasos muy desgranados y lineales en la fase de evaluación. De esta forma facilita el informe a partir de los pasos realizados y los

resultados obtenidos. Al tratarse de una metodología lineal es muy recomendable para los auditores noveles.

- Aporta mucha información y soporte acerca de como implementar estándares y buenas prácticas del sector TI tales como IEC/ISO 27001:2005(BS7799), Sarbanes Oxley SOX404, CoBIT, SAS70 and COSO.

Limitaciones

- En la definición de la metodología existen partes como la delimitación del alcance del test de intrusión y concreción de acuerdos que no están definidas de manera clara. Esto podría suponer un pequeño descontrol de límites en la realización de test.

- La metodología propone herramientas concretas en la parte extendida del manual técnico a la hora de la evaluación. Esta vinculación propuesta la hace dependiente de las aplicaciones y de tecnología existente en el momento de la definición.

- La necesidad de actualización expuesta en el punto anterior, exigiría de la metodología una continua actualización de las herramientas y tecnologías propuestas. Sin embargo esta metodología no se ha actualizado desde el año 2006, lo que puede representar una percepción obsoleta de la misma en la parte extendida del test de penetración, no así en la parte genérica de evaluación.

- Otro punto reseñable respecto a los aspectos de profundidad de la seguridad, es que no cubre temas de protección de datos y *cloud computing*.

2.4 OWASP

OWASP (*Open Web Application Security Project*) es un proyecto creado en 2001 y está apoyado por la fundación OWASP, una organización sin ánimo de lucro, cuyo objetivo es soportar y apoyar al proyecto OWASP para garantizar su continuidad. El proyecto OWASP es un proyecto para la lucha contra la causa de software inseguro, en concreto, la construcción de aplicaciones y servicios más seguros, pero dedicada de manera exclusiva a aplicaciones Web. La guía de aplicación OWASP denominada *Testing Guide Versión 3.0* [3] es la guía que está dentro del proyecto *OWASP Testing Project*, que es sobre la que se desarrollará este trabajo.

Ámbito y alcance

El ámbito de aplicación se refiere exclusivamente al entorno de aplicaciones Web de las organizaciones, generalmente desde el punto de vista de caja negra (aunque en algunas

pruebas se utiliza la caja gris). La metodología de pruebas de intrusión está desarrollada centrándose en el ciclo de vida del desarrollo de software (SDLC), en concreto en las fases de pruebas y de puesta en producción. Se hace mucho hincapié en la utilización de buenas prácticas al realizar las actividades en los entornos de desarrollo, para de esta forma obtener código de programación seguro, y por ende, aplicaciones más seguras.
Por tanto, la aplicabilidad de esta metodología cubre a todas las organizaciones posibles, con la única limitación de tener actividades de entornos Web, tanto en ámbitos de Internet como en su versión privada de Intranet.

Meticulosidad

La exposición de la metodología es muy detallada en el ámbito de la seguridad de aplicaciones Web, con prácticamente todas las pruebas necesarias para el testeo de cualquier aplicación en dicho entorno. A pesar de que el alcance de su aplicación está definido a los entornos Web, OWASP es una metodología muy didáctica y muy precisa.

Usabilidad y uso

Aporta una alta usabilidad a pesar de ser una metodología muy técnica. Esto lo consigue gracias a una descripción muy resumida de las pruebas y a las aportaciones de ejemplos y referencias. De esta forma, se permite una buena comprensión de la metodología.
En cuanto al uso de la misma por parte de los auditores, esta es una de las metodologías más utilizadas y mejor valoradas en el entorno de las auditorias. Se utiliza siempre en combinación con otra metodología que complemente los ámbitos no alcanzados con ella.

Métricas

Esta metodología aporta una valoración de riesgos también desde un punto de vista teórico, enfocado a las primeras etapas del ciclo de vida del desarrollo del software, mediante la utilización del modelado de amenazas. El enfoque que aporta la metodología está basado en un modelo de valoración de metodología estándar basado en las metodologías más utilizadas:

Riesgo = Probabilidad de ocurrencia * Impacto

Para ello es necesaria la identificación de cada uno de los riesgos que puedan producirse en el proyecto y estimar los factores de que influyan en la probabilidad de ocurrencia y en el impacto en el negocio. Una vez estimado cada uno de los factores, es necesario determinar la severidad del riesgo, aplicando para ello un método semi-cuantitativo. Este método utiliza diferentes clasificaciones a través del uso de adjetivos tales como alto, medio, bajo, que se corresponden con una escala numérica para calcular el nivel de riesgo. Es necesario relacionar el impacto técnico del cada riesgo con el impacto real sobre el negocio para

calcular la severidad real de cada riesgo. Por último es necesario decidir qué riesgo es necesario mitigar y como ajustar el modelo de valoración de riesgo de manera personalizada alineándose con el modelo de negocio.

Fases de la metodología

OWASP en el apartado de pruebas de intrusión de aplicaciones Web, describe como realizar la comprobación de cada una de las vulnerabilidades. La metodología está dividida en tres pasos las pruebas de modo pasivo, pruebas de modo activo y la realización del informe final.

1. **Modo pasivo**: Se indica la manera de realizar las pruebas para obtener una comprensión de la lógica de la aplicación y determinar los puntos de acceso a la misma, utilizando utilidades para la recopilación de información. Todos los puntos de acceso que se encuentren en esta fase, deberán ser considerados en las posteriores pruebas de modo activo.

2. **Modo activo**: Esta fase es la más importante y más detallada de las metodologías de pruebas de aplicaciones Web. Está dividida en 9 categorías diferentes con un total de 66 procedimientos a realizar.

Las categorías que componen las pruebas de intrusión de modo activo son las siguientes:

- **Recopilación de la información (*Information Gathering*):** La primera de las fases consiste en recopilar tanta información como sea posible sobre la aplicación que es objeto de las pruebas. Este paso es una tarea imprescindible para la realización del test de intrusión. Existen diversidad de formas, tales como el uso de herramientas de acceso público (motores de búsqueda), escáner, envío de peticiones HTTP, etc. Esta categoría de presenta los siguientes procedimientos:
    - **OWASP-IG-001. *Spyders*, Robots y *Crawlers*:** Consiste en la navegación y captura de recursos relacionados con la aplicación que es esta testeando.
    - **OWASP-IG-002. Reconocimiento mediante motores de búsqueda:** Los motores de búsqueda se pueden usar para el descubrimiento de incidencias que estén relacionadas con las estructuras de las aplicaciones, o por páginas de error que han sido indexadas por los buscadores.
    - **OWASP-IG-003. Identificación de puntos de entrada de la aplicación:** Consiste en la identificación y catalogación de cada sección de la aplicación que deba ser

objeto de investigación, una vez que se termine el proceso de enumeración y acotación.

- **OWASP-IG-004. Pruebas para encontrar firmas de aplicaciones Web:** Determinar la firma de la aplicación es una de las primeras actividades para la recopilación de información. La obtención de los datos del tipo de servidor y la versión del mismo, permite la determinación de las vulnerabilidades conocidas y la utilización del *exploit* adecuado a las mismas.

- **OWASP-IG-005. Descubrimiento de aplicaciones:** Consiste en la identificación de las aplicaciones Web instaladas en el servidor Web o servidor de aplicaciones. Es muy útil para la obtención de la presencia de aplicaciones Web con propósitos administrativos y la existencia de elementos con versiones antiguas u obsoletas.

- **OWASP-IG-006. Análisis de códigos de error:** Se basa en la obtención de datos que no están orientados a la vista del usuario final, tales como códigos de error que suministren información de las tecnologías y productos utilizados.

- **Pruebas de gestión de la configuración (*Configuration Management Testing*):** La realización de un análisis sobre la infraestructura o la topología de la arquitectura permite la obtención de datos significativos tales como el código fuente, los métodos HTTP permitidos, funcionalidades administrativas, métodos de autenticación y configuraciones de la infraestructura. Esta categoría de presenta los siguientes procedimientos:

  - **OWASP-CM-001. Pruebas de SSL/TLS:** Estos protocolos proporcionan soporte criptográfico para la creación de canales seguros de transmisión en la capa de transporte.

  - **OWASP-CM-002. Pruebas del receptor de escucha de la Base de Datos:** Es necesaria la protección del receptor de escucha de la base de datos, dado se puede obtener información a través del mismo que podría ser utilizada posteriormente de forma maliciosa.

  - **OWASP-CM-003. Pruebas de gestión de configuración de la infraestructura:** La compleja y heterogénea infraestructura del servidor Web hace necesaria la gestión y revisión de la configuración del mismo, dada la cantidad de aplicaciones Web que tiene que soportar.

- **OWASP-CM-004. Pruebas de gestión de configuración de la aplicación:** Se debe revisar la información adicional que puede suministrar, tales como el código fuente, archivos de registro o códigos de error.

- **OWASP-CM-005. Gestión de extensiones de archivo:** Es posible la obtención de información a partir de las extensiones de los ficheros, identificando las tecnologías que soportan y los sistemas adicionales a los que se conectan**.**

- **OWASP-CM-006. Archivos antiguos, copias de seguridad y sin referencias:** Existen ficheros redundantes legibles y descargables de los servidores Web que permiten la obtención de información importante. Es necesaria la verificación de la existencia de los mismos.

- **OWASP-CM-007. Interfaces de administración de la infraestructura y de la aplicación:** Es necesaria la búsqueda de interface de administración en las rutas comunes utilizadas, para evita que se permita acceso a las funcionalidades de administración.

- **OWASP-CM-008. Métodos HTTP y XST:** Es necesario comprobar que el servidor no permita métodos http potencialmente peligrosas y que no es posible la ejecución de *Cross Site Tracing*.

- **Pruebas de Autenticación (*Autenticación Testing*):** En el ámbito de la seguridad informática, la autenticación es el procedimiento llevado a cabo con el fin de verificar la identidad digital del emisor de una comunicación. En primer lugar, es necesaria la comprensión de cómo funciona el proceso de autenticación, para después comprobar el proceso a través de diversas pruebas, tales como cuentas de usuarios predeterminadas, fuerza bruta, saltarse el sistema de autenticación, etc. Esta categoría de presenta los siguientes procedimientos:

  - **OWASP-AT-001. Transmisión de credenciales a través de un canal cifrado:** Se verificara si la información introducida en formularios Web para la autenticación se transmite con protocolos seguros.

  - **OWASP-AT-002. Enumeración de usuarios**: Se intentara recopilar un conjunto valido de usuarios a través de la interactuación en el proceso de autenticación de la aplicación.

- **OWASP-AT-003. Pruebas de diccionario sobre cuentas de usuario o cuentas predeterminadas:** Se comprobaran las cuentas de usuarios predeterminados o con contraseñas débiles.

- **OWASP-AT-004. Pruebas de Fuerza Bruta:** Si se intenta un ataque de diccionario y falla, será necesario intentar la autenticación a través de métodos de fuerza bruta.

- **OWASP-AT-005. Saltarse el sistema de autenticación:** Se intentara acceder a los recursos inadecuadamente protegidos en la aplicación para saltarse el mecanismo de autenticación.

- **OWASP-AT-006. Comprobar Sistemas de recordatorio/restauración de contraseñas vulnerables:** Se comprobara el sistema que realiza la gestión de las contraseñas olvidadas por el usuario.

- **OWASP-AT-007. Pruebas de gestión del Caché de Navegación y de salida de sesión:** Se comprobaran el correcto funcionamiento de las funciones de cierre de sesión y cache.

- **OWASP-AT-008. Pruebas de CAPTCHA:** Es una prueba de *desafío-respuesta* para asegurar que la respuesta no se ha generado de forma automática por un ordenador. Es necesario verificar la seguridad de este tipo de implementación

- **OWASP-AT-009. Múltiples factores de autenticación:** Esta autenticación utiliza múltiples factores tales como generadores de contraseña de un solo uso, la utilización de dispositivos criptográficos, contraseñas enviadas a través de *sms* e información privada solo conocida por el usuario legítimo.

- **OWASP-AT-010. Probar por situaciones adversas:** La duración de determinadas acciones impactan sobre otras, produciendo un fallo que implica un resultado inesperado. Este tipo de fallo se define como condición de carrera.

- **Pruebas de gestión de sesiones (*Session Management Testing*):** En esta batería de pruebas se incluyen todos los controles necesarios que se realizan sobre el usuario, desde la autenticación hasta la salida de la aplicación. La mayoría de entornos de aplicación web suelen proporcionan a los desarrolladores rutinas para la gestión de sesiones. En general, es necesaria la emisión de algún tipo de testigo de identificación o cookie. Esta categoría de presenta los siguientes procedimientos:

- **OWASP-SM-001. Pruebas para el esquema de gestión de sesiones:** Es necesaria la descripción de como se realiza un análisis del esquema de gestión de sesiones, para así comprender el mecanismo desarrollado e intentar saltarse la sesión del usuario. Acciones típicas son ingeniería inversa, o manipulación de una cookie.

- **OWASP-SM-002. Pruebas para atributos de sesión:** La protección de las *cookies* es una actividad imprescindible en la implementación de la aplicación, por lo que es necesario tomar precauciones al asignarlas y probar sus atributos.

- **OWASP-SM-003. Pruebas para fijación de sesión:** Se verificara la fijación de sesión a través de la búsqueda de vulnerabilidades cuando se renueva la *cookie*, instantes después de una autenticación de usuario que resultase exitosa.

- **OWASP-SM-004. Pruebas para variables de sesión expuestas:** Se verificaran los testigos de sesión que representen la información confidencial ligada a la identidad del usuario en su propia sesión.

- **OWASP-SM-005. Pruebas para CSRF :** *Cross Site Request Forgery* (CSRF) es un tipo de vulnerabilidad que describe la forma de forzar en la realización de acciones no deseada a usuarios ya autenticados, por lo que será necesario probar que la aplicación está exenta de esta vulnerabilidad.

- **Pruebas de Autorización (*Authorization Testing*)**. La autorización hace referencia a la concesión de los permisos de acceso a recursos determinados, únicamente a los usuarios que tienen permiso para ello. Estas pruebas permiten comprender el proceso de autorización, y utilizar este conocimiento para flanquear dichos mecanismos. Dentro del orden natural de acceso a los recursos, esta es la fase siguiente a la de la correcta autenticación. Esta categoría presenta los siguientes procedimientos:

  - **OWASP-AZ-001. Pruebas de ruta transversal:** Se verificará la forma de ejecutar ataques de traspaso de ruta para acceder a la información reservada que se localice.

  - **OWASP-AZ-002. Pruebas para saltarse el esquema de autorización:** Se verificará la implementación del sistema de autorización para cada perfil de usuario/privilegio, con la intención de acceder a recursos o funciones reservadas.

- **OWASP-AZ-003. Pruebas de escalado de privilegios:** Se verificara la imposibilidad de que un usuario modifique los privilegios de su perfil, obteniendo un escalado de privilegios.

- **Comprobación de la lógica de negocio (*Busines Logic Testing*). OWASP-BL-001:** Los fallos de este tipo no puede ser detectado por un *scanner* de vulnerabilidades genérico, ya que son vulnerabilidades muy difíciles de detectar. Además son vulnerabilidades muy peligrosas y muy concretas de cada aplicación, que normalmente pueden ser verificadas un cierto nivel de habilidad y de creatividad por parte del evaluador.
  La lógica de negocio está formada por las reglas de negocio y por lo flujos de trabajo. Las reglas de negocio expresan las políticas del negocio (canales, localización, logística, precios, productos, etc.), mientras que los flujos de trabajo son las tareas ordenadas de paso de documentos o datos de un elemento participante (una persona o sistema de software) a otro.

- **Pruebas de validación de datos (*Data Validation Testing*):** Es la debilidad más habitual que presenta la seguridad de aplicaciones web. Habitualmente ocurre desde las entradas de datos procedentes tanto del cliente como del entorno de la aplicación, y es la principal causa de las vulnerabilidades en aplicaciones, tal como inyecciones de datos sobre el intérprete y sobre el sistema de ficheros, ataques local/Unicode y desbordamientos de búfer.
  Se ha de considerar el entorno como un entorno hostil, de forma que a priori los datos procedentes de cualquier entidad/cliente externos no deberían ser considerados como confiables. La realización de estas pruebas permite comprobar la mayoría de formas posibles de validación de datos, y comprobar la resistencia de las aplicaciones ante cualquier tipo de datos, sobre todo si son maliciosos.

  De forma genérica, una vulnerabilidad *Cross Site Scripting* (XSS) explota un patrón de ataque del tipo Entrada->Salida == XSS. Para explotar esta vulnerabilidad, se intentan manipular los parámetros de entrada que recibe la aplicación para que generen una salida maliciosa. Los siguientes procedimientos están basados en XSS:

  - **OWASP-DV-001. Pruebas de XSS Reflejado:** *Cross Site Scripting* reflejado se define para XSS no persistente, de manera que el ataque no es cargado con la aplicación vulnerable, pero es originado por la victima cargando la URI culpable.

- **OWASP-DV-002. Pruebas de XSS Almacenado:** XSS almacenado es el tipo de ataque a las aplicaciones Web más peligroso, y permite almacenar datos potencialmente vulnerables a este ataque en la aplicación Web.

