Universidad de Buenos Aires
Facultades de Ciencias Económicas, Cs. Exactas y Naturales
e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Enfoque arquitectónico sobre la seguridad en software.

Autora: Ing. Molina, Erica Alejandra

Tutor del Trabajo Final: Pedro Hecht

Año de Presentación: 2019

Cohorte del Cursante: 2017

Declaración Jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis de Maestría vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Molina Erica Alejandra
DNI 28488961

Resumen

En el presente trabajo, se muestra la importancia que tiene la seguridad en el ciclo de vida del desarrollo de software. Lo importante que es involucrarse desde el inicio del desarrollo de un software en cuanto a la seguridad, como así también sus ventajas y desventajas. Se analizará cómo se debe incluir la seguridad en todas las fases del desarrollo de software.

Se mostrarán algunos frameworks de aplicaciones web, en las que nos vamos a centrar en este trabajo, ya que una de las ventajas más significativas, es que tienen varias cuestiones resueltas, entre ellas, la seguridad.También se analizarán algunas herramientas, para el despliegue de nuestra aplicación y también otras herramientas para el monitoreo de la misma.

Se remarca también la importancia de la documentación de la arquitectura de nuestra aplicación como así también la importancia de incluir la lógica de negocio en cuanto a la seguridad de la información.

Finalmente, mediante varias experiencias en cuanto al desarrollo de aplicaciones, puedo decir que es muy importante capacitar a los desarrolladores para que tengas los conocimientos necesarios sobre las vulnerabilidades que puede tener la aplicación, y cómo poder evitarlas. No llegar a la etapa productiva con “vulnerabilidades conocidas” esperando corregirlas cuando “haya algún tiempo”. Tampoco debemos olvidarnos monitorear nuestra aplicación una vez que se encuentra productiva, ya que de esta manera, estamos evitando dar ventaja a posibles atacantes.

Tabla de contenido

Prólogo

Espero que este trabajo de investigación sirva para que pueda ser aplicado en organizaciones que desconocen del tema de la seguridad de la información desde el Ciclo de Vida del Desarrollo del Software.

Agradezco al Ministerio de Seguridad por haberme brindado la beca para acceder a esta Especialización en la Universidad de Buenos Aires.

Introducción

El principal objetivo será realizar un trabajo de investigación, para aumentar la importancia que tiene la seguridad informática en el ciclo de vida del desarrollo de software y que esté disponible en el Ministerio de Seguridad para ser consultado toda vez que se desarrolle un software nuevo, como así también proporcionar la fundamentación para que se genere un área de seguridad informática dentro del Ministerio con perfiles acordes a las funciones de Arquitecto en Seguridad, capacitar a la gente de Infraestructura para que se trabaje en conjunto y tener un “Gerente” o encargado del área de seguridad informática.

Como base para comprender el enfoque de este proyecto de investigación, se presentará una descripción del ciclo de vida del desarrollo de software [1] para que, de esta manera, se pueda aplicar la importancia de incluir la participación del área de seguridad en cada una de las fases que lo componen.

El proyecto además brindará una serie de objetivos deseables a cumplir a nivel seguridad de la información dentro del ciclo de vida de desarrollo del software, como así también las ventajas que tiene aplicar frameworks de desarrollo para resolver las cuestiones básicas de la seguridad del mismo.

La metodología del proyecto se basará en mostrar los principales conceptos del ciclo de vida del desarrollo de software, la interacción del área de seguridad en el mismo y también la descripción de algunas herramientas que pueden servir de ayuda en algunas de las etapas.

Ciclo de Vida del Desarrollo de Software

Etapas en el ciclo de vida del desarrollo de software y su interacción con el área de Seguridad Informática

Podemos empezar con la definición de ciclo de vida de desarrollo de software que nos brinda la ISO 12207:

"La ISO, International Organization for standardization (Organización para la Estandarización), en su norma 12207 define al ciclo de vida de un software como un marco de referencia que contiene las actividades y las tareas involucradas en el desarrollo, la explotación y el mantenimiento de un producto software, abarcando desde la definición hasta la finalización de su uso". [2]

Generalizando las etapas de ciclo de vida, encontramos tres de ellas:

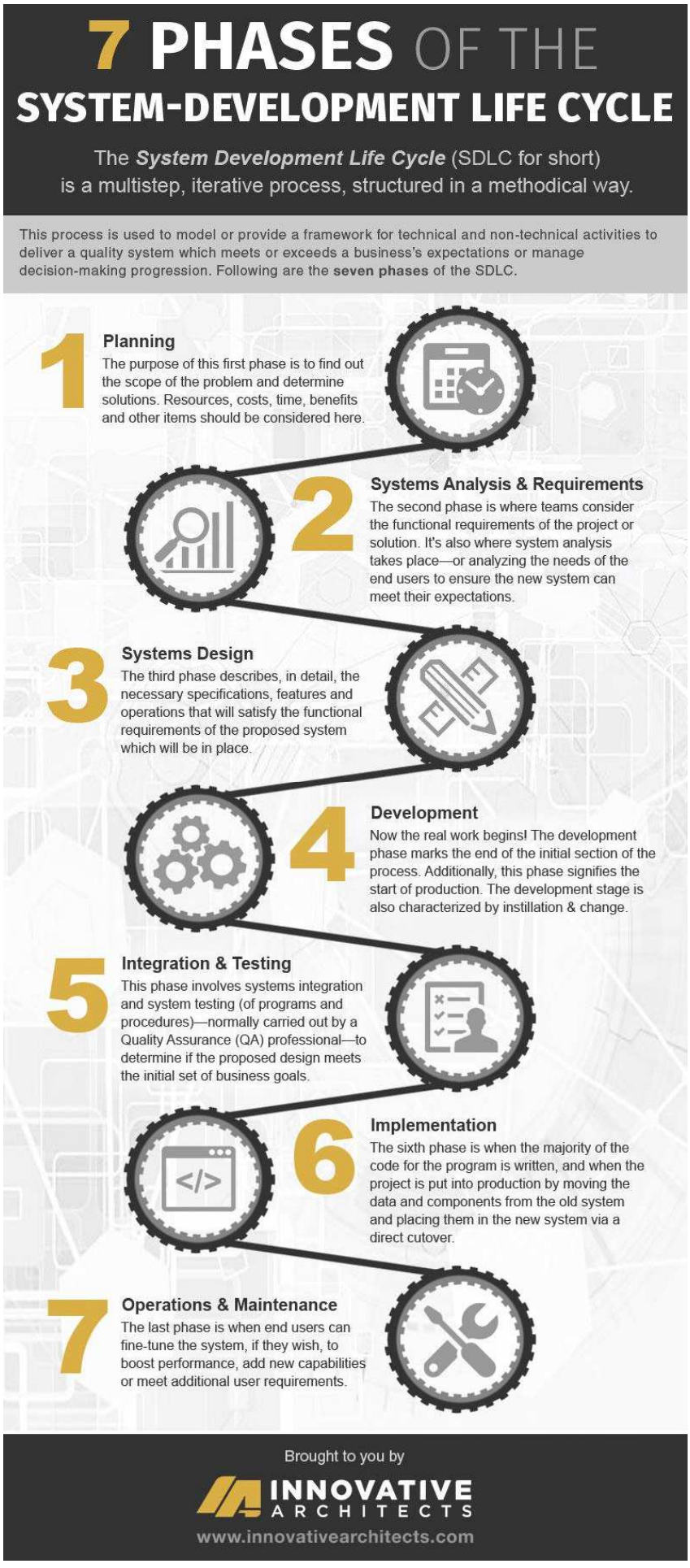
- Planificación: del proyecto en sí mismo. En esta etapa vamos a jugar con la planificación en tiempo y económica del proyecto, es decir: ponerles un valor económico tanto al tiempo que llevará el proyecto como así también a los recursos ya sean humanos como físicos que van a intervenir en el mismo.
- Implementación: sería el cómo se va a llevar a cabo el proyecto, cuál sería el conjunto de actividades para la realización del mismo.
- Puesta en producción: la presentación del producto finalizado al cliente quien será el encargado de la validación, es decir, si cumple con sus necesidades o es necesario realizarle modificaciones o cambiarlo.

Los puntos anteriores son a un nivel general los tres grandes grupos en los que se dividen las etapas del ciclo de vida de desarrollo de software que pasaremos a enumerar a continuación. Paralelamente, es necesario agregar la interacción con la seguridad informática, la cual se vuelve fundamental en estos tiempos y por sobre todas las cosas, se torna fundamental la integración desde el minuto cero, es decir desde el surgimiento de la idea del software, ya que, de esta manera, nos ahorraremos futuros retrasos y errores graves en cuanto a la seguridad de la información.

A nivel informativo, podemos mencionar los pilares de la seguridad de la información, estos son:

- Confidencialidad: la información sólo es accesible por el personal que está autorizado a accederla.
- Integridad: la información es correcta, original, es decir, que se encuentra libre de cualquier manipulación no autorizada por parte de terceros.
- Disponibilidad: la información está accesible cuando se necesita a través de los canales especificados para accederla.

Como se mencionó anteriormente, vamos a dar paso a las etapas del ciclo de vida de desarrollo de software a través de un gráfico [3] y a su relación con la seguridad informática


7 PHASES OF THE
SYSTEM-DEVELOPMENT LIFE CYCLE
The System Development Life Cycle (SDLC for short)
is a multistep, iterative process, structured in a methodical way.
This process is used to model or provide a framework for technical and non-technical activities to deliver a quality system which meets or exceeds a business's expectations or manage decision-making progression. Following are the seven phases of the SDLC.
1
Planning
The purpose of this first phase is to find out the scope of the problem and determine solutions. Resources, costs, time, benefits and other items should be considered here.
2
Systems Analysis & Requirements
The second phase is where teams consider the functional requirements of the project or solution. It's also where system analysis takes place—or analyzing the needs of the end users to ensure the new system can meet their expectations.
3
Systems Design
The third phase describes, in detail, the necessary specifications, features and operations that will satisfy the functional requirements of the proposed system which will be in place.
4
Development
Now the real work begins! The development phase marks the end of the initial section of the process. Additionally, this phase signifies the start of production. The development stage is also characterized by instillation & change.
5
Integration & Testing
This phase involves systems integration and system testing (of programs and procedures)—normally carried out by a Quality Assurance (QA) professional—to determine if the proposed design meets the initial set of business goals.
6
Implementation
The sixth phase is when the majority of the code for the program is written, and when the project is put into production by moving the data and components from the old system and placing them in the new system via a direct cutover.
7
Operations & Maintenance
The last phase is when end users can fine-tune the system, if they wish, to boost performance, add new capabilities or meet additional user requirements.
Brought to you by
INNOVATIVE ARCHITECTS
www.innovativearchitects.com

Etapa de Planificación

En esta etapa lo que vamos a hacer es dimensionar el problema que se quiere resolver mediante el desarrollo de un software para poder tratar de enmarcar una posible solución y poder dimensionar tanto costos como tiempos. A nivel seguridad informática, en esta etapa sería necesario contar con la asesoría del sector correspondiente o bien, el sector de seguridad informática, sería deseable que designe a un especialista para que acompañe el proyecto.