- **OWASP-DV-003. Pruebas de XSS basado en DOM:** XSS basado en DOM se define al fallo que resulta de la utilización del contenido activo en una página, obteniendo información desde el usuario y realizando posteriormente operaciones inseguras que originen el fallo XSS.

- **OWASP-DV-004. Pruebas de XSS basado en Flash:** Las aplicaciones Flash son incrustadas en los navegadores, por lo que una aplicación mal diseñada podría presentar una vulnerabilidad de este tipo.

- **OWASP-DV-005. Inyección SQL:** Es un tipo de vulnerabilidad que se presenta cuando se inyecta una determinada consulta directamente en la base de datos. Si la aplicación usa entradas de usuario para crear las consultas SQL, es necesario que la aplicación realice una validación de datos para evitar esta vulnerabilidad. Cuando se explota de forma exitosa se permite el acceso o manipulación no autorizada en la base de datos.
  Una vulnerabilidad de inyección de SQL explota un patrón de ataque del tipo Entrada->Consulta SQL == Inyección SQL. Existen diferentes fabricantes y desarrolladores de sistemas de gestión de base de datos (SGBD), por lo que será necesario orientar la verificación en función del sistema a testear. Existen entre otros SGBD Oracle, MySQL, SQL Server, Microsoft Access y PostgreSQL.

- **OWASP-DV-006. Inyección LDAP:** Este es un tipo similar al de SQL, salvo que en vez de utilizar el lenguaje SQL se utiliza el *protocolo Lightweight Directory Access Protocol* (LDAP) y el objetivo es un servidor LDAP.
  El patrón de ataque es del tipo Entrada→ Consulta LDAP == Inyección LDAP.

- **OWASP-DV-007. Inyección ORM:** Este es un tipo similar a los anteriores, pero en este caso se usan las pruebas de inyección SQL contra un modelo de objeto generado de acceso a datos. Es un ataque similar a Inyección SQL, pero la vulnerabilidad reside en el código generado por la herramienta *Object-relational mapping (ORM)*.

- **OWASP-DV-008. Inyección XML.** La realización de estas pruebas ocurre al introducir un determinado documento *eXtensible Markup Language* (XML) en la aplicación. En el caso de que el interprete XML falle al realizar la validación

adecuada de los datos, supondrá la presencia de esta vulnerabilidad. El patrón de ataque que sigue es Entrada -> documento XML == Inyección XML.

- **OWASP-DV-009. Inyección SSI:** La utilización de los *Server-Side Includes* (SSI), permite la inserción de código dinámico en paginas html estáticas. SSI son unas extensiones muy simples que podrían permitir la inyección de código dentro de paginas html o permitir su ejecución remota.

- **OWASP-DV-010. Inyección XPath:** XPath es un lenguaje que se utiliza para la operación de datos descritos en XML. La inyección de XPath permite incluir elementos XPath en una consulta para evitar la autenticación o la autorización a recursos.

- **OWASP-DV-011. Inyección IMAP/SMTP:** La verificación de este tipo de inyección permite detectar esta vulnerabilidad, que es debida a una incorrecta validación de los datos de entrada cuando se inyectan ordenes IMAP/SNTP de forma arbitraria. Este tipo de vulnerabilidad tiene el siguiente patrón Entrada -> orden IMAP/SMTP == Inyección IMAP/SMT

- **OWASP-DV-0012. Inyección de código:** La verificación permite comprobar la inclusión de código como entrada de una página Web, para que se ejecute por el servidor Web. Esta vulnerabilidad sigue el patrón de Entrada -> Código malicioso == Inyección de Código.

- **OWASP-DV-013. Inserción de órdenes en el sistema operativo:** Se realiza a través de la inserción de una orden del sistema operativo dentro de la petición HTTP a la aplicación. Este sigue el patrón de Entrada -> Orden del sistema == Inyección del orden

- **OWASP-DV-014. Prueba de desbordamiento de Búfer:** Al realizar este tipo de prueba se verifican las vulnerabilidades de desbordamiento de búfer (*buffer overflow*) tales como desbordamiento de memoria dinámica (*Heap overflow*), desbordamiento de Pila (*stack overflow*) y cadenas de formato (*Format strings*). Esta vulnerabilidad presenta el patrón Entrada -> (Fixed buffer) OR (Format String) == Desbordamiento

- **OWASP-DV-015. Pruebas de vulnerabilidad incubada:** Esta vulnerabilidad necesitara más de un tipo de vulnerabilidad de validación de datos para que resulte afirmativa. Se comprueba por cada patrón de entrada, validándolo antes de que se

les permita acceder a la aplicación. Se chequea de esta forma que la aplicación hace lo que debe hacer.

- **OWASP-DV-016. Pruebas de HTPP Splitting/Smuggling:** Se describirán pruebas en busca de vulnerabilidades del protocolo HTTP tales como *HTTP Splitting* o *HTTP Smuggling*.

- **Pruebas de denegación de servicios (*Denial of Service Testing*)**: Las vulnerabilidades del tipo de denegación de servicios inutilizaran uno o varios recursos del sistema atacado, y suponen la imposibilidad de acceso a los usuarios autorizados que deberían poder acceder a ellos. El tipo más común de este ataque es hacer inalcanzable la comunicación entre el servidor y usuarios válidos. La manera de explotarlo suele ser inundando con suficiente tráfico una máquina objetivo, de forma que sea incapaz de sostener el volumen de peticiones que recibe. Este tipo de ataque es mitigado de forma adecuada mediante soluciones de arquitectura de red. Sin embargo, dentro de las aplicaciones se puede presentar esta vulnerabilidad cuando se provoca que algunas funcionalidades o incluso el sitio web completo quede indisponible. Estos problemas son causados por *bugs* (fallos) en la aplicación, en ocasiones como resultado de entradas indebidas o valores de entrada no esperados. Esta categoría presenta los siguientes procedimientos:

  - **OWASP-DS-001. Denegación de servicio mediante ataques SQL *Wildcard:*** Este tipo de ataques obligan a que una base de datos ejecute un uso intensivo de la CPU al utilizar varios *wildcard* (comodines).

  - **OWASP-DS-002. Bloqueando Cuentas de Usuario:** Se comprueba la posibilidad de bloqueo de cuentas de usuario validas, a través de intentos consecutivos de registro con un *passwords* incorrectas.

  - **OWASP-DS-003. Desbordamientos de Búfer:** Se comprueba la posibilidad de causar una condición que provoque denegación de servicio a través del desbordamiento de una o más estructuras de la aplicación Web.

  - **OWASP-DS-004. Reserva de Objetos Especificada por Usuarios**: Se comprueba la posibilidad de agotar los recursos del servidor a través de la asignación de un gran número de objetos.

  - **OWASP-DS-005. Pruebas de Uso de Entradas de Usuario como Bucle:** Se comprueba la posibilidad de forzar a que la aplicación realice un bucle sobre un

segmento de código que requiera de recursos de computación elevados, disminuyendo de esta forma el rendimiento del sistema.

- **OWASP-DS-006. Pruebas de Escritura de Entradas Suministradas por Usuario a Disco:** Se verifica que al llenar los discos de almacenamiento no se provoque una situación de denegación de servicio.

- **OWASP-DS-007. Fallar en la Liberación de Recursos:** Se comprueba que la aplicación libera de forma correcta los recursos del sistema una vez terminado su uso.

- **OWASP-DS-008. Pruebas de Almacenamiento Excesivo en la Sesión:** Se verifica que se agotan los recursos de memoria al asignar grandes cantidades de datos dentro de un objeto de sesión de usuario.

- **Pruebas de Servicios Web (*Web Service Testing*)***:* Los servicios web y SOA (Arquitectura Orientada a Servicios) son aplicaciones en pleno auge, que permiten la interoperación de negocios. Los clientes de servicios web generalmente son otros servidores Web que suministran un servicio al servidor que lo requiera, usando habitualmente los protocolos HTTP, FTP o SMTP. Aquellos *frameworks* de Servicios Web que utilizan el protocolo HTTP usan las tecnologías XML, SOAP, WSDL y UDDI. WSDL se utiliza para describir las interfaces de un servicio. SOAP proporciona el medio en la comunicación entre los servicios Web y las aplicaciones cliente con XML y HTTP UDDI se utiliza para registrar y publicar los servicios Web y sus características para así poder ser encontradas por clientes potenciales. Las vulnerabilidades en servicios web son similares a otras vulnerabilidades de entornos Web, pero además también tienen vulnerabilidades de XML únicas. Esta categoría presenta los siguientes procedimientos:

  - **OWASP-WS-001. Obtención de información en Servicios Web:** Se determinara los puntos de entrada, y si el esquema de comunicación esta descrito en el WSDL.

  - **OWASP-WS-002. Pruebas de WSDL:** Una vez identificado el WDSL debe probarse el punto de entrada.

  - **OWASP-WS-003. Pruebas estructurales de XML:** Se verificara la correcta construcción del mensaje XML, para evitar los posibles ataques de denegación de servicios.

  - **OWASP-WS-004. Comprobación de XML a nivel de contenido:** Se comprobara el contenido del servidor Web, para evitar este tipo de ataque que típicamente puede

ser del tipo Inyección de SQL o XPath, desbordamiento de búfer y inyección de instrucciones.

- **OWASP-WS-005. Comprobación de parámetros HTTP GET/REST:** Se verificaran los parámetros de las aplicaciones XML que reciben parámetros a través de consultas HTTP GET.

- **OWASP-WS-006. Adjuntos SOAP Maliciosos:** Se deben verificar los archivos adjuntos que recibe la aplicación Web, tanto en el proceso del servidor como en la redistribución a los clientes.

- **OWASP-WS-007. Pruebas de Repetición:** Se debe verificar a través de pruebas de repetición para evitar la suplantación de identidad y el posterior uso no autorizado.

- **Pruebas de AJAX (*AJAX Testing*)**: AJAX (*Asynchronous JavaScript And XML*) es una técnica de desarrollo para la creación de aplicaciones web interactivas que suministra una experiencia al usuario parecido a la de una aplicación local. Desde el punto de vista de la seguridad, las aplicaciones AJAX ofrecen una mayor superficie de ataque que las convencionales, ya que el lado del usuario también presenta vulnerabilidades, de forma que tiene se añadirse estas vulnerabilidades a las vulnerabilidades de las aplicaciones Web tradicionales.

  Las aplicaciones web tradicionales envían los datos de los formularios HTML estándar a través de peticiones GET o POST sencillas, mientras que las aplicaciones AJAX pueden usar una codificación diferentes o esquemas de serialización para el envió de datos a través de peticiones POST, de forma que dificulta la creación de peticiones de pruebas de forma automática. Para mejorar esto, suelen utilizarse *proxys* Web, observando el tráfico asíncrono y modificando el tráfico para testear correctamente la aplicación AJAX. Esta categoría presenta los siguientes procedimientos:

  - **OWASP-AJ-001. Vulnerabilidades AJAX**. Las aplicaciones AJAX presentan una mayor superficie de ataque. Las funciones internas de la aplicación están más expuestas y permiten el acceso por parte de clientes a recursos sin una seguridad integrada, ni mecanismos de cifrado, etc. Por tanto, es necesario comprobar minuciosamente las vulnerabilidades de AJAX.

  - **OWASP-AJ-002. Como probar AJAX.** Todas las pruebas explicadas para las aplicaciones Web tradicionales son perfectamente validas para chequear las aplicaciones AJAX. Además de estas, se requiere la búsqueda las vulnerabilidades propias de AJAX, de forma que se debe encontrar los puntos de destino de las

llamadas asíncronas a los servidores Web y así determinar si el formato es el correcto a la hora de realizar las peticiones.

3. Redacción de informes: Una vez terminadas las fases de pruebas pasiva y activa, es muy importante la presentación del informe final de la manera más adecuada. De forma general, el informe debe seguir una serie de criterios básicos, como que debe ser perfectamente comprensible, debe plasmar la información de la forma más exacta, se debe recalcar los riesgos más importantes encontrados y debe dirigirse tanto al personal técnico como al de alta dirección. El informe debe tener las siguientes secciones:

- **Resumen ejecutivo**: Este informe analiza de forma general y resumida los hallazgos encontrados durante la evaluación, aportando una visión global del riesgo que presenta la aplicación Web. Como el destinatario entre otros es la alta dirección, debe utilizar un lenguaje sin tecnicismos, incluyendo tablas y gráficos que expliquen de forma sencilla el nivel de riesgo encontrado. Por último, es importante aporta las conclusiones obtenidas y las recomendaciones para la obtención de la aplicación segura.

- **Consideraciones técnicas generales**: Este es el informe técnico, por lo que está dirigido al personal técnico de la organización, de forma que debe tener un detalle más técnico que el resumen ejecutivo. Debe estar compuesto por el alcance de la evaluación, los objetivos, advertencias en la realización del mismo, explicaciones del tipo de medida del riesgo utilizado y un resumen técnico de los hallazgos encontrados.

- **Hallazgos realizados durante la evaluación**: Presenta detalles técnicos de las vulnerabilidades encontradas, que deben ser adecuadamente explicadas para la comprensión y posterior resolución de las mismas por parte del personal técnico de la organización. Cada vulnerabilidad deben incluir al menos:
  - Identificador numérico, que referencia las capturas de pantalla.
  - Elementos afectados.
  - Descripción técnica.
  - Resolución de la incidencia.
  - Nivel de riesgo e impacto.

- **Herramientas utilizadas**: Listado de las herramientas utilizadas durante las pruebas.

Ventajas

- Tiene una orientación eminentemente práctica con ejemplos y referencias de herramientas muy claras, con una buena estructura que facilita mucho su utilización en los ámbitos de aplicaciones Web que requieran mucho nivel de detalle. Esta alta usabilidad facilita mucho la orientación a la hora de realizar las labores del auditor novel.
- Es una metodología de referencia dentro del ámbito de la seguridad Web, muy conocida, valorada y utilizadas en las auditorias de sistemas Web. Tiene el apoyo de grandes instituciones y organizaciones que trabajan de manera constante en la actualización y desarrollo de la misma.
- Cubre perfectamente las amenazas más habituales en los entornos Web, referencia clara del los archiconocidos TOP-TEN desarrollados también dentro del proyecto OWASP.
- Es un metodología que aporta una nueva visión muy orientada a los ciclos de vida de desarrollo de software dentro del ámbito de aplicaciones Web, haciendo hincapié en el desarrollo de software seguro en cada una de las fases del ciclo de vida. Esta tendencia actualmente se está defiendo como una clara apuesta en el sector de los proyectos de desarrollo de software, que ayudan a la reducción de los costes finales y a la mejor imagen de las empresas que así lo implantan.

Limitaciones

- La cobertura de las pruebas se centra exclusivamente en las aplicaciones Web, de manera que debe ser complementada por parte de otra metodología para cubrir el espectro de las redes de infraestructura y de los sistemas que soportan las aplicaciones Web auditadas.
- La metodología no cubre la fase inicial de preparación y planificación de la misma, donde se delimitarían las cuestiones contractuales y legales de la auditoria y que otras metodologías hacen hincapié. Es una metodología muy técnica que deja todos los detalles a la correcta planificación del proyecto dentro del ciclo de vida del mismo.

2.5 Ubicación del test de intrusión dentro de la auditoria de seguridad

La auditoria informática es una actividad imprescindible dentro del modelo de negocio de una organización. Se puede definir la auditoría informática según Ron Weber [4], como el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informático:

- Salvaguarda los activos.
- Mantiene la integridad de los datos.
- Lleva a cabo los fines de la organización.
- Utiliza eficientemente los recursos.

Dentro de la auditoria informática en el contexto de la seguridad de la información se puede incluir como uno de los procesos, la auditoria de seguridad. La auditoría de seguridad tiene como objetivo principal el análisis de la seguridad de los sistemas de información y los servicios de las organizaciones. Este análisis y las posteriores medidas, son necesarias para cumplir con los objetivos de la organización donde se lleve a cabo la auditoria. La auditoria de seguridad abarca tanto la planificación, como las políticas de seguridad, la revisión de la normativas legislativas, la aplicación de las LOPD, etc. Es decir, posee una amplia visión en cuanto a los aspectos que han de ser considerados y planificados.

Una buena clasificación que engloba las diferentes actividades que compone una auditoria de seguridad, es resumida en la definición realizada en la metodología OSSTMM 2.1 [5]. En la figura 2.5 se muestra un gráfico de las actividades realizadas en el ámbito de la auditoria de seguridad teniendo en cuenta el coste y tiempo de dedicación. Solamente se han tenido en cuenta las actividades que se consideran importantes dentro del alcance de este trabajo.