Etapa de análisis y toma de requerimientos

En esta etapa vamos a tomar los requerimientos que nos proveen los usuarios finales, y realizar el análisis pertinente de los mismos para enmarcarlos en funcionales o no funcionales de acuerdo a si tienen que ver directamente con las necesidades o son accesorios a la solución. Comenzar a visualizar el producto terminado, qué comportamiento tendrá.

En esta etapa es muy importante incluir al perfil de seguridad informática ya que también se analizarán las estructuras de datos que se van a utilizar, qué tipo de información se utilizará, también se comenzará a pensar si el sistema estará intercomunicado con otro u otros, cómo será la autenticación en el mismo, si se guardarán los accesos como históricos y cómo se hará este procedimiento, etc. Por ello, es fundamental que haya una persona idónea en el tema que permita validar el grado de complejidad que va a tener la aplicación a nivel seguridad y también pueda dejarlo documentado.

Etapa de diseño

En esta etapa se especificará detalladamente el comportamiento que va a tener el sistema teniendo en cuenta el análisis que se realizó previamente. Es necesario que estas especificaciones se realicen a nivel de detalle, ya que esto facilitará la siguiente etapa de desarrollo. En esta etapa se suelen utilizar herramienta de modelado tanto de datos como de flujos de información, de clases, de casos de uso, que luego sirven al equipo de desarrollo para que pueda realizar su tarea de una manera mucho más documentada y detallada.

En esta etapa la persona encargada de seguridad informática puede especificar por ejemplo, si se encriptan datos, de qué forma se encriptarán, con qué algoritmo, también se define si se va a trabajar con un framework, el diseño de la base de datos, y en este punto es fundamental la política de backups, de

auditorías según el motor de base de datos. También, si por ejemplo, el sistema se va a intercomunicar con otros, de qué forma, cómo será la comunicación, si se va a cifrar, si va a requerir un token, qué tipo de información va a tener ese token. Hoy en día, se utiliza mucho integrar servicios, llamados APIs (Abstract Programmer Interfaces) que lo que proveen es la posibilidad de integrar distintas fuentes de información.

Etapa de desarrollo

En esta etapa es donde se pasa a la programación propiamente dicha de todo lo que volcó en las secciones anteriores.

Si vamos al método de desarrollo de cascada, hoy actualmente muy poco utilizado, es una etapa en la que se pasa a código todo lo expuesto en la etapa de diseño y una vez que se termina de desarrollar, se pasa a la etapa de integración y testing. Lo que ocurre con este método, por ello es que es utilizado sólo en los casos en los se asegura que los requerimientos no pueden variar y están bien definidos, es que, cuando se pasa a la etapa de testing e integración, si surgen modificaciones y/o desvíos en cuanto a los requerimientos, nuevamente volvemos a desarrollar y ésto lo que conlleva es a perder demasiado tiempo.

Por ello, hoy en día se utilizan las metodologías ágiles para el desarrollo, que básicamente se trata de iteraciones cortas, de entre una o dos semanas en las cuales se tiene que llegar a un entregable del cual se comienza con una funcionalidad definida. Los entregables son pequeños, la idea es que se puedan desarrollar y finalizar en una iteración y que, al final de la misma, se encuentren listos para pasar a producción. De esta forma, es mucho menos costoso, en tiempo y en recursos, detectar una desviación de requerimientos y corregirla y volver a iterar si es necesario.

En esta etapa de desarrollo, es fundamental el análisis de las posibles vulnerabilidades que el software podría llegar a tener, para analizar cómo se va a desarrollar para evitarlas.

En el sitio de OWASP (Open Web Application Security Project), podemos encontrar el documento de la última versión de las 10 vulnerabilidades principales que puede tener nuestro software [4], del cual vamos a poner un breve resumen explicando cada una de ellas, también muestra cómo se pasó de la versión anterior a la nueva versión del top ten de OWASP:

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

Pasamos a explicar brevemente cada una de las vulnerabilidades mencionadas:

Inyección: Es una vulnerabilidad mediante la cual, a través de nuestra aplicación se puede incorporar código para ejecutar directamente en la base de datos.

Agente	Vector de Ataque		Debilidades de Seguridad		Impacto	
App. Específica	Explotabilidad: 3		Prevalencia: 2	Detectabilidad: 3	Técnico: 3	¿Negocio?
Casi cualquier fuente de datos puede ser un vector de inyección: variables de entorno, parámetros, servicios web externos e internos, y todo tipo de usuarios. Los defectos de inyección ocurren cuando un atacante puede enviar información dañina a un intérprete.			Estos defectos son muy comunes, particularmente en código heredado. Las vulnerabilidades de inyección se encuentran a menudo en consultas SQL, NoSQL, LDAP, XPath, comandos del SO, analizadores XML, encabezados SMTP, lenguajes de expresión, parámetros y consultas ORM. Los errores de inyección son fáciles de descubrir al examinar el código y los escáneres y *fuzzers* ayudan a encontrarlos.		Una inyección puede causar divulgación, pérdida o corrupción de información, pérdida de auditabilidad, o denegación de acceso. El impacto al negocio depende de las necesidades de la aplicación y de los datos.	

Para prevenir inyecciones, se requiere separar los datos de los comandos y las consultas.

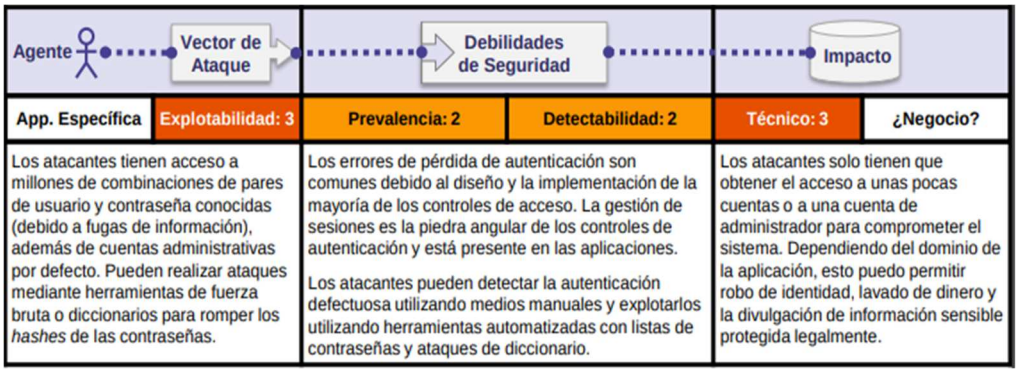
• La opción preferida es utilizar una API segura, que evite el uso de un intérprete por completo y proporcione una interfaz parametrizada. Se debe migrar y utilizar una herramienta de Mapeo Relacional de Objetos (ORMs). Nota: Incluso cuando se parametrizan, los procedimientos almacenados pueden introducir una inyección SQL si el procedimiento PL/SQL o T-SQL concatena consultas y datos, o se ejecutan parámetros utilizando EXECUTE IMMEDIATE o exec().

• Realice validaciones de entradas de datos en el servidor, utilizando "listas blancas". De todos modos, esto no es una defensa completa ya que muchas aplicaciones requieren el uso de caracteres especiales, como en campos de texto, APIs o aplicaciones móviles.

• Para cualquier consulta dinámica residual, escape caracteres especiales utilizando la sintaxis de caracteres específica para el intérprete que se trate. Nota: La estructura de SQL como nombres de tabla, nombres de columna, etc. no se pueden escapar y, por lo tanto, los nombres de estructura suministrados por el usuario son peligrosos. Este es un problema común en el software de redacción de informes.

• Utilice LIMIT y otros controles SQL dentro de las consultas para evitar la fuga masiva de registros en caso de inyección SQL.

Pérdida de Autenticación: Sucede cuando las funciones que se encargan de la autenticación en nuestra aplicación se encuentran mal implementadas y pueden llegar a brindar información a algún atacante sobre usuarios, aplicación y/o sobre cómo ingresar a nuestra aplicación.



Podemos prevenirla:

• Implemente autenticación multi-factor para evitar ataques automatizados, de fuerza bruta o reúso de credenciales robadas.

• No utilice credenciales por defecto en su software, particularmente en el caso de administradores.

• Implemente controles contra contraseñas débiles. Cuando el usuario ingrese una nueva clave, la misma puede verificarse contra la lista del Top 10.000 de peores contraseñas.

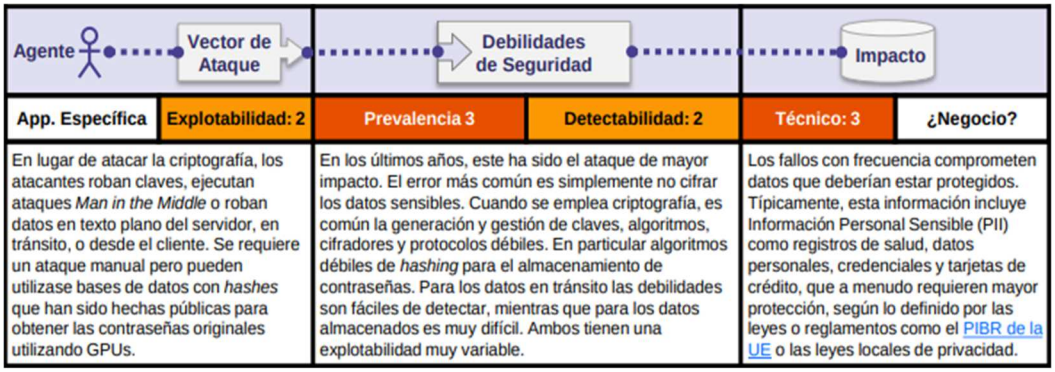
• Alinear la política de longitud, complejidad y rotación de contraseñas con las recomendaciones de la Sección 5.1.1 para Secretos Memorizados de la Guía NIST 800-63 B's u otras políticas de contraseñas modernas, basadas en evidencias.

• Mediante la utilización de los mensajes genéricos iguales en todas las salidas, asegúrese que el registro, la recuperación de credenciales y el uso de APIs, no permiten ataques de enumeración de usuarios.

• Limite o incremente el tiempo de respuesta de cada intento fallido de inicio de sesión. Registre todos los fallos y avise a los administradores cuando se detecten ataques de fuerza bruta.

• Utilice un gestor de sesión en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio con alta entropía después del inicio de sesión. El Session-ID no debe incluirse en la URL, debe almacenarse de forma segura y ser invalidado después del cierre de sesión.

Exposición de Datos Sensibles: Cuando información sensible no se encuentra adecuadamente tratada, es decir, por ejemplo, encriptada, como las tarjetas de crédito, algún atacante puede utilizarla para cometer algún fraude.



Como mínimo, siga las siguientes recomendaciones y consulte las referencias:

• Clasifique los datos procesados, almacenados o transmitidos por el sistema. Identifique qué información es sensible de acuerdo a las regulaciones, leyes o requisitos del negocio y del país.

• Aplique los controles adecuados para cada clasificación.

• No almacene datos sensibles innecesariamente. Descártelos tan pronto como sea posible o utilice un sistema de tokenizacion que cumpla con PCI DSS. Los datos que no se almacenan no pueden ser robados.

• Cifre todos los datos sensibles cuando sean almacenados.

• Cifre todos los datos en tránsito utilizando protocolos seguros como TLS con cifradores que utilicen Perfect Forward Secrecy (PFS), priorizando los algoritmos en el servidor. Aplique el cifrado utilizando directivas como HTTP Strict Transport Security (HSTS).

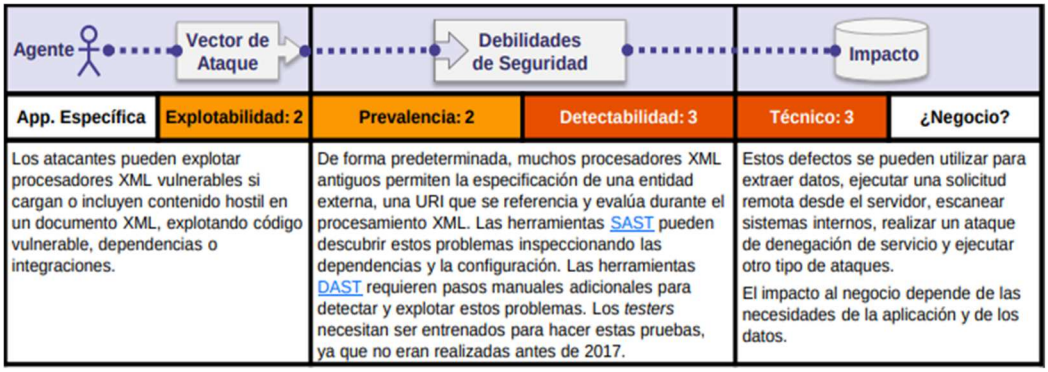
• Utilice únicamente algoritmos y protocolos estándares y fuertes e implemente una gestión adecuada de claves. No cree sus propios algoritmos de cifrado.

• Deshabilite el almacenamiento en cache de datos sensibles.

• Almacene contraseñas utilizando funciones de hashing adaptables con un factor de trabajo (retraso) además de SALT, como Argon2, scrypt, bcrypt o PBKDF2.

• Verifique la efectividad de sus configuraciones y parámetros de forma independiente.

Entidades Externas XML (XXE): Si los XML son antiguos, o están mal configurados, se pueden revelar archivos internos utilizando el controlador de URI de archivo, se pueden escanear puertos. se puede ejecutar código de forma remota o se puede realizar un ataque de denegación de servicio.



El entrenamiento del desarrollador es esencial para identificar y mitigar defectos de XXE. Aparte de esto, prevenir XXE requiere:

• De ser posible, utilice formatos de datos menos complejos como JSON y evite la serialización de datos confidenciales.

• Actualice los procesadores y bibliotecas XML que utilice la aplicación o el sistema subyacente. Utilice validadores de dependencias. Actualice SOAP a la versión 1.2 o superior.

• Deshabilite las entidades externas de XML y procesamiento DTD en todos los analizadores sintácticos XML en su aplicación, según se indica en la hoja de trucos para prevención de XXE de OWASP.

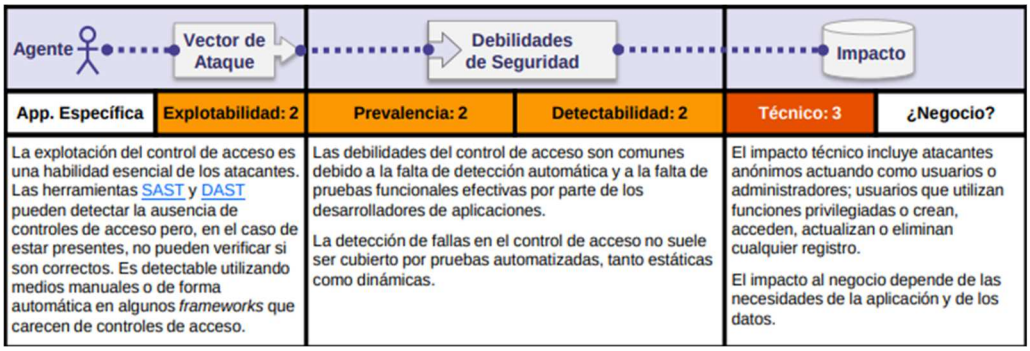
• Implemente validación de entrada positiva en el servidor (“lista blanca”), filtrado y sanitización para prevenir el ingreso de datos dañinos dentro de documentos, cabeceras y nodos XML.

• Verifique que la funcionalidad de carga de archivos XML o XSL valide el XML entrante, usando validación XSD o similar.

• Las herramientas SAST pueden ayudar a detectar XXE en el código fuente, aunque la revisión manual de código es la mejor alternativa en aplicaciones grandes y complejas.

• Si estos controles no son posibles, considere usar parcheo virtual, gateways de seguridad de API, o Firewalls de Aplicaciones Web (WAFs) para detectar, monitorear y bloquear ataques XXE.

Pérdida de Control de Acceso: Muchas veces las restricciones sobre las acciones de los usuarios no se encuentran bien implementadas, y los atacantes pueden acceder y realizar las mismas ocasionando, por ejemplo: cambios de privilegios de usuarios, visualización de información confidencial, etc.



El control de acceso sólo es efectivo si es aplicado del lado del servidor o en Server-less API, donde el atacante no puede modificar la verificación de control de acceso o los metadatos.

• Con la excepción de los recursos públicos, la política debe ser denegar de forma predeterminada.

• Implemente los mecanismos de control de acceso una vez y reutilícelo en toda la aplicación, incluyendo minimizar el control de acceso HTTP (CORS).

• Los controles de acceso al modelo deben imponer la propiedad (dueño) de los registros, en lugar de aceptar que el usuario puede crear, leer, actualizar o eliminar cualquier registro.

• Los modelos de dominio deben hacer cumplir los requisitos exclusivos de los límites de negocio de las aplicaciones.

• Deshabilite el listado de directorios del servidor web y asegúrese que los metadatos/fuentes de archivos (por ejemplo, de GIT) y copia de seguridad no estén presentes en las carpetas públicas.

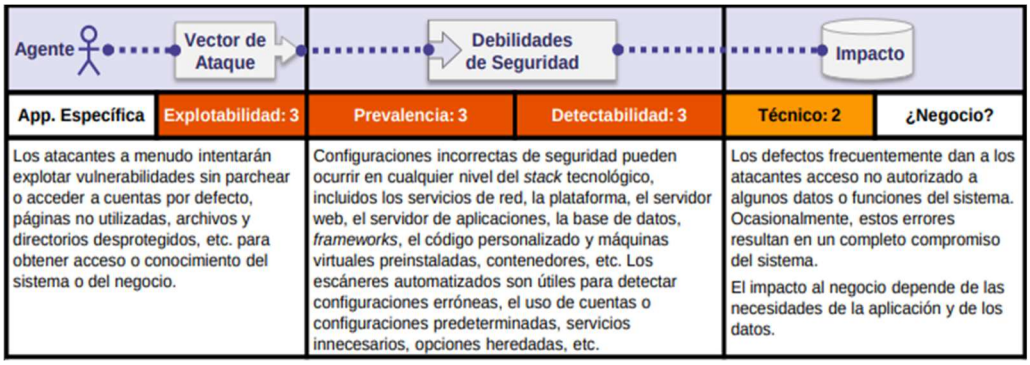
• Registre errores de control de acceso y alerte a los administradores cuando corresponda (por ej. fallas reiteradas).

• Limite la tasa de acceso a las APIs para minimizar el daño de herramientas de ataque automatizadas.

• Los tokens JWT deben ser invalidados luego de la finalización de la sesión por parte del usuario.

• Los desarrolladores y el personal de QA deben incluir pruebas de control de acceso en sus pruebas unitarias y de integración.

Configuración de Seguridad Incorrecta: Cuando las configuraciones de seguridad no se realizan correctamente, pueden llegar a darle a un atacante información valiosa, por ejemplo: mensajes de errores con demasiada información, información sobre el servidor y apache, entre otros.



Deben implementarse procesos seguros de instalación, incluyendo:

• Proceso de fortalecimiento reproducible que agilice y facilite la implementación de otro entorno asegurado. Los entornos de desarrollo, de control de calidad (QA) y de Producción deben configurarse de manera idéntica y con diferentes credenciales para cada entorno. Este proceso puede automatizarse para minimizar el esfuerzo requerido para configurar cada nuevo entorno seguro.

• Use una plataforma minimalista sin funcionalidades innecesarias, componentes, documentación o ejemplos. Elimine o no instale frameworks y funcionalidades no utilizadas.

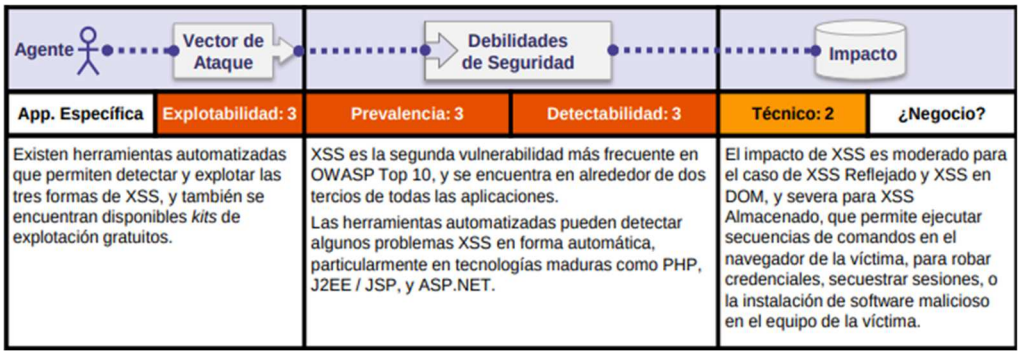
• Siga un proceso para revisar y actualizar las configuraciones apropiadas de acuerdo a las advertencias de seguridad y siga un proceso de gestión de parches. En particular, revise los permisos de almacenamiento en la nube (por ejemplo, los permisos de buckets S3).

• La aplicación debe tener una arquitectura segmentada que proporcione una separación efectiva y segura entre componentes y acceso a terceros, contenedores o grupos de seguridad en la nube (ACLs).

• Envíe directivas de seguridad a los clientes (por ej. cabeceras de seguridad).

• Utilice un proceso automatizado para verificar la efectividad de los ajustes y configuraciones en todos los ambientes.

Cross-Site Scripting (XSS): Cuando no se procesa correctamente la información cargada desde nuestra aplicación, es decir, no se escapa y se permite por ejemplo ingresar código HTML, puede ocurrir que permita a un atacante introducir scripts que se ejecuten posteriormente en los usuarios de nuestra aplicación.



Prevenir XSS requiere mantener los datos no confiables separados del contenido activo del navegador.

• Utilizar frameworks seguros que, por diseño, automáticamente codifican el contenido para prevenir XSS, como en Ruby 3.0 o React JS.