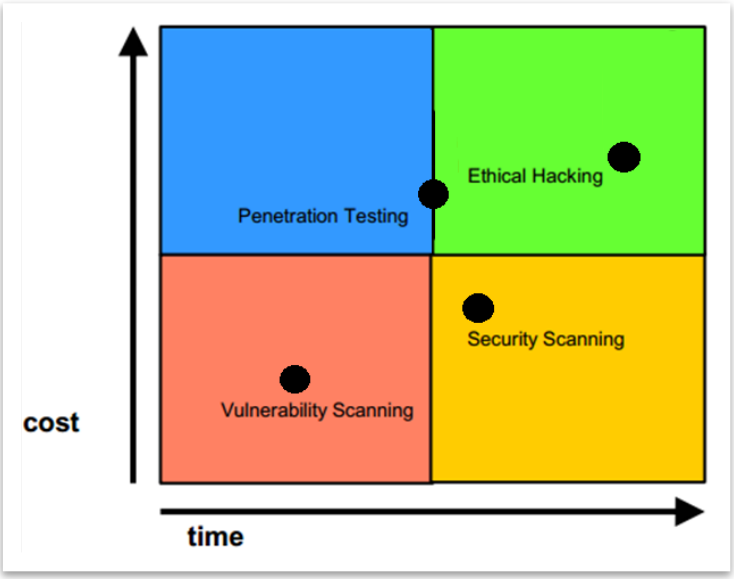

Figura 2.5. Actividades realizadas en el ámbito de la auditoria de la seguridad

Las actividades que se ha tenido en cuenta en la clasificación son las siguientes:

- ***Vulnerability Scanning***: Implica las comprobaciones automáticas de vulnerabilidades conocidas de los sistemas de una red.
- ***Security Scanning***: Conlleva de forma genérica la búsqueda de vulnerabilidades, incluyendo la identificación de los puntos débiles, análisis y verificación por parte de un profesional de los falsos positivos.
- ***Penetration Testing***: Esta orientado a los proyectos cuyo fin principal es la obtención de un trofeo, incluyendo la adquisición de acceso de forma privilegiada a un objetivo con medios pre-condicionales.
- ***Ethical Hacking***: Abarca todos los test de intrusión, a partir del cuales pueda ir ganado acceso a otros objetivos superiores para el fin propuesto. La realización del hacking ético conlleva la obtención del acceso a los objetivos dentro del tiempo predeterminado de duración del proyecto.

Una vez explicadas de forma muy genérica las diferentes partes que implican una auditoria de seguridad, ahora es necesario ubicar el alcance de los test de intrusión. Esto es necesario para acotar el alcance de este trabajo en la elaboración de la nueva metodología.

La auditoria técnica habitualmente suele utilizar el término acuñado como *hacking* ético, para diferenciarlo de las actividades que realiza habitualmente un atacante, al que se le suele llamar *hacker* de manera peyorativa. El *hacking* ético consiste en la ejecución de una serie de pruebas de manera planificada, que simulen los métodos, técnicas y acciones que utilizaría un atacante para acceder al sistema y explotar alguna de sus vulnerabilidades. Estas actividades deben realizarse de forma:

- Autorizada, habitualmente a través de un contrato.
- Controlada, para no dañar o dejar sin servicio algún dispositivo o sistema analizado.
- Ética, según los códigos éticos de esta actividad.

Las actividades de *hacking* ético están compuestas por varios tipos de análisis y pruebas, en función del alcance y los objetivos que se quieran evaluar. En concreto la actividad de test de intrusión, que es sobre la que se centra este trabajo, está dentro del *hacking* ético, junto con otras actividades. La composición que engloba estas actividades se muestran en la figura 2.6.

Figura 2.6. Conjunto de actividades que componen la auditoria de seguridad

El test de intrusión podría definirse como la evaluación activa y continua de la seguridad de los SI y de las redes que comunican estos SI, a través de la simulación de un ataque cuyo fin principal es la adquisición de privilegios de un objetivo concreto. Para simular los ataques se utilizan diferentes técnicas conjuntas, que complementan el trabajo con las herramientas de software que permitan este acceso y elevación de privilegios. El conjunto de los diferentes test de intrusiones utilizados permitirá cumplir el fin del *hacking* ético estipulado en el contrato. Este fin consistirá en el acceso a otros objetivos de nivel superior y la determinación del grado de accesibilidad que un atacante podría obtener sobre los SI.

Los test de intrusión presentan una serie de beneficios [6]:

- Adquisición del grado general de vulnerabilidad que presenta un SI, necesario para la aplicación de medidas correctivas.
- Descubrimiento de fallos de seguridad sobre sistemas configurados por defecto o después de un cambio de la configuración.
- Determinación de fallos de seguridad en SI debidos a falta de actualización de los componentes del sistema operativo o de las aplicaciones.
- Identificación de configuraciones erróneas que pueden provocar fallos de seguridad en dispositivos de red.
- Ahorro en cuanto a costes directos o indirectos derivados del tiempo dedicado a la corrección de las situaciones negativas antes de su ocurrencia.
- Reducción del impacto y de la probabilidad de materialización del mismo en caso que supongan grandes pérdidas de capital, ya sea por reclamaciones, mala imagen corporativa, perdida de oportunidades, sanciones legales, reposición de daños, etc.

Dentro del ciclo de vida de desarrollo de software se requiere la inserción de buenas prácticas de seguridad, para la obtención de software más seguro y confiable. Gary MacGraw propone un nuevo modelo de ciclo de vida de desarrollo de software seguro, que incluye la adopción de esas mejores prácticas de seguridad a aplicar a los artefactos de cada una de las fases de desarrollo. McGraw [7] plantea 7 prácticas (*McGraw's Seven Touchpoints*) a incluir en el modelo de ciclo de vida en cascada. En concreto, las pruebas de intrusión las posiciona en tercer lugar de importancia de las prácticas a añadir, por detrás de la revisión de código y el análisis de riesgo. Las pruebas de intrusión se ubican en las fases de pruebas y de resultados de las mismas, y la realimentación de la fase de producción y explotación. Esta ubicación se muestra en la figura 2.7.

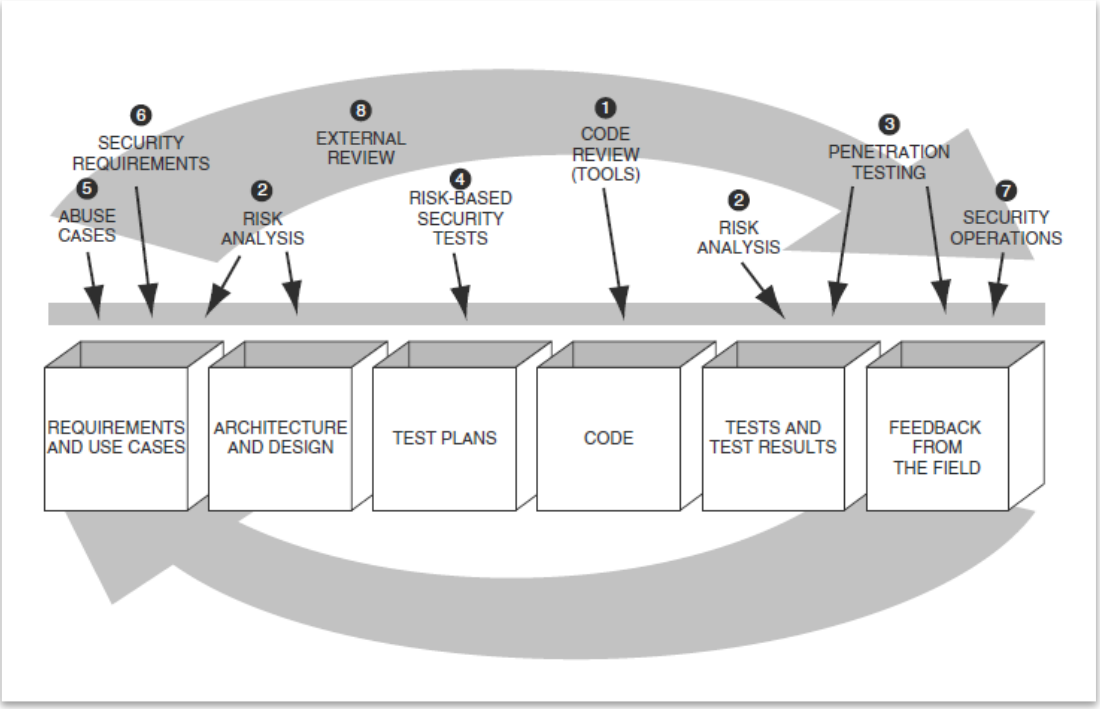

Figura 2.7. Modelo de mejores prácticas propuesto por McGraw

Este mismo enfoque es utilizado por la metodología OWASP para el testeo de las aplicaciones Web, haciendo mucho hincapié en encontrar las vulnerabilidades de las aplicaciones lo mas tempranamente posible en el ciclo de vida SDLC. Esta cuestión es muy importante, tanto desde el punto de vista de construir aplicaciones más seguras como cuestiones económicas, ya que cuanto más temprana es la fase donde se encuentre las vulnerabilidades más económico es subsanarla. Según el NIST [8], se produce una reducción del coste de hasta 30 veces en la reparación de un fallo en función de la fase en la que se detecte. Esto se muestra en la figura 2.8, donde se visualiza dicho aumento en función de la fase de detección.

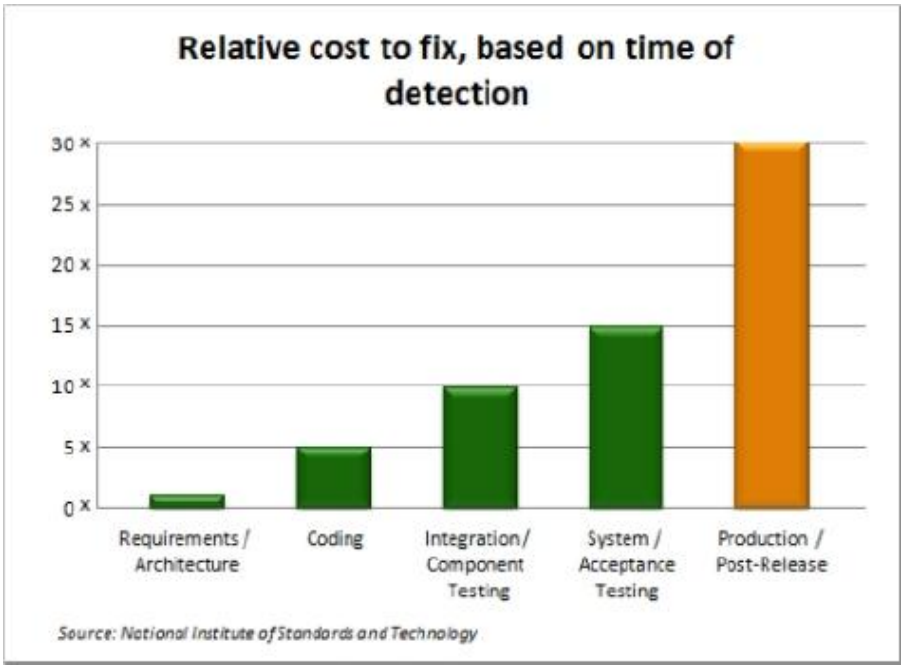

Figura 2.8. Evolución del coste de corrección de fallos en el ciclo de vida de una aplicación

Por tanto, desde el punto de vista de la construcción de aplicaciones seguras, se puede considerar el test de penetración como la verificación del comportamiento del software y la resistencia a diferentes tipos de ataques. En este sentido, existen diferentes terminologías y enfoques de los diferentes tipos de test de intrusión, que es necesario diferenciar entre el ámbito de la auditoria técnica y el de la auditoria de aplicaciones. Esta clasificación divide los test de intrusión en diferentes tipos de pruebas: Caja blanca, caja gris y caja negra. El enfoque que se quiere aportar en este trabajo es el punto de vista de las auditorias técnicas, por lo que para su explicación se va a utilizar las definiciones dadas en la metodología OSSTMM 3.0 [1]. Es importante definir el tipo de auditoría a aplicar, dado que en la fase inicial, al definir el alcance y el tipo de auditoría es necesario reflejarlos en la parte contractual.

OSSTMM presenta 6 diferentes tipos de pruebas, que varían en función de la cantidad de información que el auditor conoce sobre los objetivos a testear, que conocimiento tienen los objetivos sobre la realización de la auditoria, o sea, si los objetivos a testear han sido preparadas para la auditoria, que se espera de la prueba y la legitimidad de la misma. De los 6 tipos de pruebas de intrusión se han elegido solamente 3 de ellos, que son los que encajan dentro de las pretensiones de la nueva metodología a diseñar. Estos tipos de pruebas se muestran en la tabla 2.2.

Tipo	Conocimiento previo de las defensas, activos o canales	Preparación previa del objetivo, conociendo de antemano los detalles de la auditoria	Descripción
Double-Blind **CAJA NEGRA**	Ninguno	Ninguno	Este tipo de auditoría pone a prueba las habilidades del auditor y el estado de protección del objetivo ante variables desconocida. La amplitud y profundidad de esta prueba puede ser tan grande como el conocimiento pertinente por parte del auditor y la eficiencia permitida
Gray Box **CAJA GRIS**	Conocimiento limitado de las defensas y de los activos. Pleno conocimiento de los canales.	El objetivo ha sido preparado para la auditoria, conociendo por adelantado todos los detalles de la misma.	Este tipo de auditoría pone a prueba las habilidades del auditor. La naturaleza de la prueba es la eficiencia. La amplitud y profundidad de esta prueba dependen de la calidad de la información suministrada al auditor, así como el conocimiento pertinente del mismo. Este tipo de prueba a menudo se refiere a pruebas de vulnerabilidad y normalmente tiene como objetivo la autoevaluación.
Double Gray Box **CAJA BLANCA**	Conocimiento limitado de las defensas y de los activos. Pleno conocimiento de los canales.	El objetivo ha sido preparado para la auditoria en cuanto al alcance y espacio de tiempo de la auditoria, pero no tiene conocimiento de los canales a probar ni de los vectores de ataque.	Este tipo de auditoría pone a prueba las habilidades del auditor y el estado de protección del objetivo ante variables desconocida. La naturaleza de la prueba es la eficiencia. La amplitud y profundidad de esta prueba dependen de la calidad de la información suministrada al auditor y al objetivo antes de la prueba.

Tabla 2.2. Tipos de pruebas en los test de intrusión

En la figura 2.9 se muestra un grafico [1] donde se engloban los diferentes tipos de pruebas teniendo en cuenta por un lado que conocen los objetivos sobre los atacantes y que conocimiento tiene el atacante o auditor sobre los objetivos a testear. Aquí es donde se ubican cada uno de los tipos de pruebas explicados en la tabla 2.2 y que la nueva metodología utilizara en la realización de los test de intrusión.

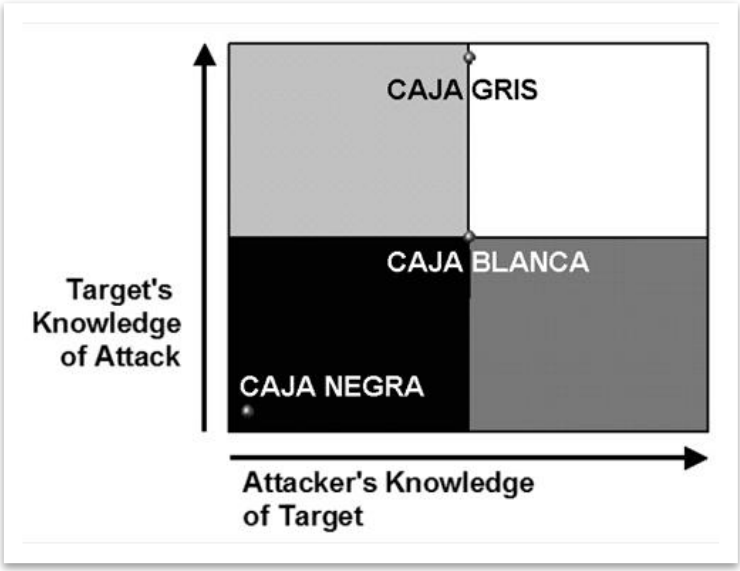

Figura 2.9. Ubicación de los tipos de pruebas de test de intrusión

Otro aspecto a destacar son las herramientas que se utilizan en los test de intrusión para la obtención de las vulnerabilidades. Estas aplicaciones son habitualmente semiautomáticas, dado que la realización de las pruebas de forma manual demoraría demasiado la realización de las pruebas. Estas herramientas no son perfectas, de forma que comenten fallos tanto por exceso como por defecto, la hora de encontrar las vulnerabilidades o debilidades de cada una de las partes que forma el sistema a analizar. Por tanto, una vez realizadas las pruebas y obtenidos los resultados correspondientes a estas, es necesario verificarlos. De esta forma se puede corroborar si la vulnerabilidad encontrada realmente lo es, y que no ha sido una falsa alarma. Existe otro caso peor, como es una vulnerabilidad que no ha sido detectada y que en un futuro puede ser explotada. Por tanto, es importante diferenciar estos dos tipos de errores, definiendo la terminología de ambos:

- **Falsos positivos**: Son vulnerabilidades reportadas por las herramientas de auditoría que realmente no existen. Este tipo de errores presentan una gran carga en la corroboración de los mismos, retrasando la obtención de conclusiones a cerca de las vulnerabilidades encontradas.
- **Falsos negativos**: Son vulnerabilidades no descubiertas por las herramientas utilizadas. Este tipo de error es muy grave, dado que el sistema auditado tiene una vulnerabilidad no detectada en la auditoria, que podría causar un impacto en el

sistema en caso de ser explotada. Además se ha creado un falso sentido de la seguridad que puede ser muy peligro, dado que las medidas de seguridad aplicadas puede ser más laxas o incluso inexistentes.