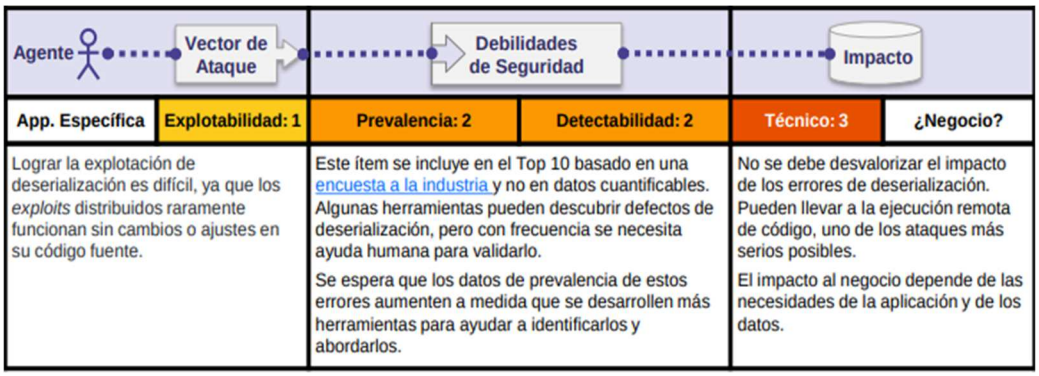
• Codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML (cuerpo, atributos, JavaScript, CSS, o URL) resuelve los XSS Reflejado y XSS Almacenado. La hoja de trucos OWASP para evitar XSS tiene detalles de las técnicas de codificación de datos requeridas.

• Aplicar codificación sensitiva al contexto, cuando se modifica el documento en el navegador del cliente, ayuda a prevenir DOM XSS. Cuando esta técnica no se puede aplicar, se pueden usar técnicas similares de codificación, como se explica en la hoja de trucos OWASP para evitar XSS DOM.

• Habilitar una Política de Seguridad de Contenido (CSP) es una defensa profunda para la mitigación de vulnerabilidades XSS, asumiendo que no hay otras vulnerabilidades que permitan colocar código malicioso vía inclusión de

archivos locales, bibliotecas vulnerables en fuentes conocidas almacenadas en Redes de Distribución de Contenidos (CDN) o localmente.

Deserialización Insegura: Si la deserialización de datos no se encuentra correctamente desarrollada, puede ocurrir que un atacante pueda realizar ataques de repetición, inyección y/o escalada de privilegios.



El único patrón de arquitectura seguro es no aceptar objetos serializados de fuentes no confiables o utilizar medios de serialización que sólo permitan tipos de datos primitivos. Si esto no es posible, considere alguno de los siguientes puntos:

• Implemente verificaciones de integridad tales como firmas digitales en cualquier objeto serializado, con el fin de detectar modificaciones no autorizadas.

• Durante la deserialización y antes de la creación del objeto, exija el cumplimiento estricto de verificaciones de tipo de dato, ya que el código normalmente espera un conjunto de clases definibles. Se ha demostrado que se puede pasar por alto esta técnica, por lo que no es aconsejable confiar sólo en ella.

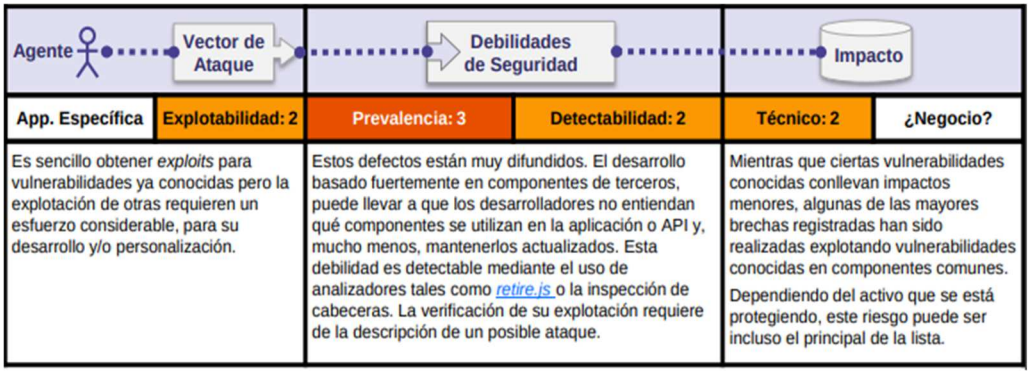
• Aísle el código que realiza la deserialización, de modo que se ejecute en un entorno con los mínimos privilegios posibles.

• Registre las excepciones y fallas en la deserialización, tales como cuando el tipo recibido no es el esperado, o la deserialización produce algún tipo de error.

• Restrinja y monitoree las conexiones (I/O) de red desde contenedores o servidores que utilizan funcionalidades de deserialización.

• Monitoree los procesos de deserialización, alertando si un usuario deserializa constantemente.

Uso de Componentes con Vulnerabilidades Conocidas: Los componentes que se utilizan en nuestras aplicaciones como las librerías, por ejemplo, suelen ejecutarse con los mismos privilegios que la aplicación, con lo cual, hay que tener mucho cuidado de bajar los que estén certificados, en las últimas versiones estables y sean confiables.



Se puede prevenir realizando las siguientes acciones:

• Remover dependencias, funcionalidades, componentes, archivos y documentación innecesaria y no utilizada.

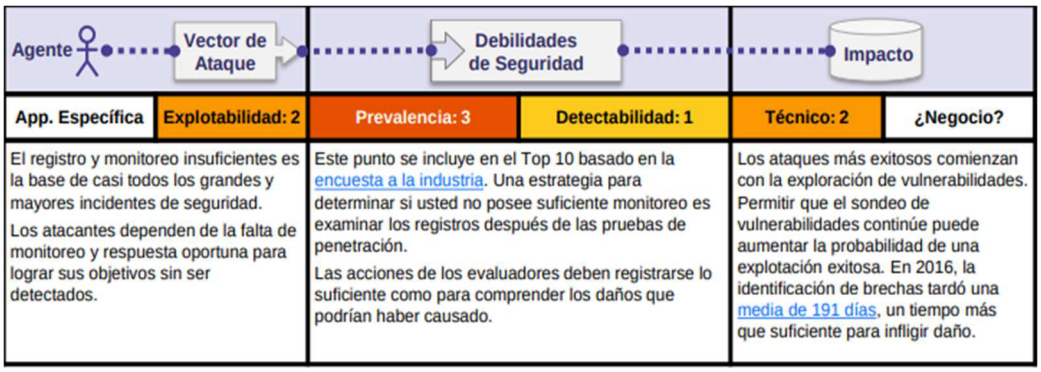
• Utilizar una herramienta para mantener un inventario de versiones de componentes (por ej. frameworks o bibliotecas) tanto del cliente como del servidor. Por ejemplo, Dependency Check y retire.js.

• Monitorizar continuamente fuentes como CVE y NVD en búsqueda de vulnerabilidades en los componentes utilizados. Utilizar herramientas de análisis automatizados. Suscribirse a alertas de seguridad de los componentes utilizados.

• Obtener componentes únicamente de orígenes oficiales utilizando canales seguros. Utilizar preferentemente paquetes firmados con el fin de reducir las probabilidades de uso de versiones manipuladas maliciosamente.

• Supervisar bibliotecas y componentes que no poseen mantenimiento o no liberan parches de seguridad para sus versiones obsoletas o sin soporte. Si el parcheo no es posible, considere desplegar un parche virtual para monitorizar, detectar o protegerse contra la debilidad detectada. Cada organización debe asegurar la existencia de un plan para monitorizar, evaluar y aplicar actualizaciones o cambios de configuraciones durante el ciclo de vida de las aplicaciones.

Registro y Monitoreo Insuficientes: Los monitoreos y registros, nos facilitan encontrar incidentes y poder determinar las causas de los mismos, es importante que contemos con ellos para evitar que posibles atacantes realicen acciones sin que nosotros nos enteremos.



Según el riesgo de los datos almacenados o procesados por la aplicación:

• Asegúrese de que todos los errores de inicio de sesión, de control de acceso y de validación de entradas de datos del lado del servidor se pueden registrar para identificar cuentas sospechosas. Mantenerlo durante el tiempo suficiente para permitir un eventual análisis forense.

• Asegúrese de que las transacciones de alto impacto tengan una pista de auditoría con controles de integridad para prevenir alteraciones o eliminaciones.

• Asegúrese que todas las transacciones de alto valor poseen una traza de auditoría con controles de integridad que permitan detectar su modificación o borrado, tales como una base de datos con permisos de inserción únicamente u similar.

• Establezca una monitorización y alerta efectivos de tal manera que las actividades sospechosas sean detectadas y respondidas dentro de períodos de tiempo aceptables.

• Establezca o adopte un plan de respuesta o recuperación de incidentes, tales como NIST 800-61 rev.2 o posterior. Existen frameworks de protección de aplicaciones comerciales y de código abierto tales como OWASP AppSensor, firewalls de aplicaciones web como ModSecurity utilizando el Core Rule Set de OWASP, y software de correlación de registros con paneles personalizados y alertas.

Ya vimos las descripciones de las principales vulnerabilidades de una aplicación web y algunas formas de cómo prevenirlas, según OWASP. En esta etapa de desarrollo, es fundamental tenerlas en cuenta.

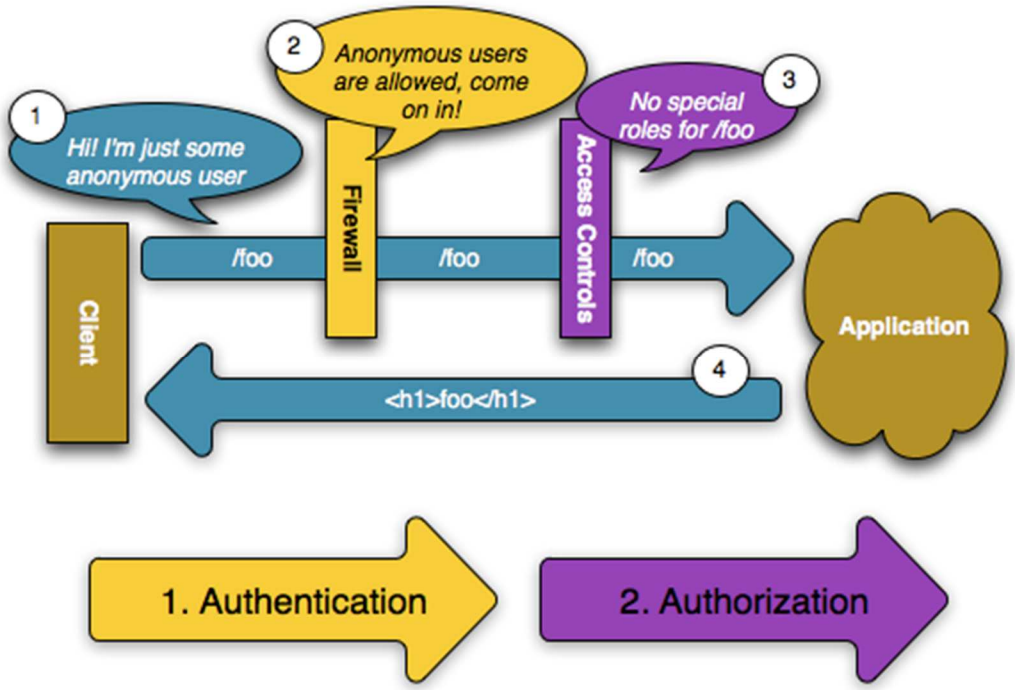
Unas de las opciones es analizar la posibilidad de utilizar algún framework para el desarrollo, ya que los mismos tienen por lo general, la parte de seguridad cubierta, y no nos tenemos que preocupar por ello en una primera instancia.

A continuación presentamos un estudio que se realizó en distintos frameworks[5], que son (se podría decir) de los más utilizados del lenguaje PHP:

• El autor de Laravel, Taylor Otwell, nos ofrece diferentes maneras para tener un sistema más seguro en diferentes aspectos. Primero que nada Laravel utiliza el componente que es “form request” para validar su información y asi delimitar al usuario diferentes los diferentes valores para los tipos de datos para la base de datos que se está utilizando. Además, Uno de los principales componentes de Laravel en seguridad y que se habla mucho es el uso del Middleware, este componente se encarga de analizar y filtrar las llamadas HTTP en el servidor. Además de que lo puedes utilizar para que se encargue de verificar que se trate de un usuario registrado y asi evitar problemas de tipo Cross-Site-Scripting (XSS) y otras medidas de seguridad. También Laravel viene listo para implementar autenticación de usuarios de forma nativa; además de que te permite incluir parametros adicionales, lo que nos asegurara, por ejemplo, si es un usuario activo. Una aplicación segura necesita ser capaz de encriptar sus datos. Con Laravel tienes todo lo necesario para empezar a usar seguridad OpenSSL y cifrado AES-256-CBC. Adicionalmente, todos los valores encriptados están firmados por un código de autenticación de mensaje “Token” que detecta si el mensaje encriptado fue alterado. Para finalizar, cuando un desarrollador crea un sistema que tenga acceso a datos, siempre debe estar atento a los tipos de ataques como los ataques de inyección SQL, Laravel preocupado por esto, incorpora un ORM para que el desarrollador deje de

preocuparse por este tipo de ataques ya que el ORM está basado en una capa de objetos y así no ser capaz de interpretar el lenguaje SQL.

• Para Symfony, la seguridad es un proceso de dos etapas, cuyo objetivo es evitar que un usuario acceda a un recurso al cual no debería tener acceso. En el primer paso del proceso, el sistema de seguridad identifica quién es el usuario obligándolo a presentar algún tipo de identificación. Esto se llama autenticación, y significa que el sistema está tratando de determinar quién eres. Una vez que el sistema sabe quién eres, el siguiente paso es determinar si deberías tener acceso a un determinado recurso. Esta parte del proceso se llama autorización, y significa que el sistema está comprobando si tienes suficientes privilegios para realizar una determinada acción. El sistema de seguridad de Symfony trabaja identificando a un usuario (es decir, la autenticación) y comprobando si ese usuario debe tener acceso a una URL o recurso específico. Cuando un usuario hace una petición a una URL que está protegida por un cortafuegos, se activa el sistema de seguridad. El trabajo del cortafuegos es determinar si el usuario necesita estar autenticado, y si lo hace, enviar una respuesta al usuario para iniciar el proceso de autenticación. Un cortafuegos se activa cuando la URL de una petición entrante concuerda con el patrón de la expresión regular configurada en el valor configuración del cortafuegos. Además de esto, Symfony está asegurado con el forzamiento de HTTP y HTTPS, lo cual hace que estas peticiones forzadas sean rechazadas por el sistema. También hace la selección de usuarios “Agregar usuarios a la lista negra por dirección IP con un votante personalizado” como lo menciona Symfony. Es capaz de implementar listas de control de acceso (ACL), para los accesos no permitidos al sistema y así proteger objetos individuales en la base de datos. Y al igual que Laravel tiene una funcionalidad de “recuérdame” en su inicio de sesión. Y como cualquier buen Framework de seguridad tiene un sistema de encriptación muy útil, utilizando codificadores de contraseña como PBKDF2 Y BCrypt.



Una vez que finalicemos mediante iteraciones o bien mediante la implementación del método en cascada, del desarrollo de nuestra aplicación, idealmente aplicando algún framework, el cual nos haya facilitado no dedicar demasiado tiempo a prestar atención a las vulnerabilidades más conocidas. No por ello, debemos dejar de dedicarle un largo tiempo a revisar nuestra aplicación antes de la implementación.

Etapa de Testing e Integración

En esta etapa, se procede a comprobar que nuestra aplicación cumple con los requerimientos relevados en la etapa de análisis, idealmente por un equipo de QA (Quality Assurance). Para ellos, se pueden utilizar:

• **Test de Integración**: se verifica el diseño de nuestra aplicación a alto nivel y demuestra que todos los componentes pueden combinarse juntos y que se pueden realizar operaciones básicas sin fallas.

• **Test de Aceptación**: Es el nivel final de la validación de nuestra aplicación. Verifica que nuestra aplicación satisface las necesidades del usuario.

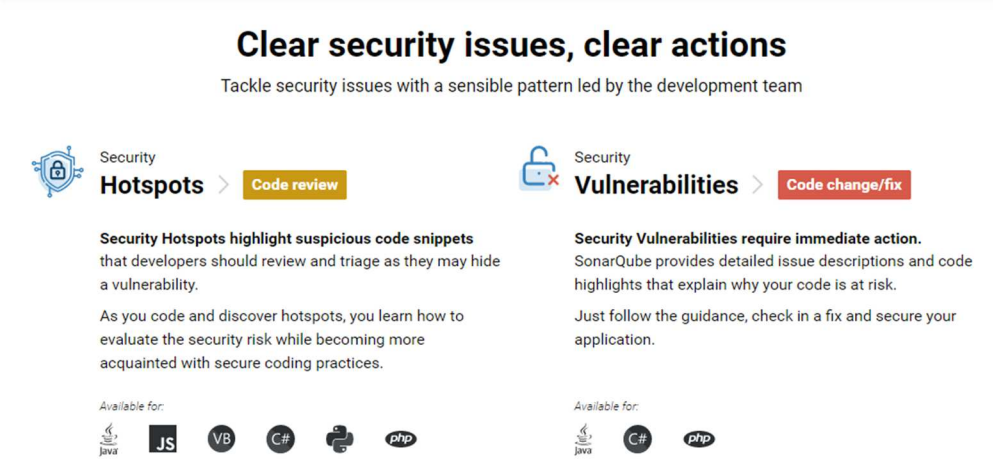
Este suele ser un test funcional y usualmente es realizado por el usuario final en un entorno de testing emulando la funcionalidad total de nuestra aplicación

Además de estos tests, es conveniente que nuestra aplicación se desarrolle a la par de tests unitarios. Los tests unitarios son los que nos previenen de fallas durante el desarrollo, nos van testeando a nivel código nuestro propio código y son muy útiles para también testear posibles vulnerabilidades. Hay que tener la práctica recomendable de desarrollarlos inclusive antes de desarrollar el propio código.

Es importante mantener una revisión continua, es decir, ante cualquier corrección o modificación de nuestra aplicación, es necesario, volver a testear la misma para ver si por ejemplo, en la nueva implementación se incluyó alguna vulnerabilidad. Para ello, es necesario tener alguna batería de tests, por ejemplo de regresión, para cubrir toda nuestra aplicación.

En esta etapa, además, podemos contar con algunas herramientas que nos pueden ayudar a encontrar, por ejemplo, algunas vulnerabilidades, siempre y cuando estén bien configuradas para ese objetivo:

Sonarqube[6]:



Según nos recomienda OWASP:

“No comience por probarlo todo. Concéntrese en lo que es importante y amplíe su programa de verificación con el tiempo. Esto significa ampliar el conjunto de defensas y riesgos de seguridad que se prueban automáticamente, así como ampliar el conjunto de aplicaciones y APIs que se incluyen en el alcance. El objetivo es lograr un estado en el que la seguridad esencial de todas sus aplicaciones y API se verifique continuamente”

Etapa de Implementación

En esta etapa es en la cual se pone productiva nuestra aplicación, donde la colocamos en los servidores definitivos y con la/las bases de datos definitivas.

Para esta etapa vamos a tomar y describir algunas de las recomendaciones de OWASP:

• Automatizar el despliegue seguro de la aplicación, interfaces y todo componente, incluyendo las autorizaciones requeridas: Existen algunas herramientas que actualmente permiten automatizar despliegues, tanto en aplicaciones en sí como también en bases de datos. Una de ellas es Jenkins, que nos provee de una interfaz en la que podemos crear distintos perfiles, cada uno de los cuales, con sus privilegios, para poder realizar los despliegues de nuestra aplicación.

• Probar las funciones técnicas, integración a la arquitectura de TI, y coordinar pruebas de funciones de negocio. En estos casos también se puede idear una línea de tests automáticos, que incluyan, por ejemplo: tests unitarios, tests automáticos con postman que es una herramienta para probar APIs (Abstract Program Interfaces) que nos permite automatizar las pruebas.

• Crear casos de “uso” y de “abuso” tanto desde el punto de vista netamente técnico como del negocio. En este caso podemos utilizar robots para que nos completen y nos hagan las pruebas automáticas desde el lado del usuario, existen herramientas y frameworks como Robot Framework, el cual también nos brinda estadísticas de los errores que ocurrieron.

• Administrar pruebas de seguridad de acuerdo a los procesos internos, las necesidades de protección y el nivel de amenazas asumido para la aplicación. No estaría de más, en caso de que nuestra aplicación sea una aplicación web, realizar algún pentesting para verificar en qué estado se encuentra nuestra aplicación en cuanto a seguridad se refiere.

• Poner la aplicación en operación y migrar las aplicaciones usadas previamente en caso de ser necesario. En el caso de que haya habido entornos de pruebas, quizás disponibles con perfiles de accesos a datos, que por algún motivo se compartan con el entorno productivo, sería indispensable darlos de baja.

• Actualizar toda la documentación, incluyendo la Base de Datos de Gestión de la Seguridad y la arquitectura de seguridad. A medida que se va diseñando y desarrollando, inclusive en las etapas de testing y de implementación, es absolutamente necesario mantener actualizada la documentación de la arquitectura de la aplicación.

Etapa de Operación y Mantenimiento:

En esta etapa, nuestra aplicación ya se encuentra operativa en un entorno productivo. Por lo tanto, se ingresa en el estadío de mantenimiento correctivo, en el que se corrigen posibles fallas en el funcionamiento de la misma, como así también la incorporación de nuevas funcionalidades. En este caso siempre debemos tener presente correr todos los tests antes de que las funcionalidades y/o correcciones pasen a nuestro ambiente productivo como así también, debemos mantener un sistema de monitoreo y análisis de logs para estar atentos ante cualquier intento de intromisión o posible ataque a nuestra aplicación.