Para evitar en gran medida ambos tipos de errores es recomendable la utilización de una amplia variedad de herramientas que prueben el mismo tipo de vulnerabilidades. De esta manera se evita en lo posible los falsos negativos, que como se decía son errores muy graves en la realización de la auditoria. Este tipo de errores expresado en ratio suele utilizarse para la evaluación de la efectividad de las herramientas.

Capitulo 3: Desarrollo de una nueva metodología de test de intrusión

Una vez estudiadas cada una de las metodologías más utilizadas en la realización del test de intrusión, en este capítulo se pretende diseñar una nueva metodología de test de intrusión. Como se explicaba en la introducción, las pretensiones de esta metodología es la de aportar un punto de vista práctico y muy resumido, orientada a auditores nóveles.
La estructura del desarrollo va a ser similar a los resúmenes de las metodologías expuestas en el capítulo 2.

3.1 Características generales de la metodología

En este punto se muestra las características generales que se quieren obtener en la nueva metodología, estructurándolo de la misma forma que en el resumen de las metodologías OSSTMM, ISAFF y OWASP para tener una visión comparativa, y situar el desarrollo de la metodología dentro del mismo ámbito.

Ámbito y alcance

El ámbito de aplicación que se pretende cubrir con esta metodología es muy genérico, intentando cubrir todos los entornos de aplicabilidad posibles, tanto desde el punto de vista organizativo, de actividad, como tecnológico. Dado su enfoque global, las metodologías que mejor encajan en el objetivo de esta, son tanto la metodología ISSAF como OSSTMM, con un alcance que cubrían aspectos de sistemas, infraestructura de red cableada e inalámbrica, aplicaciones tanto locales como de entornos Web y sistemas de gestión de base de datos. No se entrara en aspectos como la seguridad física, o la seguridad orientada a la ingeniería social, que también cubre la metodología OSSTMM.

En este sentido la ubicación de esta metodología en el ciclo de vida desarrollo de software (SDLC), está ubicada en la puesta en producción y posterior explotación del sistema. En este aspecto, aunque no se abarquen pasos anteriores del SDLC, es altamente recomendable seguir los buenos hábitos que tan bien marcan la metodología OWASP, y que desde esta nueva metodología pueden complementarse con ellos.

En cuanto al punto de vista aportado por la metodología en función del nivel de información, tanto por parte del auditor como de los objetivos auditados, se aportaran tanto pruebas de caja negra como de caja blanca. La definición exacta de las pruebas será delimitada en la formalización contractual con la organización donde se realice la auditoria.

Meticulosidad

La metodología a desarrollar aportara una visión muy genérica de los test de intrusión, por lo que la profundidad y minuciosidad de la misma es muy leve. Se definirá una metodología con referencias a las metodologías OSSTMM, ISSAF y OWASP, que son las que realmente ya aportan el nivel de detalle necesario para la correcta realización de las pruebas en cada uno de los ámbitos que sean definidos en el alcance.

Usabilidad y uso

Uno de los objetivos principales en el desarrollo de esta metodología es la facilidad de uso y una curva de aprendizaje lo más ascendente posible, para su máxima comprensión y utilización en el mínimo tiempo posible. Estos son unos aspectos muy valorados entre los auditores jóvenes (entre los que se incluye el autor de este trabajo), dado lo abrumador que pueden parecer cada una de las metodologías que se han resumido en el capitulo anterior, sobre todo desde el punto de vista de satisfacción subjetiva en la aplicación de esta. No quiere decir con esto que esta metodología sustituya en algún punto a las anteriores metodologías, sino que sirva de guía rápida de referencia a las mismas, que son las verdaderas metodologías de test de intrusión. A través de un esquema de bloques de tipo cíclico, se pretende que sea lo más visual y fácilmente recordable, y cuya ejecución sea lo más sencilla posible. Dado lo generalista de esta metodología, en cada uno de los puntos en los que se divide la misma se referenciaran a los puntos clave de las metodologías estudiadas que cubran todos los aspectos y características necesarias al realizar las pruebas.

Métricas

En la metodología desarrollada en este trabajo no se cubrirá este punto, que es uno de los más importantes para la obtención de una visión más objetiva y manejable del nivel de riesgo analizado. Por tanto, se va a posponer dentro de las líneas futuras, siempre referenciándose a las buenas prácticas ya implantadas, desarrolladas y bien conocidas en los ámbitos de las auditorias informáticas.

3.2 Fases de la nueva metodología del test de intrusión

En primer lugar, se va a definir de forma muy genérica las distintas fases que englobaran la metodología del test de intrusión. Estas fases se desarrollaran y se dividirán en diferentes puntos a tratar en la ejecución del test de intrusión, creando las referencias necesarias a los ámbitos y fases de las otras metodologías estudiadas.

La nueva metodología se divide en 3 fases:

I. **Fase de planificación**: Esta es la fase inicial de la metodología, donde se definirá el alcance de la auditoria, acotando los ámbitos a cubrir y el tipo de metodología a realizar. En esta fase se formalizara en forma de contrato todas los detalles de las pruebas y las correspondientes clausulas contractuales de obligaciones y responsabilidades.

II. **Fase de actuación:** Esta fase es donde se realizaran las pruebas técnicas para el análisis de las vulnerabilidades y la explotación de las mismas. A partir de la batería de pruebas acordadas, se obtendrán los correspondientes resultados que deberán ser corroborados durante la explotación para la eliminación de falsos positivos.

III. **Fase de generación de informes:** Esta es la fase final de la metodología, donde se presentaran de forma ordenada las conclusiones y las recomendaciones para subsanar los errores de seguridad. Esta fase tiene como resultado la redacción de un informe a nivel ejecutivo y un resumen a nivel técnico.

La figura 3.1 muestra cada una de las fases, con sus correspondientes pasos que serán desarrollados a lo largo del capítulo.

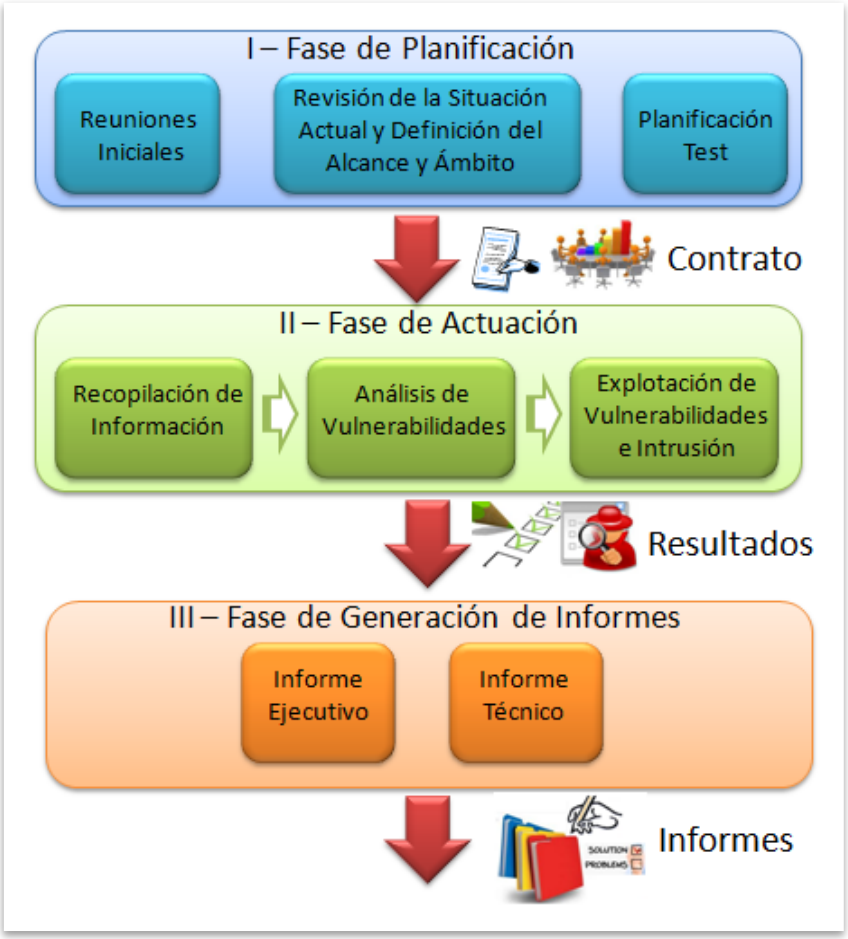

Figura 3.1. Fases de la metodología propuesta en este trabajo

I – Fase de planificación

La fase de planificación es la fase inicial de la metodología y es fundamental para el buen desarrollo posterior de las siguientes fases. En esta fase es muy importante acotar el alcance, definir los ámbitos y decidir tipo de auditoría técnica a realizar, para evitar desviaciones respecto de los objetivos pactados. Estas desviaciones pueden suponer una mala asignación de los recursos, retrasando los plazos y aumentando el coste, además de afectar a la calidad y rigurosidad de la misma. Esta fase a su vez, está dividida en una serie de pasos o hitos que se resumen más adelante.

En cuanto a cómo se plantea en las metodologías estudiadas, se puede referenciar a los siguientes puntos de estas:

- **OSSTMM Vers.3.0** [1]**:** Capítulo 2 – *What You Need To Do*. Desde el apartado 2.1 al apartado 2.5. Se definen los activos, alcance, ámbito de pruebas, tipo de pruebas, vectores de ataque y reglas de compromiso. A través de estos consejos se concretara de forma similar la fase de planificación. Página 33 - 40.
- **ISSAF Vers. 0.2.1** [2]**:** Capítulo 5.1.1 a 5.1.9 – *Phase I – Pre-Assessment*. En este apartado de la metodología explica cómo desarrollar la fase de planificación de las pruebas de intrusión. Se exponen desde la petición de la propuesta, evaluación de contratos con terceras partes, estudio inicial del modelo de negocio de la organización, autorizar y asegurar las pruebas definir el alcance, definir las áreas que no serán alcanzadas, firma del acuerdo, etc. Páginas 61 – 69.
  Además en el capítulo 4 de la metodología se explica la gestión de los acuerdos, objetivos, alcance, etc. para la formalización de un contrato. Páginas 39 – 54.

Reuniones iniciales

Las pruebas de intrusión deben comenzar con una serie de reuniones previas entre los auditores que van a celebrar la auditoria técnica y la organización donde se va a ejecutar la auditoria. Estas reuniones inician la auditoria, de manera que sirve como primera toma de contacto entre las partes, donde se definirán de forma muy general los objetivos de la auditoria. Dado que los test de intrusión pueden causar daños lógicos a los sistemas, y por ende a la actividad del negocio, se debe asegurar y acotar por parte del auditor la autorización explícita por parte de la organización. Esto se formalizara a través de la inclusión de las correspondientes obligaciones, limitación de responsabilidades y exenciones en la fase de actuación.

Revisión de la situación actual y definición del alcance y ámbito

La definición de la situación actual de la empresa permite a los auditores obtener información importante a cerca de la organización donde se desarrollara la auditoria. Se adquirirá información acerca de las políticas de seguridad, estándares y procedimientos fijados y de los controles implantados, pero también se conseguirá información sobre la cultura, hábitos, organigramas, etc. La recopilación de esta información se obtendrá a través de las reuniones iniciales y entrevistas personales. El grado de información que los auditados deben conocer, influye de forma determinante en los actores a entrevistar y la información a obtener.

Toda la información de la organización obtenida ayudará a definir de forma más exacta el alcance que va a tener la auditoria técnica, determinando todo los aspectos que se van a revisar durante la auditoria. En este punto de la fase de planificación se definirá el alcance teniendo en cuenta los siguientes aspectos:

- Ámbito de aplicación de las pruebas, que englobara las diferentes áreas a testear: Infraestructura de red cableada e inalámbrica, sistemas operativos, aplicaciones y servicios locales y Web.
- Objetivos concretos de la organización que deben ser auditados, a través de la realización de las pruebas.
- Tanto las diferentes ubicaciones físicas que se auditaran como las diferentes áreas organizativas de la empresa, ya sea áreas de desarrollo, de *testing* o de producción.
- Tipo de prueba a realizar en función del conocimiento del auditor del entorno a auditar (caja blanca, caja gris, caja negra) y del conocimiento por parte de los técnicos y usuarios de la realización de la auditoría sobre el objetivo (planificada, sorpresiva).

Por tanto, una recopilación adecuada de toda la información y de los aspectos enumerados, permite desarrollar de forma más ágil y concreta la planificación de las pruebas.

Planificación del test

Una vez recogida toda la información necesaria de la empresa, alcance, ámbitos, tipos de pruebas, ubicaciones, información general, etc., en este punto será necesaria la creación de un plan de trabajo. Este plan de trabajo se estudiará y se fijara en función de los datos recabados en las anteriores reuniones y fijación de ámbitos, alcance, etc. El plan de trabajo determinará los recursos que deben estar disponibles y los que serán utilizados (tanto técnicos como humanos), el tiempo de realización estimada y las pruebas que se ejecutaran. Normalmente la designación de auditores y el tiempo de auditoría se definen con

la asignación jornadas/hombre, que variara en función del alcance definido y de la experiencia de los auditores. Todos estos factores influyen mucho en el coste de la auditoria, por lo que deben ser cuidadosamente tratados. Por tanto, el plan de trabajo debe ser adecuado y debe estar optimizado para aprovechar al máximo tanto el tiempo como los recursos de ambas partes.

Propósito final de la fase de planificación

El resultado final de la fase de planificación es la firma por ambas parte de un contrato informático, donde se refleje la conformidad por ambas partes en la realización de la auditoria. En dicho contrato se reflejaran el objeto del mismo, todas las decisiones y acuerdos obtenidos en las reuniones anteriores, el plan de trabajo detallado con plazos concretos, el presupuesto acordado, formas de pago, y las correspondientes clausulas contractuales de derechos, obligaciones, responsabilidades y exenciones de la auditoria.

El contrato deber ser muy minuciosamente redactado, para reflejar perfectamente todos estos aspectos tratados durante toda la fase de planificación y su ubicación dentro del marco legislativo.

II- Fase de actuación

En esta fase del test de intrusión se van a ejecutar la batería de pruebas acordadas en el plan de trabajo, para cubrir el alcance que se haya definido anteriormente. En primer lugar, en función de lo acordado en la fase de planificación, se deben clasificar los ámbitos por diferentes áreas físicas y lógicas orientada a las pruebas. Por tanto, se clasificaran los ámbitos en función del entorno, mecanismos y tecnologías de los sistemas de información (SI) que cubre la metodología, y que se indican a continuación:

1. **Infraestructura de red**:
    - Entornos de red cableada tipo Ethernet: *Router*, *Switcher.*
    - Entornos de red inalámbricas: Puntos AP Wifi, Bluetooth, 3G.
    - Elementos de seguridad: *Firewall*, IDS, IPS, Honey Pots.
    - Accesos remotos: VPN, SSL.
2. **Sistemas operativos** de los SI, tales como las diferentes plataformas, versiones, etc.
3. **Servicios** de los SI, tales como sistemas de gestión de base de datos, servidor de correo electrónico, servidor FTP, servidor Web, servidor de DNS, etc.
4. **Aplicaciones** de los SI, tanto locales como con ámbito Web.

También es importante remarcar el tipo de test de intrusión seleccionado, que se determina en función del conocimiento que tiene el auditor y los departamentos auditados. En este caso se va a utilizar los siguientes tipos de pruebas:

- **Test de caja negra**: El auditor no tiene ningún conocimiento de la infraestructura de red de datos ni de los objetivos que tienen que ser alcanzados. En este tipo de prueba se ubicara al auditor fuera del perímetro de seguridad, por lo que solo se dispone de la información de acceso público. Este tipo de prueba simula una intrusión más real que el resto de las pruebas, dado que consiste en acceder de forma remota a los sistemas de la organización y obtener privilegios que no deberían estar disponibles desde el exterior. Habitualmente, solo unos pocos trabajadores de la organización auditada conocen la realización de la prueba.
- **Test de caja blanca**: El auditor recibe una amplia información acerca de la organización tanto a nivel de organizativo (estructura, departamento) como de la topología de los elementos de red y de los dispositivos a testear (S.O., Firewall, *routers*, BBDD, etc.). En este tipo de prueba se ubicará al auditor con privilegios de acceso a la red interna como usuario estándar, para acceder a los recursos del sistema a auditar, simulando un ataque realizado internamente. Este tipo de prueba supone un estudio exhaustivo y minucioso de la seguridad del sistema objetivo. Habitualmente se colabora activamente con trabajadores de la organización auditada.
- **Test de caja gris**: Este tipo de prueba es una combinación de las pruebas de caja negra y caja blanca. El auditor habitualmente recibe algo de información de los elementos y servicios a testear, pero bastante limitada. Para lograr su objetivo debe utiliza las técnicas de caja negra desde el exterior, pero con el conocimiento privilegiado de información que ha sido previamente comunicado por la organización.