Como herramientas de monitoreo, podemos mencionar algunas de las más utilizadas o más reconocidas:

- Pandora FMS: Su versión libre es capaz de monitorizar más de 10,000 nodos y cubrir sin limitaciones monitorización de redes, de servidores y de aplicaciones. Tiene funcionalidades completas para informes, alertas, integraciones, etc
- Nagios: Es probablemente la herramienta libre más conocida. Nos ofrece un potente sistema de monitorización de código abierto que permite monitorizar toda una infraestructura IT para asegurar que los sistemas, aplicaciones, servicios y procesos de negocio funcionan adecuadamente.
- Zabbix: Nos ofrece una herramienta de fácil configuración y potente interfaz gráfico y se pueden monitorizar hasta 10,000 nodos sin problemas de rendimiento y sin necesidad de instalar agentes.
- GroundWork: Reutiliza diferentes software de Nagios, Icinga o Cacti para crear su solución global. Consigue entrar entre las mejores herramientas de monitorización de red gracias a su agrupación de otras herramientas.
- Zenoss: Con Zenoss podremos monitorizar almacenamiento, redes, servidores, aplicaciones y servidores virtuales sin necesidad de instalar agentes. Dispone de una versión “Community” con funcionalidades muy reducidas y una versión comercial con todas las funcionalidades.
- Monitis: Esta herramienta está muy enfocada para la PYME y por esta razón aparece dentro de las mejores herramientas de monitoreo de redes.
- Icinga: Se integra con varias bases de datos y destaca su interfaz REST API para integrar otras aplicaciones. Está muy enfocada a redes complejas y monitorizaciones de protocolos, recursos de máquinas y servidores.
- Manage Engine / OPManager: Es una de las herramientas de monitoreo de redes a tener en cuenta. Su tendencia en cuanto a demanda va al alza.

- Open5 Monitor: Es capaz de monitorizar múltiples plataformas, sistemas en la nube y entornos virtuales. Esta herramienta de monitoreo está muy centrada en monitorización de hardware, tráfico de red y servicios y destaca su capacidad para grandes entornos.
- Solarwinds: Se desmarca del resto por su automático mapeo de redes y nodos sin necesidad de acciones manuales. Tiene un interfaz gráfico bastante potente en el que se puede ver fácilmente la topología de red y el estado de la misma. Nos permite integrar máquinas virtuales en su monitorización.

Experiencia Microsoft

Como un caso de aplicación, podemos mencionar, el concepto de seguridad en el Ciclo de vida del desarrollo de software que utiliza Microsoft[7]. Ellos mencionan, que para tener un software más seguro, hay que tener en cuenta tres aspectos: procesos reproducibles, conocimientos del ingeniero e indicadores y responsabilidad.

A continuación, se muestran las partes más importantes del informe:

Introducción al ciclo de vida de desarrollo de seguridad

La experiencia en seguridad del software real ha permitido establecer una serie de principios de alto nivel para lograr un software más seguro. Microsoft hace referencia a estos principios como SD3+C – Seguro por diseño, Seguro por definición, Seguro en distribución y Comunicaciones. A continuación, se incluye una breve definición de estos principios:

- Seguro por diseño: la arquitectura, el diseño y la implementación del software se deben realizar de manera que proteja tanto el software como la información que procesa, además de poder resistir ataques.

- Seguro por definición: en el mundo real, el software no es nunca totalmente seguro, por lo que los diseñadores deben asumir que habrá errores de seguridad. Para minimizar los daños que se producirán cuando los atacantes descubran estos errores, el estado predeterminado del software debe elegir las opciones más seguras. Por ejemplo, el software debe ejecutarse con los mínimos privilegios necesarios y los servicios y las características que no sean necesarios de manera habitual deben deshabilitarse de manera predeterminada o establecer que sólo unos pocos usuarios puedan tener acceso a ellos.

- Seguro en distribución: se debe incluir con el software información y herramientas que ayuden a los administradores y a los usuarios a utilizar este software con seguridad. Además, la implementación de las actualizaciones debe ser sencilla.

- Comunicaciones: los programadores de software deben estar preparados para detectar las vulnerabilidades de seguridad del producto y deben comunicarse de manera abierta y responsable con los usuarios y los administradores para ayudarles a tomar las medidas de protección

adecuadas (como la actualización o la implementación de soluciones alternativas).

Aunque todos los elementos de SD3+C imponen ciertos requisitos durante el proceso de desarrollo, los dos primeros elementos, seguro por diseño y seguro por definición, son los que más favorecen la seguridad. Seguro por diseño obliga a utilizar procesos que tratan de evitar la inclusión de vulnerabilidades de seguridad desde el principio, mientras que Seguro por definición exige que la exposición predeterminada del software, la "superficie de ataque", sea la mínima posible.

El proceso de ciclo de vida de desarrollo de seguridad

Como se comentó anteriormente, este artículo no está destinado a ampliar los conocimientos del ingeniero. No obstante, es importante señalar que el programa de educación es básico para que el SDL se realice correctamente. Al terminar los estudios universitarios o profesionales sobre informática y disciplinas afines, por lo general no se disponen de los conocimientos necesarios para comenzar a trabajar en un equipo destinado al diseño, el desarrollo o la prueba de software seguro. Incluso si se han realizado cursos sobre seguridad, es más probable que se hayan estudiado algoritmos de cifrado y modelos de control de acceso que saturaciones de búfer y errores de resolución de nombres canónicos. En general, los diseñadores de software, los ingenieros y los encargados de las pruebas también carecen de los conocimientos adecuados sobre seguridad.

Teniendo esto en cuenta, toda organización que quiera desarrollar software seguro deberá asumir la responsabilidad de asegurarse de que sus empleados adquieren los conocimientos necesarios. La manera concreta de hacerlo depende del tamaño de la organización y los recursos disponibles. Una organización con un gran número de ingenieros puede crear un programa de educación interno que proporcione a sus ingenieros los conocimientos de seguridad de manera continua, mientras que una organización de menor tamaño es posible que deba recurrir a servicios de enseñanza externos. En Microsoft, todo el personal implicado en el desarrollo de software acude todos los años a un curso de "puesta al día en seguridad".

Fase de requisitos

La necesidad de considerar la seguridad "de abajo a arriba" es uno de los principios fundamentales del desarrollo de sistemas seguros. Teniendo en cuenta que muchos proyectos de desarrollo generan la siguiente versión a partir

de la anterior, la fase de requisitos y el planeamiento inicial de una nueva versión o lanzamiento ofrece una oportunidad estupenda para crear software seguro.

Durante la fase de requisitos, el equipo de producto se pone en contacto con el equipo de seguridad central para solicitar la asignación de un asesor de seguridad (conocido como el encargado de la seguridad en la implementación del SDL en Microsoft) que actúa como punto de contacto, recurso y guía a través de los procedimientos de planeamiento. El asesor de seguridad ayuda al equipo de producto revisando los planes, aportando recomendaciones y asegurándose de que el equipo de seguridad planea los recursos necesarios de acuerdo con el programa de fechas del equipo de producto. El asesor de seguridad advierte al equipo de producto de los puntos básicos de seguridad y los criterios de salida que serán necesarios en función del tamaño, la complejidad y los riesgos del proyecto. El asesor de seguridad actúa como contacto entre el equipo de producto y el equipo de seguridad desde el inicio del proyecto hasta la finalización de la revisión final de seguridad y el lanzamiento del software. Este asesor también actúa como contacto entre el equipo de seguridad y la administración del equipo de producto, informando a este último del correcto avance de la seguridad del proyecto para evitar sorpresas de última hora relacionadas con la seguridad.

La fase de requisitos es la oportunidad ideal para que el equipo de producto se plantee cómo se integrará la seguridad en el proceso de desarrollo, identifique los objetivos de seguridad clave y, por lo demás, maximice la seguridad del software procurando minimizar el impacto sobre los planes y los programas. Como parte de este proceso, el equipo debe considerar cómo se integrarán las características de seguridad y las medidas de control con otros programas que probablemente se utilizarán con el software que están desarrollando. (El funcionamiento con otros programas es vital para responder a la necesidad de los usuarios de integrar los productos en sistemas seguros.) La consideración general por parte del equipo de producto de los objetivos, los retos y los planes de seguridad debe reflejarse en los documentos de planeamiento generados durante la fase de requisitos. Aunque es posible que estos planes cambien a medida que el proyecto avanza, articularlos desde el principio garantiza que no se pasa por alto ningún requisito ni surgen sorpresas de última hora.

Cada equipo de producto debe considerar los requisitos de características de seguridad como parte de esta fase. Aunque algunos requisitos de características de seguridad aparecerán a partir del modelo de amenazas, es probable que sean los requisitos de los usuarios los que dictaminen la inclusión de características de seguridad como respuesta a las demandas de los clientes. Los requisitos de características de seguridad también surgirán a partir de la

necesidad de cumplir los estándares del sector y los procesos de certificación, como los criterios comunes. El equipo de producto debe detectar y reflejar estos requisitos como parte de su proceso de planeamiento normal.

Fase de diseño

La fase de diseño identifica la estructura y los requisitos globales del software. Desde el punto de vista de la seguridad, los elementos clave de la fase de diseño son:

- Definir la arquitectura de seguridad y las directrices de diseño: definir la estructura global del software desde el punto de vista de la seguridad e identificar los componentes cuyo correcto funcionamiento es esencial para la seguridad (la "base de computación confiable"). La identificación de técnicas de diseño, como el uso de capas o lenguaje con tipos inflexibles, la aplicación de privilegios mínimos y la minimización de la superficie de ataque, que se aplican al software de manera global. (El uso de capas se refiere a la organización del software en componentes bien definidos que se estructuran para evitar dependencias circulares entre componentes. Los componentes se organizan en capas y una capa superior puede depender de los servicios de capas inferiores, pero se prohíbe que las capas inferiores dependan de las capas superiores.) Los detalles específicos de cada uno de los elementos de la arquitectura se indican en las especificaciones de diseño individuales, pero la arquitectura de seguridad corresponde a una perspectiva global sobre el diseño de seguridad.
- Documentar los elementos de la superficie de ataque del software. Teniendo en cuenta que el software no logrará una seguridad perfecta, es importante que únicamente se expongan de manera predeterminada las características que utilicen la mayoría de los usuarios y que dichas características se instalen con el mínimo nivel de privilegios posible. La medición de los elementos de la superficie de ataque ofrece al equipo de producto un indicador continuo de la seguridad predeterminada y les permite detectar las instancias en las que el software es más susceptible de recibir ataques. Aunque algunas instancias con mayor superficie de ataque pueden estar justificadas por una mayor facilidad de uso o unas mejores funciones del producto, es importante detectar y considerar cada una de estas instancias durante el diseño y la implementación para lanzar el software con la configuración predeterminada más segura posible.
- Realizar un modelado de las amenazas. El equipo debe realizar un modelado de amenazas por componentes. Mediante una metodología estructurada, el equipo de componentes identifica los activos que debe administrar el software y las interfaces que permitirán el acceso a dichos activos. El proceso de modelado de

amenazas identifica las amenazas que pueden dañar a estos activos y la probabilidad de que se inflija dicho daño (estimación del riesgo). A continuación, el equipo de componente identifica las contramedidas que pueden mitigar el riesgo, ya sea mediante características de seguridad (por ejemplo, el cifrado) o mediante un funcionamiento correcto del software que proteja a los activos del daño. Por tanto, el modelado de amenazas ayuda al equipo de producto a identificar las necesidades de características de seguridad y las áreas en las que es necesario revisar con especial minuciosidad el código y probar la seguridad. El proceso de modelado de amenazas debe realizarse con una herramienta capaz de capturar modelos de amenazas en un formato que pueda leer un equipo para almacenarlo y actualizarlo.

- Definir los criterios de publicación adicionales. Aunque los criterios de publicación de seguridad básicos deben definirse para toda la organización, puede que existan criterios concretos para determinados equipos de producto o lanzamientos de software que sea preciso cumplir para poder lanzar el software. Por ejemplo, un equipo de producto dedicado al desarrollo de una versión actualizada del software que se enviará a los clientes y que está expuesta a un gran número de ataques puede optar por exigir que la nueva versión no presente ninguna de las vulnerabilidades de seguridad detectadas durante cierto tiempo antes de considerar que está lista para su lanzamiento. (Es decir, el proceso de desarrollo debe descubrir las vulnerabilidades de seguridad y solucionarlas antes de que se detecten, en vez de tener que solucionarlas después de su detección.)

Fase de implementación

Durante la fase de implementación, el equipo de producto programa, prueba e integra el software. Los pasos destinados a eliminar los errores de seguridad o a impedir que se incluyan desde el principio son de gran utilidad, ya que reducen considerablemente la probabilidad de que las vulnerabilidades de seguridad lleguen a la versión final del software que se lanzará a los clientes.

Los resultados del modelado de amenazas ofrecen una orientación especialmente importante durante la fase de implementación. Los programadores deben asegurarse de que escriben correctamente el código para mitigar las amenazas de alta prioridad, mientras que los encargados de las pruebas deberán asegurarse de que estas amenazas se han bloqueado o mitigado de manera efectiva.

Los elementos del SDL que se aplican en la fase de implementación son:

- Aplicar estándares de codificación y de pruebas. Los estándares de codificación evitan que los programadores incluyan errores que puedan producir vulnerabilidades de seguridad. Por ejemplo, el uso de construcciones de manipulación de búferes y de manejo de cadenas más seguras y coherentes ayuda a evitar la aparición de vulnerabilidades de seguridad de saturación del búfer. Los estándares de pruebas y las prácticas recomendadas permiten garantizar que las pruebas se centran en detectar posibles vulnerabilidades de seguridad, en vez de centrarse únicamente en el funcionamiento correcto de las características y las funciones del software.
- Aplicar herramientas de comprobación de seguridad, incluidas herramientas de confusión. Estas herramientas ofrecen entradas estructuradas pero no válidas a las interfaces de programación de aplicaciones (API) de software y a las interfaces de red para maximizar la probabilidad de detectar errores que puedan ocasionar vulnerabilidades de seguridad del software.
- Aplicar herramientas de exploración del código de análisis estático. Las herramientas pueden detectar algunos tipos de errores de codificación que producen vulnerabilidades de seguridad, incluidas saturaciones de búfer, desbordamientos con enteros y variables no inicializadas. Microsoft ha realizado una importante inversión en el desarrollo de este tipo de herramientas (las dos que se han utilizado durante más tiempo son PREfix y PREfast) y mejora continuamente estas herramientas a medida que surgen nuevos tipos de errores de codificación y vulnerabilidades de seguridad del software.
- Realizar revisiones del código. Las revisiones del código complementan las herramientas automatizadas y las pruebas, ya que aplican el esfuerzo de programadores expertos para examinar el código fuente y detectar y eliminar posibles vulnerabilidades de seguridad. Estas revisiones constituyen un paso fundamental para eliminar las vulnerabilidades de seguridad del software durante el proceso de desarrollo.

Fase de comprobación

La fase de comprobación es el punto en el que software ya incorpora toda la funcionalidad y los usuarios pueden comenzar a probar la versión beta. Durante esta fase, mientras se prueba la versión beta del software, el equipo de producto realiza una campaña de seguridad que incluye revisiones del código de seguridad aparte de las realizadas en la fase de implementación, así como la realización de pruebas centradas en la seguridad.

Microsoft realizó campañas de seguridad durante la fase de comprobación de Windows Server 2003 y otras versiones de software a principios de 2002. Existían dos motivos para introducir la campaña de seguridad en el proceso:

- El ciclo de vida del software de las versiones en cuestión había alcanzado la fase de comprobación, que era un punto adecuado para realizar las revisiones del código y las pruebas necesarias.
- La realización de la campaña de seguridad durante la fase de comprobación asegura que la revisión del código y las pruebas se realizan con la versión terminada del software y ofrece una oportunidad de revisar tanto el código desarrollado o actualizado durante la fase de implementación como el código heredado que no se ha modificado.

El primero de estos motivos refleja un accidente histórico: la decisión de iniciar una campaña de seguridad se tomó en principio durante la fase de comprobación. Pero Microsoft ha llegado a la conclusión de que es una buena idea realizar una campaña de seguridad durante esta fase, tanto para asegurar que el software final cumple los requisitos como para permitir una revisión en detalle de todo el código heredado de versiones anteriores del software.

Hay que resaltar que las revisiones del código y las pruebas del código de alta prioridad (código que forma parte de la "superficie de ataque" del software) son esenciales para varias partes del SDL. Por ejemplo, estas revisiones y pruebas deben ser obligatorias en la fase de implementación para corregir cuanto antes los problemas, así como para identificar y corregir los orígenes de dichos problemas. También son fundamentales en la fase de comprobación cuando esté a punto de finalizarse.

Fase de lanzamiento

Durante la fase de lanzamiento, el software debe someterse a una revisión final de seguridad (FSR). Esta FSR debe responder a la siguiente pregunta: "Desde el punto de vista de la seguridad, ¿está este software preparado para los clientes?" La FSR se realiza en un plazo de dos a seis meses antes de la finalización del software, según el alcance del software. El software debe ser estable antes de la FSR y es de esperar que antes del lanzamiento sólo se realicen cambios mínimos y no relacionados con la seguridad.

La FSR es una revisión independiente del software que realiza el equipo de seguridad central de la organización. El asesor de seguridad del equipo de seguridad aconseja al equipo de producto sobre el ámbito de la FSR que requiere el software y ofrece al equipo de producto una lista de los requisitos de recursos

antes de la FSR. El equipo de producto proporciona al equipo de seguridad los recursos y la información necesarios para llevar a cabo la FSR. Al comienzo de la FSR, el equipo de producto debe rellenar un cuestionario y entrevistarse con un miembro del equipo de seguridad asignado a la FSR. En toda FSR se deben revisar los errores que se identificaron en un principio como errores de seguridad, pero que tras analizarlos se consideró que no afectaban a la seguridad, para asegurarse de que este análisis es correcto. Una FSR también incluye una revisión de la capacidad del software para soportar vulnerabilidades de seguridad detectadas recientemente en un software similar. Una FSR para una versión de software importante requerirá realizar pruebas de penetración y, posiblemente, recurrir a asesores de revisión de seguridad externos que ayuden al equipo de seguridad.

La FSR no es únicamente un examen que se puede aprobar o suspender ni tampoco pretende detectar todas las vulnerabilidades de seguridad que quedan en el software, lo que no sería factible, sino proporcionar al equipo de producto y a la administración superior de la organización una idea global del nivel de seguridad del software y de la probabilidad de que pueda resistir ataques una vez que se haya entregado a los clientes. Si la FSR detecta patrones de vulnerabilidades de seguridad restantes, no bastará con solucionar las vulnerabilidades detectadas, sino que habrá que repetir la fase anterior y tomar las acciones necesarias para tratar los orígenes (por ejemplo, mejorar los conocimientos, mejorar las herramientas).

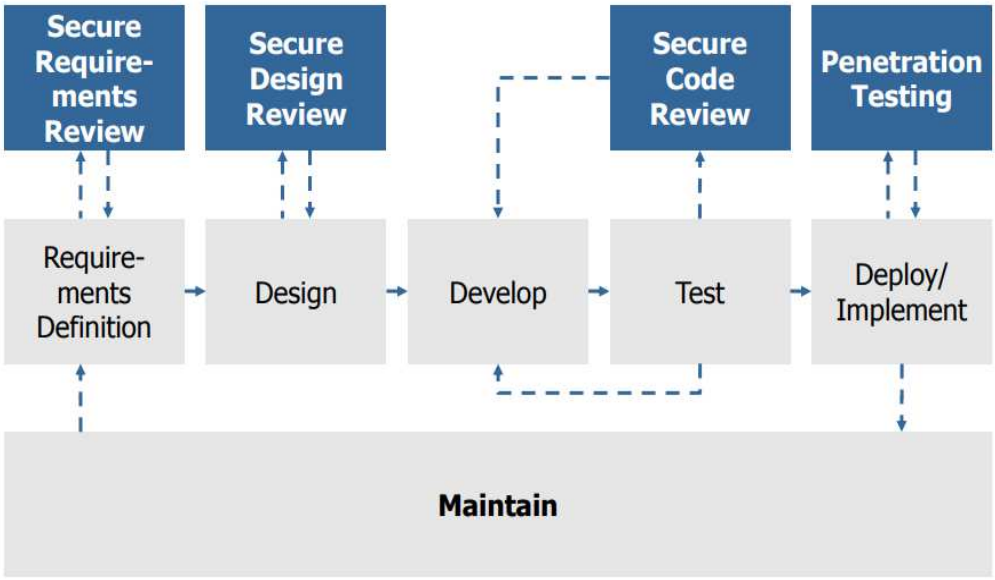
Fase de servicio técnico y mantenimiento