La definición de los ámbitos, tecnología y tipos de pruebas va a condicionar la manera en la que se realicen las pruebas. Por tanto, antes de comenzar con los pasos de la metodología se debe determinar claramente lo ámbitos y tipos de test, cubriendo adecuadamente el alcance del test de intrusión. En la figura 3.2 se muestran todos los tipos de auditoría y todos los ámbitos a investigar en esta metodología.

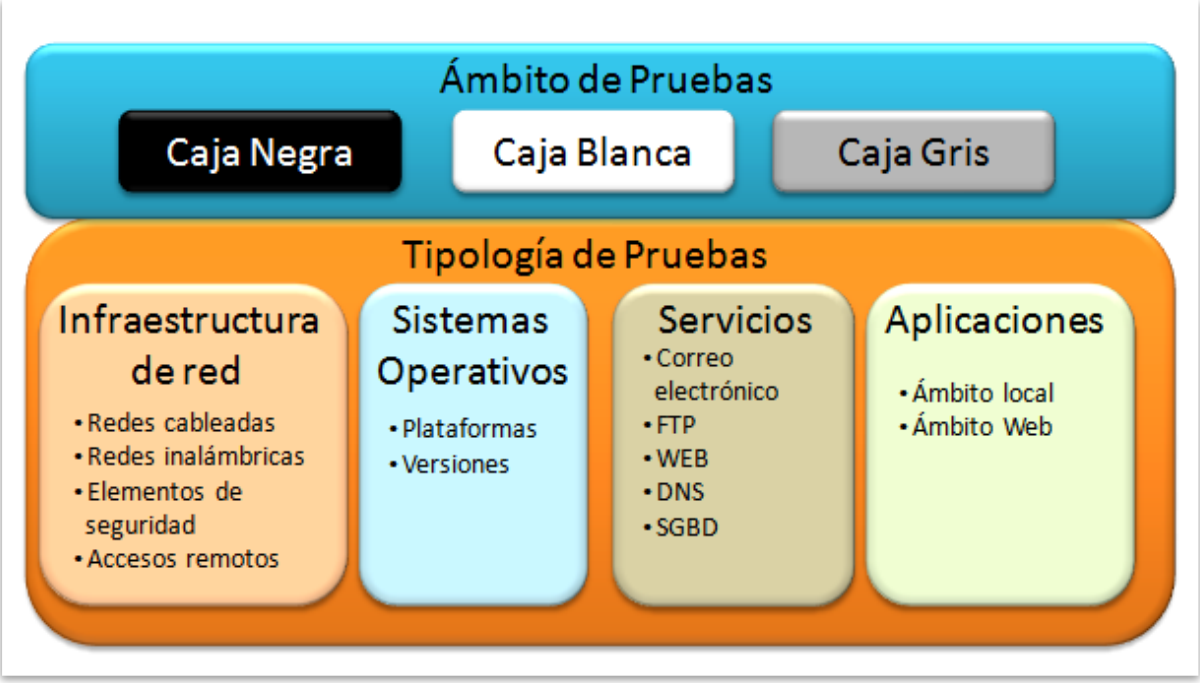

Figura 3.2. Tipos y ámbitos acordados sobre el alcance de las pruebas

En cuanto a cómo se plantea en las metodologías estudiadas anteriormente, se pueden referenciar los siguientes puntos de estas:

- **OSSTMM Vers.3.0** [1]: Capítulo 6 – *Workflow*. En este capítulo se explica la metodología propuesta por OSSTMM para el test de penetración. Esta metodología se expuso en el capítulo 2 del presente trabajo. Páginas 96 – 103.
  La metodología se ubica en los diferentes ámbitos de utilización de la misma, sin entrar en detalles muy concretos para la realización de las pruebas. Los ámbitos que tienen relación con los que se cubren en la nueva metodologías son:
  - Capítulo 9 – *Wireless Security Testing (SPECSEC)*. Se enumera de forma genérica el entorno de comunicaciones inalámbricas. Páginas 138 - 150.
  - Capítulo 11 – *Data Network Security Testing (COMSEC).* Se cubre de forma genérica el entorno de comunicación de datos en las redes de organizaciones. Páginas 167 - 183.

- **ISSAF Vers. 0.2.1** [2]: Capítulo B.2 - *Phase II – Assessment*. En este capítulo se explica de forma genérica la metodología propuesta por ISSAF para la fase de valoración del test de penetración. Esta metodología se expuso en el capítulo 2 del presente trabajo. Página 136 – 145.
  En el capítulo C – *Penetration Testing Methodoly, Phase II, Explained* se explica la metodología de forma detallada en cada una de las fases expuestas en el capitulo B.2. La exposición es muy detallada con los objetivos, metas y resultados

que deben ser obtenidos explicados de una manera muy clara y con ejemplos de herramientas y técnicas utilizadas. Páginas 147 – 289.

Los ámbitos con relación con los que se cubren en la nueva metodologías son:

- Capítulo E – *Password Security Testing.* Se cubren las técnicas y métodos para las pruebas de seguridad a nivel de contraseñas. Páginas 294 – 358.
- Capítulo F – *Switch Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad a nivel de *switcher* (Capa 2 del modelo OSI). Páginas 359 – 393.
- Capítulo G - *Router Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad a nivel de *router* (Capa 3 del modelo OSI). Páginas 394 – 435.
- Capítulo H – *Firewall Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de los elementos de seguridad *firewall*. Páginas 436 – 482.
- Capítulo I – *Intrusion Detection System Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración los elementos de seguridad IDS. Páginas 483 – 505.
- Capítulo J – *VPN Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad de las conexiones VPN. Páginas 506 – 515.
- Capítulo M – *WLAN Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad de las conexiones WLAN. Páginas 539 – 560.
- Capítulo Q – *UNIX/Linux System Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad de los sistemas operativos basados en UNIX y Linux. Páginas 598 – 635.
- Capítulo R – *Windows System Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad de los sistemas operativos de la familia de Windows. Páginas 636 – 703.
- Capítulo T – *Web Server Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad de los servidores Web. Páginas 707 – 718
- Capítulo U – *Web Application Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad de las aplicaciones Web. Páginas 719 – 779.
- Capítulo V – *Web Application Security Assessment – SQL Injections.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad

de las aplicaciones Web a través de ataques hacia vulnerabilidades por inyección de código SQL. Páginas 780 – 807.

- Capítulo Z – *Database Security Assessment.* Se cubren las técnicas y métodos para las pruebas de valoración de seguridad de las bases de datos. Páginas 835 – 883.

- **Guía de pruebas de OWASP Ver 3.0 (Castellano)** [3]: Capitulo 4 – *Pruebas de Intrusión de Aplicaciones Web*. En el capítulo se explica de forma muy detallada las pruebas de intrusión de aplicaciones Web. Esta metodología se expuso en el capítulo 2 del presente trabajo Páginas 53 – 341.

A continuación se van a exponer las diferentes fases de la metodología para la realización de las pruebas de intrusión.

Recopilación de información del SI

El objetivo de este primer paso en la fase de actuación es la de recopilar toda la información que sea posible y útil del entorno del sistema auditado y de los objetivos marcados, así como del resto de sistemas que interactúan con los objetivo. Esta fase es fundamental para la realización con éxito de las posteriores pruebas de análisis, dado que un estudio exhaustivo del objetivo y de su entorno permite una mejor valoración de la situación real, la planificación de los ataques y de posibles inconvenientes en la realización de las pruebas. Un factor muy importante a la hora de ejecutar esta fase, es la cantidad de tráfico de red y accesos a sistemas que se puede generar, ya que tales evidencias pueden ser detectadas por los administradores de los sistemas auditados. Dependiendo del tipo de auditoría que se realice, esta información puede ser fundamental para obtener el éxito de las pruebas.

Este paso de recopilación se puede dividir en 2 aspectos: uno destinado a la recolección de información pública del sistema y objetivos a auditar (*footprinting*), y otro encargado de la obtención de información muy concreta (*fingerprinting*) de los elementos de red, sistemas, mecanismo de seguridad, versiones de los sistemas, etc. En la figura 3.3 se muestran ambas fases condicionadas y ejecutadas en función de los ámbitos y tipos de prueba.

Figura 3.3. Etapas que componen la recopilación de Información

Recolección información (*FootPrinting*): La recolección de información está basada en la utilización de Internet para la obtención de toda la información pública posible sobre el objetivo definido. Para ello se utilizan técnicas basadas en DNS, WHOIS, protocolo ICMP, etc. que permitan consultar las bases de datos publicadas y así conseguir información de dominios y direcciones IP. Para la realización de este punto se utilizaran las siguientes técnicas o tipos de herramientas:

- Técnicas avanzadas en buscadores (Google, Bing), utilizando parámetros para dirigir y filtrar búsquedas y obtener información indexada por estos.
- Paginas especializadas (www.netcraft.com, www.goolag.org, www.kartoo.org) donde se complementara la información de dominios y servidores DNS obtenida en los buscadores.
- Herramientas diseñadas para realizar las funciones anteriores de manera controlada y automática (Maltego, Netglub, Plug-in Firefox, Optos, Foca, Anubis).
- Herramientas creadas para el descubrimiento del sistema operativo, modelo y estructura de directorios de un servidor Web o FTP (Anubis, DirBuster). También se puede utilizar herramientas para la descarga completa o parcial de los ficheros del sitio Web (Wget, Teleport).
- Herramientas para la extracción de los metadatos de los documentos de los sitios Web, FTP, etc. Existen tanto sitio Web como herramientas que automatizan esta tarea (Foca, Anubis).

Esta fase es una de las que más tiempo consume en la prueba de intrusión. El resumen de estas actividades se puede observar en la figura 3.4.

Figura 3.4. Etapas que componen la recopilación de información pública

Este punto podría orientarse a la obtención de información del las personas físicas que trabajan o colaboran en la organización, explotando la técnica de ingeniería social, pero este aspecto no se cubrirá en esta metodología, al menos en este trabajo inicial.

El reconocimiento que se realiza en este punto es totalmente pasivo y no intrusivo, por lo que habitualmente no es necesario el conocimiento por parte de la organización. Este punto puede ser realizado tanto en las auditorias de tipo caja blanca o de caja negra, pero en este

último caso, esta fase de reconocimiento es fundamental para las fases posteriores. El objetivo final como se decía anteriormente, es la obtención de información que sea útil en sucesivas fases.

La información que puede obtenerse en esta fase es:

- Fuentes de información en Internet.
- Direcciones físicas, rangos y direcciones IP públicas, nombres de dominio, maquinas conectadas al dominio y direcciones IP privadas.
- Información de registro de servidores de nombres (NS) y de intercambio de correo (MX).
- Números telefónicos, nombres de personas, usuarios, perfiles, cargos, y cuentas de correo electrónico.
- Información de blog o páginas Web sobre la organización.
- Información y ficheros de las páginas Web institucionales e Intranet corporativa.
- Información del código fuente de elementos Web públicos.
- Estructura de directorios en servidores Web y FTP y elementos permitidos.

Sondeo y enumeración (*Fingerprinting*): El sondeo y la enumeración es también un punto fundamental para la adecuada ejecución de las posteriores fases de análisis y explotación de vulnerabilidades. Por un lado, el sondeo es una actividad que consiste en que de una manera activa se intenta la conexión a cada uno de los sistemas para provocar una respuesta y extraer la información de esta consulta. Por otro lado, la enumeración se utiliza para obtener información detallada y precisa sobre el objetivo. Esta actividad habitualmente forma parte de la información obtenida en el punto anterior de recolección de la información, con el objetivo de detectar posibles vectores de ataque que serán explotados más adelante.

Habitualmente en la **fase de sondeo** se intentara detectar que sistemas están activos, se escanearan los puertos, se detectara que sistema operativo y versiones tiene el sistema instalado, se identificaran que servicios están siendo ejecutados, que aplicaciones han sido instaladas y se intentare crear un mapa de la infraestructura de red. Las herramientas que se utilizan para detección y obtención de información suelen cubrir todas estas acciones a través de diferentes módulos o del uso de otra herramienta especializada (nmap, netcat, hping, traceroute).

Para la realización de este punto se utilizaran las siguientes técnicas, módulos o tipos de herramientas:

- Técnicas para la detectar si el host esta activo, utilizando para ello el envió de paquetes ICMP y la detección de respuesta.

- Para el sondeo de puertos suele utilizarse un modulo o herramientas de escaneo de puertos, que sirven para la detección del estado de los puertos de un sistema y por ende de los servicios que están conectados a la red de datos. De esta manera, se puede determinar el estado de un puerto concreto, ya sea abierto, cerrado o protegido por cortafuegos. A partir de estos puertos abiertos, se asociaran los mismos a las aplicaciones o servicios que el sistema está ejecutando. La base de estas herramientas es la utilización de las características de los *flags* de los protocolos de transporte TCP y UDP, tales como SYN, ACK, PSH, URG, FIN, y RST.
- Análisis de las respuestas del *host* ante el envió de determinados paquetes de datos, para detectar el sistema operativo instalado en el sistema. Este proceso se basa en las diferentes formas de implementar los protocolos de transporte de cada uno de los sistemas operativos.
- Identificación de servicios que están ejecutándose en el sistema. Esta información se obtendrá a partir de la técnica de *banner grabing*, que permite la identificación de los servicios, leyendo los *banner* que las aplicaciones responden ante ciertas peticiones. Aquí se podrá obtener información de las versiones, arquitectura, parches, *service pack* de los sistemas operativos y de las aplicaciones instaladas.
- Para la realización de un mapa de la topología que presenta la infraestructura de red y de los sistemas instalados en la misma, se utilizaran todos los datos recopilados en los pasos anteriores a este. Además se intentan identificar tanto *routers*, *switcher* como *firewall*, IDS, *proxies*, etc. utilizando diferentes técnicas que permite recoger información de redes protegidas por *firewall*, topologías, etc.
- En el caso de que el ámbito cubra las redes inalámbricas, será necesaria la obtención de información de las redes inalámbricas utilizadas en la empresa. La detección de las mismas será físicamente una vez dentro de la organización, o en las cercanías, para la obtención de la cobertura necesaria para la realización de las pruebas. La información que es hay que obtener de las redes WiFi de la organización son datos tales como SSID, BSSID, canal de comunicación, algoritmo de cifrado (WEP, WPA, WPA2). Para ello se utilizaran herramientas de detección y conexión de redes inalámbricas habitualmente basadas en distribuciones Linux (wicd de la distribución de LINUX-WIFISLAX).

Por otra parte, la **fase de enumeración** se basa en las prestaciones que los servidores dan a los usuarios en forma de servicios y recursos disponibles para que estos puedan utilizarlos. El objetivo de esta técnica es por tanto la obtención de la información relativa a todos estos recursos y servicios compartidos, y el descubrimiento de los usurarios que acceden a los mismos. Para realizar esta actividad será necesaria la generación de

conexiones activas con cada sistema objetivo y la consulta directa de esta información. La consulta que se hace es directa al sistema objetivo de una manera activa, por los que estos intentos pueden quedar registrados y ser detectados por los administradores del sistema. Dependiendo del sistema operativo (Windows, Linux, Unix, Mac) que tenga instalado cada sistema se utilizaran técnicas y herramientas diferentes (telnet, netcat, LANguard, NetBruta, SuperScan, Hyena) a la hora de enumerar. Todas estas técnicas se basaran los protocolos que permiten la obtención de información útil, tales como NetBIOS, SNMP y LDAP.

Para la realización de este punto se utilizaran las siguientes técnicas, módulos o tipos de herramientas:

- Obtención de información a través del protocolo NetBIOS, tales como recursos compartidos de los sistemas, dominios accesibles, sistemas y recursos compartidos dentro de los dominios accesibles y controladores de dominio (net view).
- Adquisición de información utilizando el protocolo SNMP, sobre todo en equipos tales como *routers*, *switchers*, servidores de impresión, etc. La información que se puede obtener son datos de la base de datos SNMP e interfaces instalados. (SNMPc Network Manager).
- Obtención de datos de información desde un directorio jerárquico a través del protocolo LDAP, ya sea en un sistema con *Active Directory*, *OpenLDAP* o servidor *NIS*. La información que puede obtenerse son nombres de usuario, ficheros, carpetas y atributos (ldp).
- Enumeración de información de los registros, donde se pueden mostrar información de hardware software y instalado, configuraciones de los programas, programas ejecutados al inicio, etc.

Por último, dentro de esta fase de sondeo y enumeración, cuando se realiza una prueba de intrusión de caja blanca (si se utilizase en caja negra habría que acceder e instalarlo en alguna maquina victima dentro de la red interna) se utilizara también la técnica de *fingerprinting* pasiva. Esta técnica consiste en la captura de paquetes de la red de comunicaciones cableada. Para realizar esta actividad se utilizan herramientas de captura de paquetes de red, habitualmente denominadas herramientas de *Sniffing* (WhireShark, Cain&Abel, Satori, Yersinia). En los entornos de *switching*, solamente se envía la información por el puerto adecuado, salvo los paquetes de *broadcast*. A partir de estos paquetes *broadcast* retransmitidos se puede obtener información muy útil, tales como identificar sistemas operáticos, obtener paquetes de los protocolos HPSP, CPD, DHCP, SMB y de protocolos de *enrutamiento* como OSPF y EIGRP. La técnica de *sniffing* al ser completamente pasiva aporta una gran transparencia de cara a firewall, IDS e IPS en la red en la que se encuentra escuchando, por lo que es una buena opción para no ser detectado.

El resumen de estas actividades se puede observar en la figura 3.5.

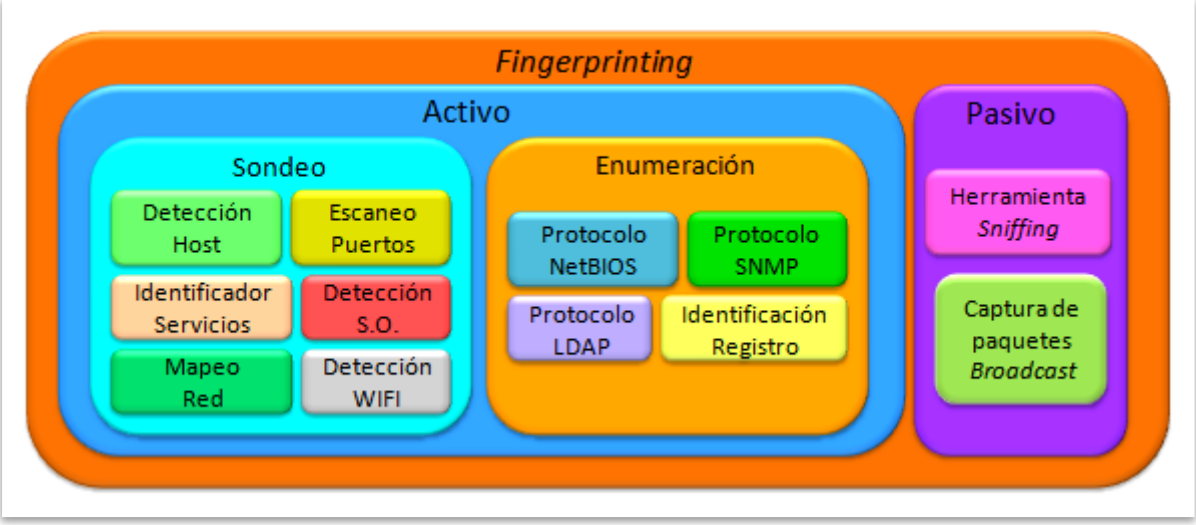

Figura 3.5. Etapas que componen la actividad *Fingerprinting*

El reconocimiento que se realiza en este punto es eminentemente activo (*fingerprinting* activo), salvo en el caso de la captura de paquetes, y en algún caso incluso podría ser intrusivo, como en los casos de caja negra. De esta forma se están aumentando las probabilidades de ser detectados. Esto implica la adecuada habilidad y diligencia del auditor para no ser descubierto, y para no provocar ningún daño lógico, que influya en el buen funcionamiento de los sistemas TI, y por ende en la actividad normal de la organización.

Al igual que en la etapa de *footprinting*, la etapa de *fingerprinting* etapa puede ser realizada tanto en las auditorias de tipo caja blanca o de caja negra, pero en este último caso, se presenta una mayor dificultad, dado que la actividad puede ser intrusiva en función del objetivo a acceder y de la distribución de la infraestructura de la red de comunicaciones.

La información que puede obtenerse en esta fase es:

- Rangos, sub-rangos, y direcciones IP de sistemas y elementos de red.
- Detección de hosts activos, detección y análisis de servicios activos y de sistemas operativos.
- Información de los elementos de protección de red instalados, de los tipos y versiones de *firewall*, IDS, IPS, *honey pot*, *honey nets*, *proxies*.
- Información de los sistemas operativos, servicios y aplicaciones instaladas en los diferentes sistemas y las versiones que tiene estos.
- Detección de redes WiFi y *bluetooth* y determinación de mecanismos de criptografía en redes Wi-Fi.
- Relevamiento de aplicaciones y servicios Web, correo, telnet, ftp, SSH, https.

- Listado de sistemas instalados en la red, recursos compartidos en red, dominios internos accesibles, sistemas en dominios accesibles y nombres de cuentas de usuario.
- Captura y análisis de trafico sin cifrar, para corroboración y adquisición de nueva información.

Análisis de vulnerabilidades (*Vulnerability Assessment*): El análisis de vulnerabilidades es el siguiente paso en la fase de actuación. Una vez que se ha recopilado toda la información posible, que es útil para detectar las vulnerabilidades que presentan los objetivos a testear, se utilizaran diferentes técnicas, mecanismos y herramientas en función de los objetivos y límites marcados en la auditoria para llevar a cabo este paso.

En primer lugar es necesario crear un listado ordenado y clasificado con todos los datos que han sido recopilados. Se indicara el tipo de dispositivo, datos completos del sistema operativo, servicios ejecutados, aplicaciones instaladas, datos de interfaces de red, funcionalidad dentro del sistema, etc. Estos datos serán listados como un inventario de dispositivos, y a partir de este listado y de la información recabada, se intentara diseñar un esquema de la infraestructura de red. Este esquema debe permitir la visualización de la ubicación, funcionalidad y elementos de software y hardware asociados e instalados, para posteriormente realizar análisis profundo de las vulnerabilidades que pueden presentan cada uno de estos dispositivos.

A continuación se determinara la existencia de vulnerabilidades conocidas utilizando herramientas automáticas, que permiten identificar las posibles vulnerabilidades que presentan los elementos de red y sistemas. Estas herramientas de detección automática de vulnerabilidades (OpenVas, Nessus. Saint, GFI Languard, Saint, WatchFire, hackvertor, Nikto, WFuzz) sondean estas posibles vulnerabilidades a partir de los datos que ellas recopilan sobre los sistemas operativos, servicios y aplicaciones, tanto de ámbito local como Web. Esta actividad tiene como objetivo la identificación de debilidades tales como:

- Versiones antiguas e inseguras que han sido descatalogadas.
- Falta de instalación de parches y actualizaciones de seguridad.
- Configuraciones por defecto y errores de configuración.
- Usuarios, perfiles y contraseñas débiles o por defecto.
- Listas de control de acceso, reglas o componentes de autenticación mal configurados.
- Identificación de fallos de punto único.
- Dependencias entre componentes o sistemas en las relaciones de confianza.
- Incorrecta funcionalidad y rendimiento en el uso de las políticas de seguridad.

Las herramientas automáticas solamente detectan vulnerabilidades conocidas, que han sido previamente publicadas en las bases de datos públicas de vulnerabilidades y que son introducidas en las herramientas como medio de conocimiento a la hora de aplicar las reglas. Es importante comprende el funcionamiento, posibilidades y limitaciones de un escáner de vulnerabilidades, a la vez que la utilización de varios tipos de escáneres en función del ámbito que cubra el alcance de la prueba. Las características que deben presentar este tipo de herramientas son:

- Identificar un subconjunto de vulnerabilidades de seguridad.
- Permitir la configuración de las diferentes opciones en función del entorno y tipo de auditoría que se realice.
- Generar informes que detallen cada vulnerabilidad que ha sido detectada.
- Presentar un aceptable ratio de falsos positivos.

Otro aspecto a destacar es la dificultad que implica la detección de vulnerabilidades aun desconocidas, que requieren de otro tipo de técnicas, habilidades y experiencia para su descubrimiento por parte del auditor.

La utilización de este tipo de herramientas, al igual que en la fase de *fingerprinting*, genera mucho tráfico de red y un gran número de conexiones sobre los sistemas. Estas acciones puede pueden ser detectadas por los administradores, o en el peor caso posible, si no se configurasen adecuadamente, podrían incurrir en un ataque de denegación de servicios. Por lo tanto el auditor debe ser muy cuidadoso a la hora de gestionar estos dos matices.

A partir de la información inventariada y de la nueva información obtenida a través de las herramientas de escaneo, las vulnerabilidades deben ser enumeradas para una planificación adecuada de la posterior fase de explotación de las mismas. En este listado se debe estimar de manera genérica el riesgo técnico y posible impacto que produciría la explotación de cada una de las vulnerabilidades (clasificándolo en función de su criticidad), el vector de ataque que puede ser utilizado y los escenarios donde podría ser explotada.

La planificación de la explotación de las vulnerabilidades permitirá una adecuada y eficiente ejecución de esta posterior etapa, permitiendo la correlación entre las vulnerabilidades recopiladas con el resultado del escáner automático y la posterior comprobación de la vulnerabilidad en la fase de explotación. Esta actividad por tanto proporcionara la enumeración y corroboración de falsos positivos que las herramientas automáticas presentaron en forma de vulnerabilidades detectadas.

La figura 3.6 muestra cada uno de las etapas del análisis de vulnerabilidades.

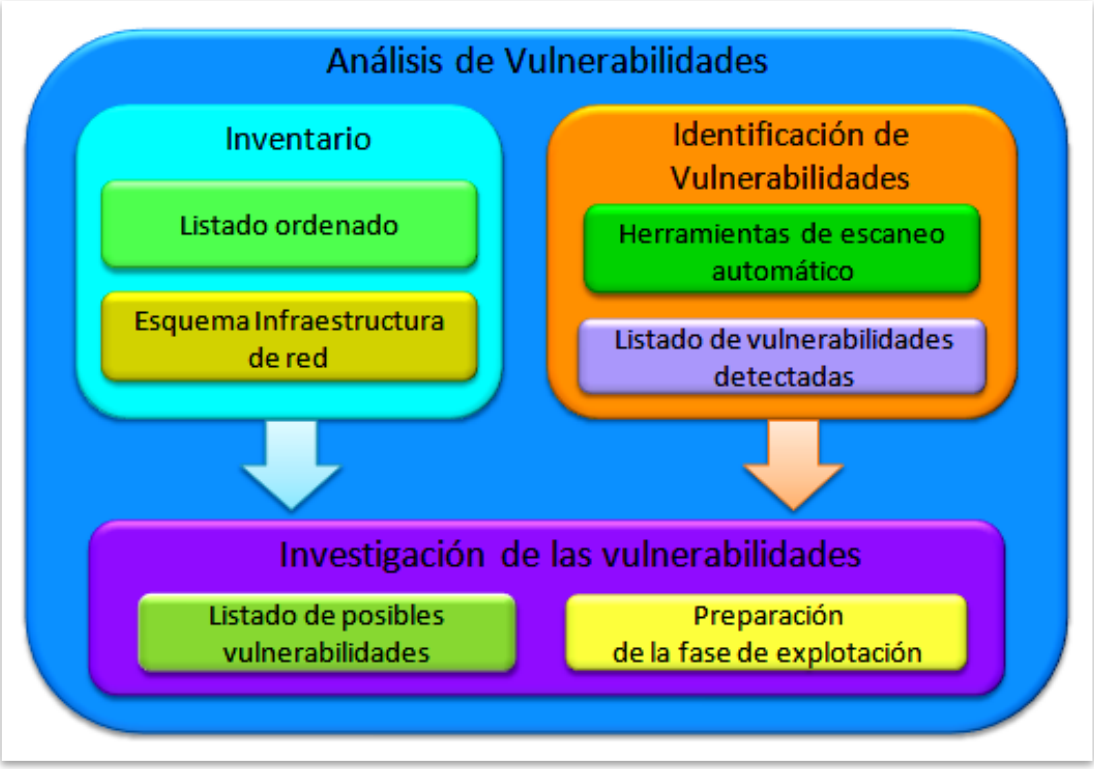

Figura 3.6. Etapas que componen el análisis de vulnerabilidades

En una prueba del tipo *Vulnerability assement*, la fase de actuación terminaría aquí, obteniendo los resultados y generándose un informe final. Sin embargo en un test de intrusión deben explotarse las vulnerabilidades encontradas, tal y como se realizara en la posterior etapa de explotación de vulnerabilidades.

La información que puede obtenerse en esta fase es:

- Vulnerabilidades de seguridad en accesos de modo remoto.
- Vulnerabilidades de seguridad en elementos de la red de comunicaciones cableada (*switcher*, *router*) e inalámbrica (PA WiFi).
- Vulnerabilidades de seguridad en estaciones de trabajo y servidores.
- Grado de eficacia de la funcionalidad y vulnerabilidades de elementos de seguridad de red (*firewall*, *proxies*, IDS, IPS)
- Vulnerabilidades de seguridad en sistemas de gestión de bases de datos.
- Vulnerabilidades de seguridad en aplicaciones de ámbito local o ámbito Web, ya sea en Intranet o en Internet (Web, correo, telnet, ftp, SSH, https, etc.).

Explotación de vulnerabilidades e intrusión: Esta es la última etapa de la fase de actuación. De forma genérica esta actividad consiste en la explotación de las vulnerabilidades encontradas en la etapa anterior, permitiendo la eliminación de falsos positivos y la posterior intrusión en cada uno de los sistemas que presenten vulnerabilidades explotables. Una vez consolidada la intrusión en uno de los objetivos, se obtendrán las evidencias que demuestren la existencia de las vulnerabilidades explotadas y se intentara escalar los privilegios para aumentar los permisos y acceder a cada uno de los sistemas que son objetivo de la auditoria.

Opcionalmente, en función del tipo de auditoría y del alcance pactado contractualmente con la organización auditada, se podrán utilizar técnicas *hacking* para mantener el posterior acceso a los sistemas (*sniffer*, *keylogger*, *rootkit*, etc.) y la eliminación de las huellas, borrando la información de los registros de cada una de las intrusiones.

Por tanto, esta última etapa de la fase de actuación mostrara el impacto real de cada uno de los ataques simulados sobre los sistemas, obteniendo una visión realista de la seguridad implantada en el momento de la auditoria.

Es importante resaltar la necesidad de tomar una serie de precauciones a la hora de realizar esta última etapa, que debería haberse reflejado y detallado en la fase de planificación cuando se redactó el contrato de la auditoria técnica. Las medidas de prevención a tomar durante esta etapa son entre otras, la prevención ante bloqueos e inestabilidades de los diferentes servicios y sistemas, preservación del rendimiento y de la funcionalidad de los sistemas y dispositivos de red, confidencialidad sobre la información sensible obtenida durante la intrusión y resguardar la integridad de los sistemas auditados.

La primera parte de esta etapa comienza con la lectura del informe donde se listan las vulnerabilidades encontradas, y donde se indica la planificación para la explotación de las mismas. A partir de este informe se verificará la existencia de dichas vulnerabilidades, corroborando y disociando las vulnerabilidades reales de las que son falsos positivos. Por lo tanto, en este paso es posible la explotación y ataque de las vulnerabilidades detectadas e incluso de las no detectadas, dependiendo del conocimiento, pericia y metas del auditor. Para la explotación de las vulnerabilidades se utilizaran un conjunto de técnicas y herramientas de *hacking* ético, que pueden ser ejecutadas de forma manual o automática. Estas técnicas y herramientas son usadas habitualmente por atacantes reales para obtener acceso a los sistemas. Para cada una de las vulnerabilidades se utilizara un *exploit* concreto que explote la misma. Se puede definir *exploit* como el código o secuencia de comandos que es capaz de intencionadamente causar un comportamiento que no es deseado, ya sea en una aplicación o en un sistema. Este comportamiento permitirá cambios en el flujo de

ejecución del código y la obtención de un beneficio por parte del ejecutor del *exploit*. Estas herramientas o *Frameworks* (Metasploit Framework, Core Impact, Immunity Canvas, Saintexploit, Inguma, Karma) permiten probar los controles de seguridad implantados y atacar los sistemas a través de secuencias controladas de ataques de las vulnerabilidades propias de los sistemas identificados.

Posteriormente, una vez consumado el éxito en la utilización del *exploit*, se va a obtener acceso a los sistemas y dispositivos. Este acceso se llevara a cabo sobre los elementos que presentan más debilidades y que son más sencillos de explotar, como son las cuentas de usuario con mínimos privilegios. Dependiendo del tipo de auditoría, será necesaria la ocultación de la intrusión dentro del sistema, para pasar lo más desapercibidamente posible ante los administradores y usuarios del sistema.

Una vez que se ha accedido a un sistema objetivo, habitualmente con las mínimas credenciales, es necesaria la colonización del resto del sistema, obteniendo un escalado de privilegios. Habitualmente esta acción se lleva a cabo utilizando un *exploit* local que permita la obtención de las credenciales de usuarios con altos privilegios, tales como el usuario administrador (*root*). Para la consumación de este escalado se utilizaran técnicas y herramientas especializadas en estas labores a nivel de maquina local (John The Ripper, THC-Hidra, Medusa, Ettercap, Scapy/Scruby, Rainbowcrack, NTLM). Esto permitirá el control total del sistema colonizado y un mayor acceso a los recursos y sistemas que están en la red interna. De esta forma se irá invadiendo poco a poco y de forma prudente y sigilosa, cada uno de los objetivos marcados en el alcance de la auditoria.