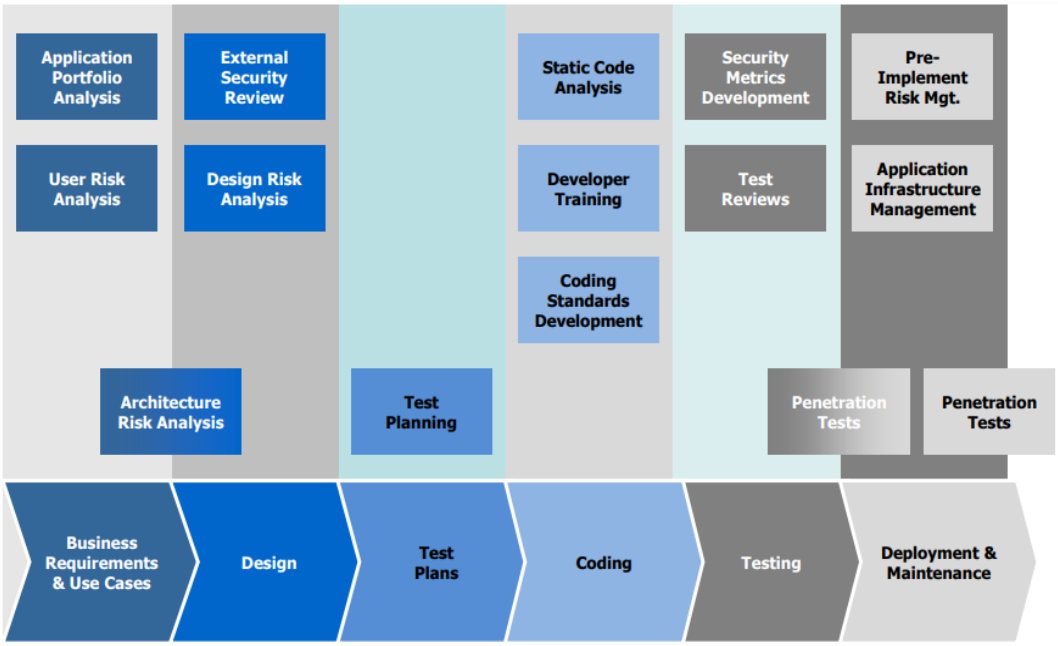
A pesar de la aplicación del SDL durante el desarrollo, las prácticas de desarrollo más avanzadas no consideran que se pueda publicar software que no tenga ninguna vulnerabilidad de seguridad (y hay buenos motivos para creer que siempre será así). Incluso aunque el proceso de desarrollo pudiera eliminar todas las vulnerabilidades de seguridad del software que se va a publicar, se descubrirían nuevos ataques y el software considerado "seguro" pasaría a ser vulnerable. Por tanto, los equipos de producto deben prepararse para responder a nuevas vulnerabilidades en el software que se entrega a los clientes.

Parte del proceso de respuesta consiste en la preparación para evaluar los informes de vulnerabilidades y lanzar consejos y actualizaciones de seguridad siempre que sea necesario. El otro componente del proceso de respuesta consiste en realizar una autopsia de las vulnerabilidades detectadas y tomar las medidas oportunas. Estas medidas pueden oscilar desde el lanzamiento de una actualización que resuelva un error aislado hasta la actualización de las herramientas de actualización del código para iniciar

revisiones de código de los subsistemas principales. El objetivo durante la fase de respuesta consiste en aprender de los errores y utilizar la información de los informes de vulnerabilidades para detectar y eliminar otras vulnerabilidades antes de que se descubran en la práctica y se utilicen para poner en peligro a los clientes. El proceso de respuesta también ayuda a los equipos de producto y de seguridad a adaptar los procesos para que otros errores similares no se repitan en el futuro.

Comparando con la información que vemos en OWASP, podemos observar algunas similitudes en Microsoft[7], en el siguiente gráfico:





Hay una frase, dentro de la experiencia de Microsoft, que no se mencionó anteriormente, que dice “no se puede controlar lo que no se puede medir”, lo que me lleva a mencionar la importancia de las métricas para poder controlar y medir qué cubrimos y qué no. Otra mención importante es que, puede ser que la empresa no tenga especialista en Seguridad, y en estos casos, lo ideal, sería contratar a personal externo tanto para que ofrezcan consultoría, como también, capacitación.

Si bien ambos ejemplos, tienen sus similitudes, el que está mejor explicado, es el de Microsoft.

Metodología y Frameworks de Testeo de la Seguridad de las Aplicaciones

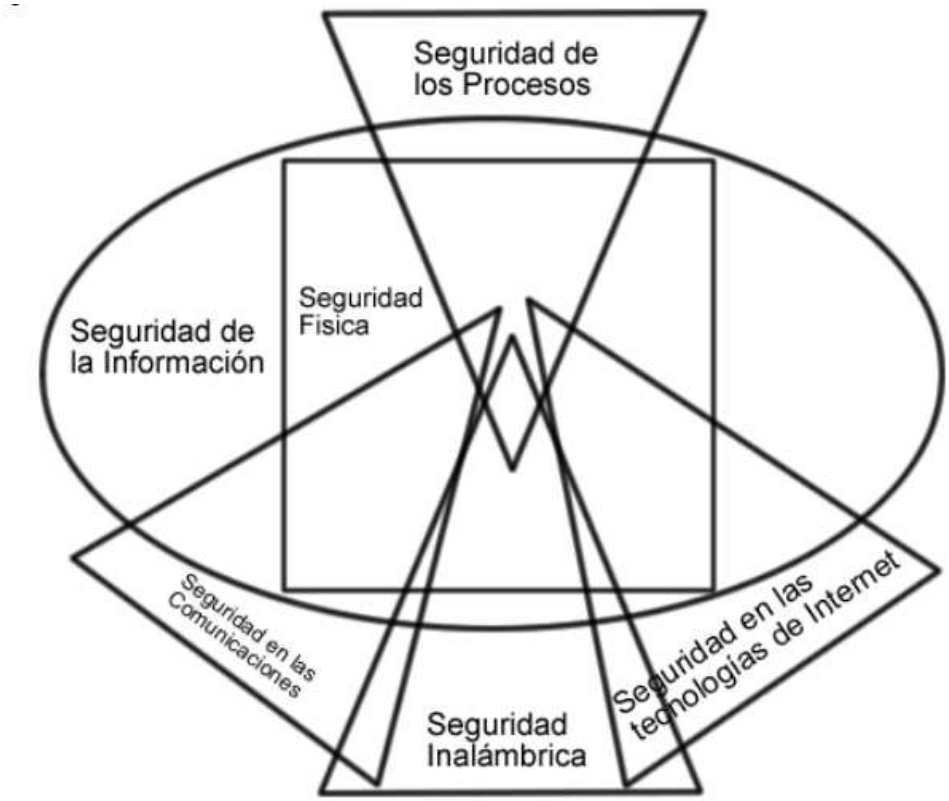
En un sitio de España [10], encontré que utilizan la siguiente metodología para testear la seguridad de las aplicaciones:

OSSTMM

El “Manual de la Metodología Abierta de Testeo de Seguridad” se ha convertido en un estándar de facto. Sin duda supuso el primer acercamiento a una estructura global de concepto de seguridad. Si bien las pruebas incluidas y los test que se ejecutan no son especialmente innovadores, se ha convertido en una auténtica referencia para los organismos que quieren desarrollar un Testing de calidad, ordenado y eficiente.

Para organizar estructurar su contenido, la metodología se subdivide en los aspectos más importantes de los sistemas de información. Se destacan los siguientes aspectos como:

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



De manera sencilla se identifican una serie de actividades de testeo específicas por área, sobre las que se comprueban las especificaciones de seguridad, integradas con las verificaciones realizadas en las revisiones rutinarias.

Con esta metodología, se realiza un esfuerzo para convertir en predecible QUE se debe de probar, COMO se puede hacer y CUANDO es necesario ejecutarlo. De esta manera se aumenta la calidad del desarrollo, ya que la seguir esta metodología, se tiene la certeza de que se cumplen unos objetivos prefijados.

Un aspecto importante de esta metodología, es que no solo se centra en los aspectos eminentemente técnicos de seguridad tradicionales, sino que abarca aspectos sobre los responsables del testeo. Trata de estandarizar las credenciales del desarrollador a cargo del test, el formato de los resultados, crear un código ético, un plan temporal de ejecución, etc… Un aspecto muy importante de la metodología, es la incorporación del concepto de Valores de Evaluación de Riesgo, que permiten diferenciar y clasificar las diferentes problemáticas.

OSSTMM plantea categorizaciones estándar, que permiten identificar claramente el alcance de cada una de las actividades, evitando inconvenientes en tal sentido:

Búsqueda de Vulnerabilidades: Orientado principalmente a realizar comprobaciones automáticas de un sistema o sistemas dentro de una red.

Escaneo de la Seguridad: Orientado a las búsquedas principales de vulnerabilidades en el sistema que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles en el sistemas y análisis individualizado.

Test de Intrusión: Se plantean test de pruebas que se centran en romper la seguridad de un sistema determinado.

Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

Auditoria de Seguridad: Se refiere a la continua inspección que sufre el sistema por parte de los administradores que controlan que se cumplan las políticas de seguridad definidas.

Hacking Ético: Orientado a tratar de obtener, a partir de los test de intrusión, objetivos complejos dentro de la red de sistemas.

A continuación, se muestra el proceso en el que se basa este manual de procedimientos:

El proceso de un análisis de seguridad, se concentra en evaluar las siguientes areas, que reflejan los niveles de seguridad presentes, siendo estos el ambiente definido para el análisis de seguridad. Estos son conocidos como las Dimensiones de Seguridad:

Visibilidad: La visibilidad es lo que puede verse, registrarse, o monitorearse en el nivel de seguridad con o sin la ayuda de dispositivos electrónicos. Esto incluye, pero no se limita a, ondas de radio, luz por encima del espectro visible, dispositivos de comunicación como teléfonos, GSM, email y paquetes de red como TCP/IP.

Acceso: El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física. Esto puede incluir, pero no se limita a, una página web, una ventana, una conexión de red, ondas de radio, o cualquier cosa cuya ubicación soporte la definición de casi-público o donde un computador interactúa con otro por medio de una red. Limitar el acceso significa negar todo excepto lo que este expresamente permitido financieramente y por buenas prácticas.

Confianza: La confianza es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.

Autenticación: La autenticación es la medida por la cual cada interacción en el proceso está privilegiada.

No-repudio: El no-repudio provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.

Confidencialidad: La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.

Privacidad: La privacidad implica que el proceso es conocido únicamente por los sistemas o partes involucradas.

Autorización: La autorización es la certeza que el proceso tiene una razón o justificación de negocios y es administrado responsablemente dando acceso permitido a los sistemas.

Integridad: La integridad es la certeza que el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reversado sin el conocimiento de los sistemas o partes involucradas.

Seguridad: La seguridad son los medios por los cuales un proceso no puede dañar otros sistemas, o procesos incluso en caso de falla total del mismo. Alarma La alarma es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad. En la mayoría de violaciones de seguridad, la alarma es el único proceso que genera reacción.

ISSAF

ISSAF, de OISSG (Open Information System Security Group) ha presentado formalmente su versión “Draft 0.2". Es uno de los frameworks más interesantes dentro del ámbito de metodología de testeo. Realiza un análisis detallado de todos los posibles aspectos que afectan al testeo de seguridad.

La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar “Criterios de Evaluación”, cada uno de los cuales ha sido escrito y revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez, se componen de los siguientes ítems:

- Una descripción del criterio de evaluación.
- Puntos y objetivos a cubrir.
- Los prerrequisitos para conducir la evaluación.
- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y Documentación Externa.

Para organizar de forma sistemática las labores de testeo, dichos “Criterios de Evaluación”, se han catalogado, desde los aspectos más generales, como pueden ser los conceptos básicos de la “Administración de Proyectos de Testeo de Seguridad”, hasta técnicas tan puntuales como la ejecución de pruebas de Inyección de Código SQL o como las “Estrategias del Cracking de Contraseñas”.

OTP