Las técnicas *hacking* utilizadas para la explotación de vulnerabilidades, intrusión y escalado de privilegio son las siguientes:

- Desbordamientos de buffer, desbordamiento de enteros, desbordamiento de memoria dinámica, *Format String*.
- Secuestro de sesiones.
- Técnicas de *fuzzing* para la comprobación de entradas no esperadas y el análisis de las excepciones.
- Explotación con inyección de secuencias de datos sobre entradas que no están correctamente validadas, tales como SQL *Inyection*, XPath *inyection*, XML *inyection*, SSI *inyection,* LDAP *inyection,* MX *inyection,* HTTP *inyection.*
- Explotación de vulnerabilidades clásicas en sitios Web*, Cross-Site Scripting,* HTTP *Response Splitting*, *Cross-Site Request Forgery*, etc.

- Redirección del tráfico y captura de la información a nivel de capa de enlace con la técnica denominada *ARP Poisoning* o a niveles de aplicación con técnicas de *Man In The Middle.*
- Ataques de fuerza bruta o de diccionario sobre los servicios y los mecanismos de autenticación para acceder a sistemas objetivos.
- Explotación de los mecanismos de cifrado de la red Wi-Fi y posterior captura del tráfico de los sistemas de usuario conectados a la red.

Por último y de forma opcional, ya que dependerá del alcance y del tipo de auditoría que se haya consensuado, será necesario el mantenimiento del acceso y el borrado de las evidencias que puedan demostrar que se ha realizado la intrusión. El mantenimiento del acceso, permitirá un futuro ataque y explotación de vulnerabilidades en otros sistemas con más privilegios o información más relevante, que este dentro del objetivo de la auditoria. Esta permanencia futura se realizará a través de la instalación de aplicaciones (VNC, BO2k, hxdef, Adore-ng, netcat, CryptCat, nstx, socat, icmptx), que habitualmente son maliciosas y que son utilizadas también por atacantes reales. Las aplicaciones típicas que realizan este tipo de acciones son entre otras: puertas traseras, *sniffers*, *keylogger*, *spyware*, troyanos, *rootkit*, etc. En este punto será importante utilizar técnicas para evitar ser detectados tanto por usuarios y administradores, así como por sistemas antivirus, IDS, IPS, etc.

Para la eliminación de las huellas del medio utilizado, del acceso consumado y de las acciones realizadas, y por tanto evitar el descubrimiento del ataque por parte de los usuarios o administradores de los sistemas atacados, es importante la eliminación o modificación de los registros de eventos (*logs*), y de cualquier evidencia que pueda delatar dicha intrusión. Para realizar esta acción suele recurrirse al uso de *rootkit* u otras herramientas que permitan borrar las evidencias de las actividades realizadas.

La figura 3.7 muestra cada uno de las etapas de la fase de explotación de vulnerabilidades e intrusión en los sistemas.

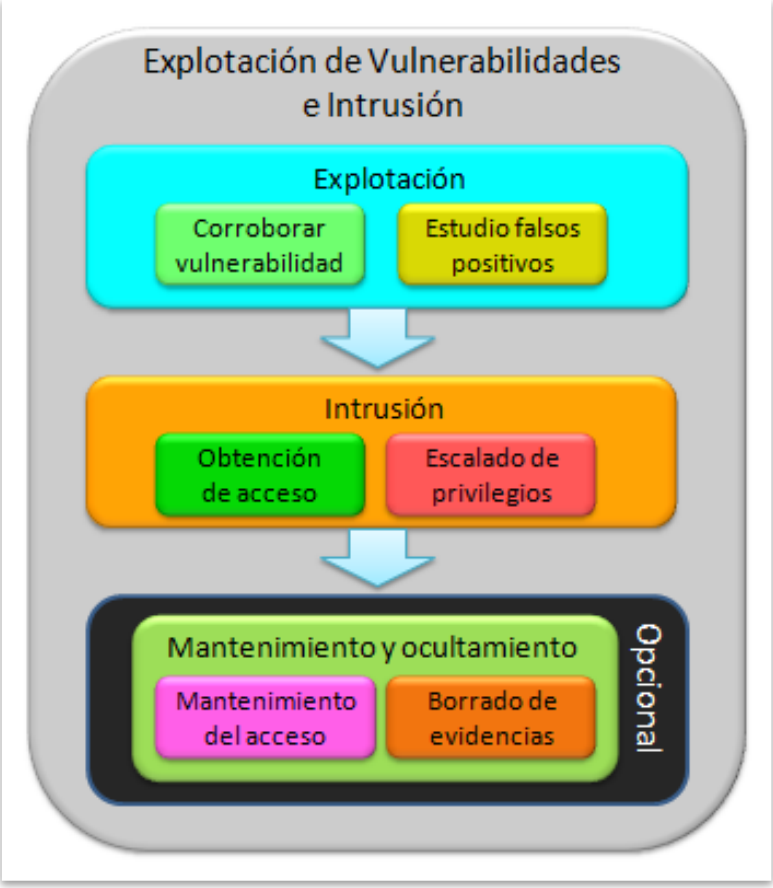

Figura 3.7. Etapas que componen la explotación de vulnerabilidades e intrusión

Esta fase por tanto presenta como objetivo principal la ejecución de las siguientes acciones:

- Explotación de las vulnerabilidades detectadas, ya sea dentro de la red interna o utilizando el acceso remoto.
- Intrusiones vía *switch*, *router*, punto de acceso, web, ftp, telnet, servidor de autenticación o de acceso, SSH, https.
- Escalada de privilegios.
- Combinación de vulnerabilidades para elevar el control.
- Acceso a información interna.
- Generación de evidencia de expuestos detectados.

Propósito final de la fase de actuación

La fase de actuación debe terminar con la recopilación de todos los resultados y comentarios obtenidos durante la realización de las pruebas. Estos resultados servirán para la correcta redacción del informe final que se desarrollara en la siguiente fase. Por tanto, el resultado final de esta etapa es un documento de comentarios y evidencias con cada una de las pruebas realizadas en cada ámbito, las vulnerabilidades detectadas, que vulnerabilidades son falsos positivos, que herramientas han sido utilizadas, si las

vulnerabilidades han podido ser explotadas y un resumen con la presentación de los resultado y las alarmas. Este documento es íntegramente técnico, y será la base tanto para el informe ejecutivo como del informe técnico. A partir este documento se obtendrán y expondrán las conclusiones y las recomendaciones necesarias.

III – Fase de generación de informes

La fase de generación de informes es la fase final de la auditoria, y es imprescindible darle la importancia necesaria, dado que esta fase muestra un resumen de la realización de la auditoria, las metodologías utilizadas, los resultados obtenidos a partir de los hallazgos encontrados, las conclusiones obtenidas y las recomendaciones de subsanación.

Estos resúmenes deben ser generados y presentados a la organización que ha contratado la auditoria de una forma clara y ordenada, para que su comprensión sea la adecuada por todos los actores involucrados y justifique la realización de la misma. Habitualmente suele crearse un borrador que se entrega al auditado, para informar previamente de los hallazgos y conclusiones, y obtener la realimentación por parte de la organización. De esta manera las conclusiones serán aceptadas o se presentarán de alegaciones sobre las mismas, antes de la redacción del informe final. Esta última fase se divide en la generación de 2 tipos de informes diferentes, uno enfocado a la alta dirección y otro orientado al personal técnico.

En cuanto a cómo se plantea en las metodologías estudiadas se puede referenciar a los siguientes puntos de la misma:

- **OSSTMM Vers.3.0** [1]: Capítulo 13 – *Reporting with the STAR* Se explica cómo redactar el informe ejecutivo y se ofrece una plantilla para realizar el resumen general. Se aporta un cuestionario con cada uno de los puntos a tratar en la metodología. Páginas 192 – 202.
- **ISSAF Vers. 0.2.1** [2]: Capítulo 5.3.1 a 5.3.2 – *Phase III – Post-Assessment.* En este apartado de la metodología se explica la última fase de la misma, posterior a la valoración. Se expone la forma de realizar los informes y la presentación de los mismos ante los responsables de la organización. Páginas 82 – 85.
- **Guía de pruebas de OWASP Ver 3.0 (Castellano)** [3]: Capitulo 5.2. – *Como Escribir el Informe de Pruebas*. Se explica de forma muy resumida como redactar el informe final de las pruebas realizadas. Se añade un cuestionario con cada una de las pruebas a realizar. Páginas 354 – 358.

Informe ejecutivo

El informe ejecutivo debe ser redactado de forma breve y comprensible, para que sea entendido por parte del personal que no sea experto en la tecnología ni en la seguridad informática, sin incluir tecnicismos. Este informe está orientado a la alta dirección de la organización y a los departamentos involucrados en la auditoria.

De forma general el informe ejecutivo se estructurara en los siguientes puntos:

- **Introducción**: Se expondrá brevemente la situación inicial antes de la auditoria y la necesidad de la misma, haciendo una breve referencia a los acuerdos pactados durante las reuniones iniciales.
- **Objetivo y alcance**: En este punto se mostraran los objetivos concretos de la auditoria y el alcance real que se ha logrado a lo largo de la auditoria, que puede ser superior al pactado inicialmente.
- **Resumen:** En este punto se sintetizara las acciones realizadas en la auditoria, exponiendo de forma resumida las etapas de la auditoria técnica y el trabajo que se ha realizado. Este resumen expondrá los sistemas, ámbitos y ubicaciones que han sido auditados, que incidencias y desviaciones se ha producido respecto a lo esperado, y como se han alcanzado los objetivos iniciales.
- **Conclusiones y recomendaciones:** Este punto es el más importante del informe. En el mismo se indicaran todas las conclusiones que se han alcanzado a partir de las pruebas y resultados obtenidos. Estas conclusiones deben ser orientadas al público objetivo del informe, por los que deben ser a nivel ejecutivo, con una exposición clara y breve de las evidencias obtenidas, ordenadas en función del riesgo detectado que pueda impactar más en la actividad de la organización.

  Una vez expuestas las conclusiones, deben realizarse una serie de recomendaciones que deben llevarse a cabo para evitar, reducir o mitigar el riesgo encontrado durante la auditora**.**
- **Anexo:** Al final del informe ejecutivo se añadirá el informe técnico con cada uno de los hallazgos encontrados y los comentarios realizados por el auditor.

Informe técnico

Durante la realización de la auditoria técnica los auditores van ejecutando las pruebas que han sido planificadas. Con los resultados de las mismas, se van redactando comentarios sobre los resultados obtenidos. Todos estos comentarios deben analizarse en profundidad para obtener una valoración de las mismas y redactar las conclusiones. Estos comentarios son los que se añadirán en el informe técnico, cuya orientación es para el personal técnico, incluyendo al director del área de TI.

Este informe técnico se añadirá al informe ejecutivo como anexo al mismo, para justificar cada una de las conclusiones y recomendaciones expuestas en el informe ejecutivo, y que serán estudiadas por el personal técnico de la organización. Este informe está compuesto por los siguientes puntos:

- **Tipología de auditoría, alcance y objetivos concretos:** Este punto ampliará y complementará el informe ejecutivo desde un punto de vista técnico, redactándolo con un nivel de alto de detalle.
- **Resumen detallado**: Se describirá el proceso de intrusión y la explotación de las vulnerabilidades, indicando los puntos más críticos detectados y las evidencias encontradas.
- **Resultados obtenidos, conclusiones y recomendaciones:** Este último punto ampliara y justificara la información aportada en el mismo apartado del informe ejecutivo, con los resultados obtenidos durante la auditoria. Cada uno de estos resultados o comentarios serán referenciados desde el apartado de conclusiones y recomendaciones para acreditar cada una de ellas con el suficiente nivel de detalle técnico. Esto permite que los responsables de esa área técnica se encarguen de su revisión para evitar, reducir o mitigar los riesgos encontrados.

Propósito final de la fase de generación de informes

Esta es la fase final de la auditoria, donde se presentaran los resultados a la organización que contrato la auditoria. Estos resultados se expondrán en los informes redactados y en la presentación de los mismos ante la dirección ejecutiva de la organización donde se realiza la auditoria. En esta presentación final se expondrán las conclusiones y las recomendaciones a seguir para reducir las vulnerabilidades encontradas, y por tanto el riesgo de explotación de las mismas. Todo esto servirá a la dirección ejecutiva para comprender el nivel de riesgo que presenta la organización y que puede afectar al modelo de negocio de la organización. Con las conclusiones y las recomendaciones la organización estudiara que riesgos serán tratados, que controles serán implantados y que plazos se impondrán para el seguimiento de las recomendaciones.

La figura 3.8 muestra el proceso completo de la nueva metodología, aportando una visión global de la misma.

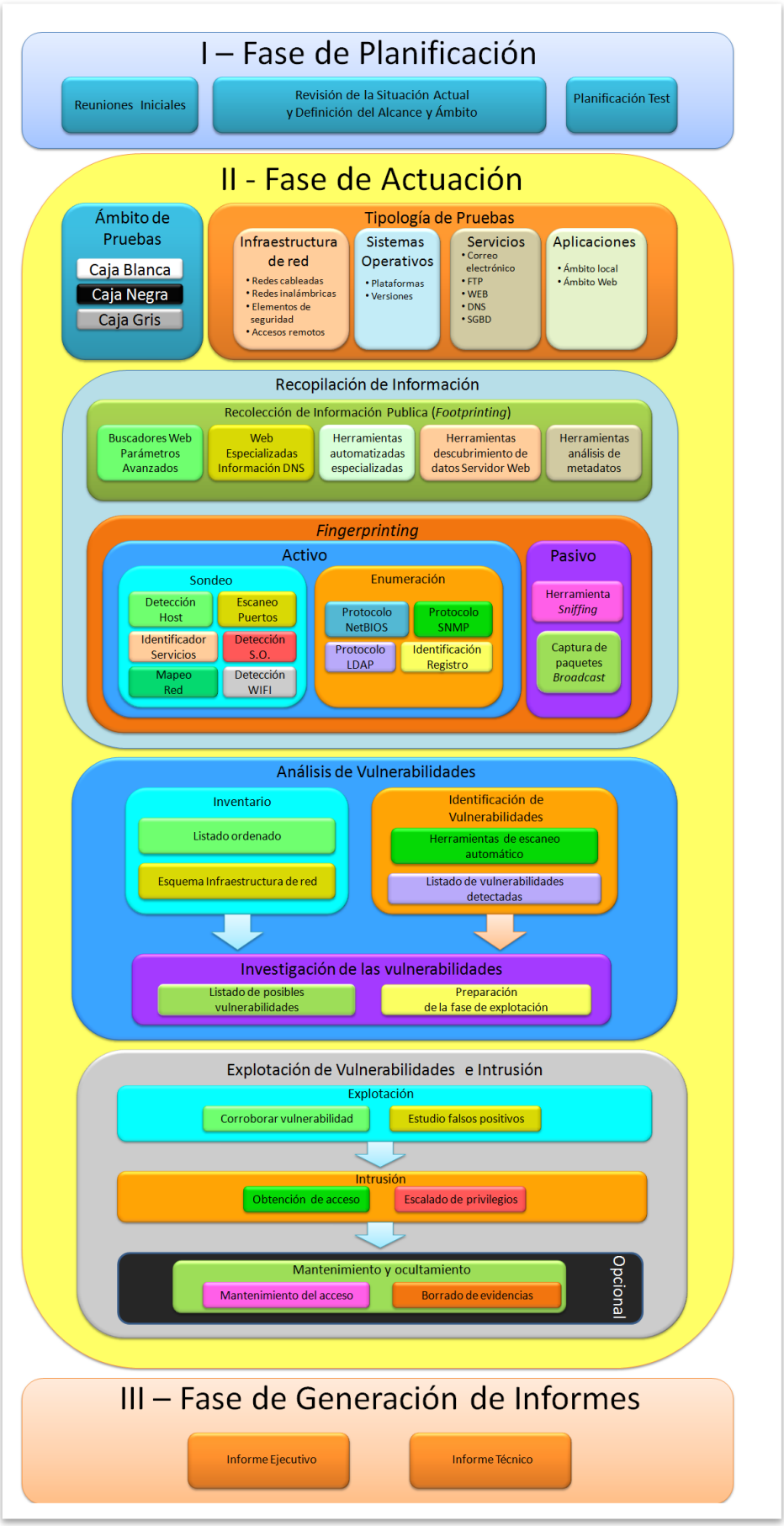

Figura 3.8. Procedimiento completo de la nueva metodología de test de intrusión

Capitulo 4: Validación de la metodología

Una vez definida la nueva metodología de test de intrusión es necesario realizar una evaluación de la misma. Para demostrar su validez y asegurar su efectividad, debe realizarse una validación de la metodología a través la construcción de un pequeño prototipo con un escenario real o virtual orientado a las pruebas de intrusión. Dado que el trabajo no cubre la construcción del prototipo, este será considerado como trabajo en líneas futuras del desarrollo de la nueva metodología. En este capítulo por tanto se va a pergeñar este prototipo, especificando los requisitos mínimos que debe tener a nivel de arquitectura y tecnología.

4.1 Arquitectura y requisitos mínimos del prototipo de validación

La realización de pruebas de intrusión sobre un entorno similar a una organización es un escenario adecuado para la validación de la metodología propuesta. La validación se llevara a cabo a través de la extracción de resultados que permitan su análisis y posterior valoración de aspectos tales como la usabilidad, meticulosidad, ámbito y profundidad del test de intrusión. Esta valoración permitirá de esta forma comparar la metodología desarrollada con las metodologías estándar de facto estudiadas a lo largo del trabajo.

El prototipo permitirá la captura de requisitos mínimos tanto a nivel de arquitectura como de tecnologías actuales. La arquitectura del prototipo debe permitir la realización del test de intrusión sobre todos los ámbitos propuestos en la metodología desarrollada, simular un entorno de red real con los ámbitos que deben ser cubiertos tal y como se ha definido en la metodología. Los ámbitos a cubrir son los siguientes:

- Infraestructura de red:
  - Entornos de red cableados: *Router*, *Switcher*
  - Elementos de seguridad: Firewall
  - Accesos remotos: VPN
  - Entornos inalámbricos: WIFI
- Sistemas operativos.
- Servicios de públicos de correo electrónico, FTP, HTTP, DNS.
- Aplicaciones locales y servicios de Intranet.

La infraestructura de red presentara diferentes tecnologías, tanto de elementos de comunicación como de elementos de seguridad. Cada uno de estos elementos se

configuraran de la manera más segura posible, similar a como se realizaría en un entorno real. Se crearan al menos 4 zonas de red diferenciadas tales como conexión a Internet, zona DMZ publica, zona de servidores y zona LAN de usuarios finales. En esta última zona se ubicara también el punto de acceso Wifi.

En cuanto a los sistemas operativos se intentara simular entornos de producción reales, por tanto se instalaran los sistemas operativos más utilizados para cada uno de los servidores que soportan servicios y estaciones de usuario. Igualmente se instalaran los servicios y aplicaciones más utilizadas habitualmente. Todos estos elementos deberán ser configurados de manera segura para simular en lo posible un entorno de producción real.
La ubicación del auditor dependerá del tipo de prueba de intrusión que se realice, de forma que si se realizan pruebas de caja blanca se situara en la zona de LAN de usuarios y si el tipo de prueba es de caja negra la situación será en el ámbito de Internet.

A partir de los ámbitos cubiertos y de los requisitos mínimos en cuanto a tecnología y servicios que cubre la metodología se propone la arquitectura del siguiente prototipo, como se muestra en la figura 4.1.

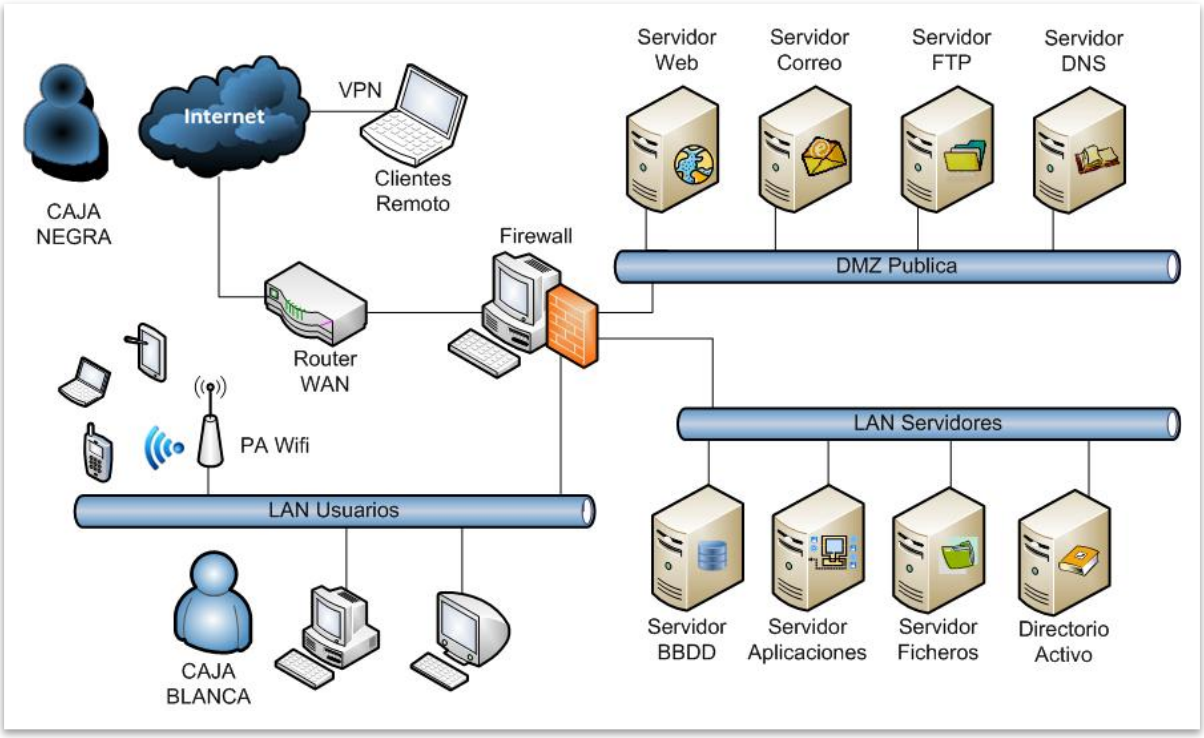

Figura 4.1. Esquema propuesto como prototipo de validación

La elección de todos estos elementos para la creación del prototipo se pospondrá a un futuro desarrollo del prototipo, como ampliación al trabajo actual en un estudio futuro.

Capitulo 5: Conclusiones y líneas futuras

Este trabajo expone el desarrollo de una nueva metodología, partiendo del estudio previo de las características principales de las metodologías de referencia en las auditorias técnicas. A lo largo del mismo se ha ido describiendo las tareas que componen los test de intrusión, y se ha desarrollado una nueva metodología una vez que se han obtenidos los conocimientos necesarios. Durante el estudio y realización de este trabajo se han alcanzado las siguientes conclusiones y se han anotado y enumerado las posibles líneas futuras que no han podido ser desarrolladas con mayor profundidad, tanto por los plazos de entrega como por los objetivos del trabajo.

Conclusiones

- Las tres metodologías expuestas cubren perfectamente todos los aspectos y ámbitos necesarios para la realización de una auditoria técnica independientemente del ámbito y del tipo de pruebas a realizar. La nueva metodología no mejora como tal ningún aspecto de las anteriores, sin embargo presenta la información y las fases de ejecución de la misma de una forma más resumida y sencilla. Este enfoque permite una mejor asimilación y retención de las fases generales. De cara al auditor novel, supone una guía de referencia rápida a las otras metodologías, ya que para ello se incluyen las referencias a las mismas, aportando una satisfacción subjetiva en el auditor mayor que las anteriores.

- El éxito en la realización de un test de intrusión tiene un aspecto artesanal, que se basa en la habilidad y experiencia del auditor, por lo que la utilización de las metodologías es imprescindible para que las auditorias técnicas sean objetivas, rigurosas, sistemáticas e independientes. Estos beneficios no pueden aportarse sin la utilización de alguna de estas metodologías. El aporte de la nueva metodología es similar a las estudiadas, por la forma sistemática y repetible de la misma, de manera que presente resultados similares, aunque sea realizada con diferente nivel de conocimiento o experiencia en las auditorias técnicas.

- Las metodologías cuanto más minuciosas sean, tendrán un mayor nivel de profundidad para la obtención de evidencias de la existencia de vulnerabilidades que presenta cada sistema auditado. Para obtener ese nivel de detalle, se debe profundizar a nivel de herramienta en su detección y explotación, de forma que esa metodología se vuelve dependiente de la tecnología actual. Dada la rápida actualización de la tecnología en estos tiempo, llegar a ese nivel de detalle supondrá

que la metodología quede rápidamente obsoleta y deba ser actualizada al mismo ritmo de la tecnología. Esto supone la dedicación exclusiva y un alto coste. La ventaja que presenta una metodología muy generalista como la que se ha desarrollado en este trabajo es la facilidad de actualización de la misma, dado que no es dependiente de la tecnología más utilizada ni de las herramientas, sino que es trabajo del auditor estar pendiente de la actualización de la misma acorde a los conocimientos y preferencias del mismo.

- Dentro de las auditorias técnicas, en concreto en la fase de planificación, la delimitación del alcance y la determinación de los ámbitos y tipos de auditoría es una de las partes más importante de la misma. Estas decisiones deben ser estudiadas a fondo, dado que suponen la definición de los recursos tecnológicos y humanos y su duración, y por ende el coste de la auditoria. Todos estos aspectos deben ser reflejados en la parte contractual de la auditoria, acotando también las obligaciones, responsabilidades, limitaciones y posibles incidencias sobre servicios que estén en producción y que puedan verse afectados en la realización de las pruebas de la auditoria técnica.

- Dado que van surgiendo nuevas herramientas o actualizaciones de las mismas, para adaptarse a los nuevos métodos y tecnologías, es difícil definir una lista de herramientas genéricas, siendo responsabilidad del auditor el disponer de una recopilación lo más adaptada posible al tipo de auditoría y ámbito de actuación. El auditor deber elegir varios métodos y herramientas por cada técnica y ámbito que tenga que cubrir. Esto permitirá complementar y asegurar que los ámbitos y aplicaciones que son evaluadas se realizan con la suficiente amplitud y profundidad. De manera que en cada una de las pruebas que realice evite en lo posible la presentación de falsos negativos en la auditoria, que supongan una vulnerabilidad futura y la creación de una falsa sensación de seguridad que disminuya la implantación de los controles necesarios. Además el auditor debe trabajar de forma meticulosa y constante en el aprendizaje y comprensión de la lógica de las mismas, para optimizar los tiempos de actuación y acotar de esta forma el coste auditor/hora que se presupueste.

- La gran mayoría de pruebas de intrusión utilizan herramientas automatizadas para el descubrimiento y explotación de vulnerabilidades. Si estas pruebas se realizasen de forma manual, el tiempo de realización de las pruebas se dispararía, y por tanto el coste de la auditoria. El uso de esta herramientas automatizas es por ello imprescindible, pero requiere una posterior corroboración de las vulnerabilidades

detectadas por parte del auditor. Esto es necesario para evitar que el numero de falsos positivos se dispare, y que las posterior implantación de controles de seguridad siguiendo las recomendaciones sea lo más eficiente y eficaz posible.

- Las pruebas de intrusión presentan ciertas limitaciones a la hora de detectar todas las vulnerabilidades que presente un sistema auditado, sobre todo a nivel de aplicaciones. Por ello es necesario no centrar de forma exclusiva la seguridad a solo el ámbito de pruebas de intrusión, sino alinear y complementar este tipo de pruebas al resto de actividades y buenas prácticas de implantación la seguridad de la información.

- La figura del auditor debe alejarse de la imagen del examinador que busca fallos o deficiencias en la organización auditada. Esta imagen debe enfocarse a la de un instrumento más utilizara la dirección de la organización para el estudio del nivel de riesgo que presenta la organización en cuanto a la preservación de la integridad, confidencialidad y disponibilidad de los sistemas de información. Aporta un punto de vista más objetivo, sistemático e independiente, de forma que este debe integrarse dentro de las áreas que vayan a ser auditas como un elemento más de la misma, consultando, explicando y evaluando cada una de las evidencias obtenidas con los actores de dichas áreas.

- A la hora de redactar el informe final es necesario hacer mucho hincapié en la correcta redacción del mismo. En ocasiones se infravalora, pero cabe destacar que en este se plasma todo el trabajo realizado y se justifica la realización de la auditoría, sobre todo desde el punto de vista del resumen ejecutivo.

- La metodología que tiene más puntos en común con la desarrollada en este trabajo es la propuesta por ISSAF, sobre todo destaca los aspectos de sencillez, usabilidad, claridad y una rápida curva de aprendizaje. Por tanto, desde el punto de vista del auditor novel la metodología que más se ajusta la visión inexperta es la mostrada en el capítulo B de la metodología ISSAF 0.2.1: *Penetration Testing Methodology.*

- La realización de las auditorias técnicas ayudan a mantener la alineación de los objetivos, características y necesidades de las organizaciones respecto a la adecuada utilización de los sistemas de información. Esto aporta una serie de ventajas muy beneficiosas para las organizaciones auditada, tales como la reducción del nivel de riesgo que suponga un impacto negativo y por tanto un ahorro tanto de tiempo como económica que permita una mejor imagen corporativa y unas menores perdidas de oportunidades de negocio.

Líneas Futuras

- La utilización de una métrica para calcular el nivel de riesgo de una organización es uno de los aspectos principales, tanto para tener una visión más objetiva del riesgo, ya que puede ser medida, como para mejorar el nivel real del riesgo de la organización después de seguir las recomendaciones de la auditoria. Definir una métrica para calcular el riesgo real en la parte del test de intrusión, es un objetivo a desarrollar en futuras versiones de esta metodología.

- En el presente trabajo se han estudiado y resumido las metodologías más utilizadas actualmente en las auditorias técnicas, como son OSSIMM, ISSAF y OWASP. Sin embargo existen otras metodologías que son muy utilizadas que aportan aspectos diferentes y alternativos a las metodologías estudiadas, permitiendo complementarlas. Cabe destacar 2 metodologías como las de PTES [9] y NIST SP 800-115 [10] que en futuras versiones de este trabajo deberán ser estudiadas y resumidas para que aporten nuevos puntos de vista y características a la nueva metodología desarrollada.

- La validación de las metodologías diseñadas es un factor muy importante a la hora cerciorarse de que la metodología cubre los aspectos mínimos para la que fue diseñada, que se obtienen resultados adecuados en la utilización de la misma y de una posterior aceptación por parte del ámbito de los auditores. Para la realización de la validación es necesario el diseño y la implementación de un prototipo que permita la construcción de un entorno de pruebas. Este prototipo se pergeño en el capítulo 4, fijando la arquitectura y los requisitos mínimos necesarios para poder simular todos los ámbitos necesarios a testear. La creación de este prototipo sobre un entorno real, o en su defecto un entorno mezcla entre elementos de red reales y maquinas virtualizadas, dependerá siempre en función del presupuesto disponible. Este prototipo se presenta como línea futura de este trabajo.

- Una de las líneas de trabajo con mas recorrido es la del diseño de ciclo de vida seguro en el desarrollo de software. En dicha línea se aportan aspectos diferentes a la hora de testear las aplicaciones, ya sean locales u orientadas a ámbitos Web. La realización de pruebas en fases más tempranas del ciclo de vida, aportará más información a testear en las pruebas de intrusión, y permitirá realizar una batería de pruebas en las que se disminuyan los falsos negativos. Este aspecto ampliaría y complementaria la metodología de pruebas de intrusión desarrollado en este trabajo.

- Los ámbitos que son cubiertos por esta metodología abarcar un gran porcentaje de ambientes y entornos de los sistemas de información utilizados por la mayoría de las organizaciones. Sin embargo esta metodología no es muy exhaustiva, dado que quedan sin cubrir ámbitos tan importantes tales como la ingeniería social, medidas de seguridad de acceso físico, comunicaciones telefónicas así como tecnologías de voz IP y aspectos de cumplimiento tanto de buenas prácticas como de la legislación vigente en cada uno de los países donde se realice en la auditoria. Al igual que el punto anterior son aspectos que permitirían ampliar y complementar la metodología expuesta en este trabajo.

Referencias bibliográficas

[1] ISECOM (Institute for Security and Open Methodologies). Diciembre 2010. *OSSTMM Versión 3.0. (The Open Source Security Testing Methodology Manual).* http://www.isecom.org/mirror/OSSTMM.3.pdf

[2] OISSG (Open Information Systems Security Group). Abril 2006. *ISSAF Draft 0.2.1. (*Information *Systems Security Assessment Framework).* http://www.oissg.org/files/issaf0.2.1.pdf

[3] OWASP (Open Web Application Security Project). Diciembre 2008. *OWASP Testing Guide versión 3.0*. https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

[4] Ron Weber. (Enero 1988). *Edp Auditing: Conceptual Foundations and Practice*. Mcgraw-Hill College.

[5] Pete Herzog. ISECOM (Institute for Security and Open Methodologies). Agosto 2003. *OSSTMM Versión 2.1 (The Open Source Security Testing Methodology Manual).* http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

[6] Javier de Pedro Carracedo. Universidad de Alcalá. 2010. *Seguridad en profundidad en los Sistemas de Información*. Apuntes asignatura: Aplicaciones Telemáticas http://it.aut.uah.es/~jdp/at/SEGURIDAD06.pdf

[7] Gary McGraw. (2005*). Software Security: Building Security In*. Addison Wesley Professional.

[8] Gregory Tassey, NIST (National Institute of Standards and Technology). Mayo 2002. The Economic Impacts of Inadequate Infrastructure for Software Testing. http://www.nist.gov/director/planning/upload/report02-3.pdf

[9] PTES (Penetration Testing Execution Standard). Noviembre 2010. *PTES Technical Guidelines.* http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

[10] Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. NIST (National Institute of Standards and Technology). Septiembre 2008. *Technical Guide to Information Security Testing and Assessment. Special Publication 800-115.* http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf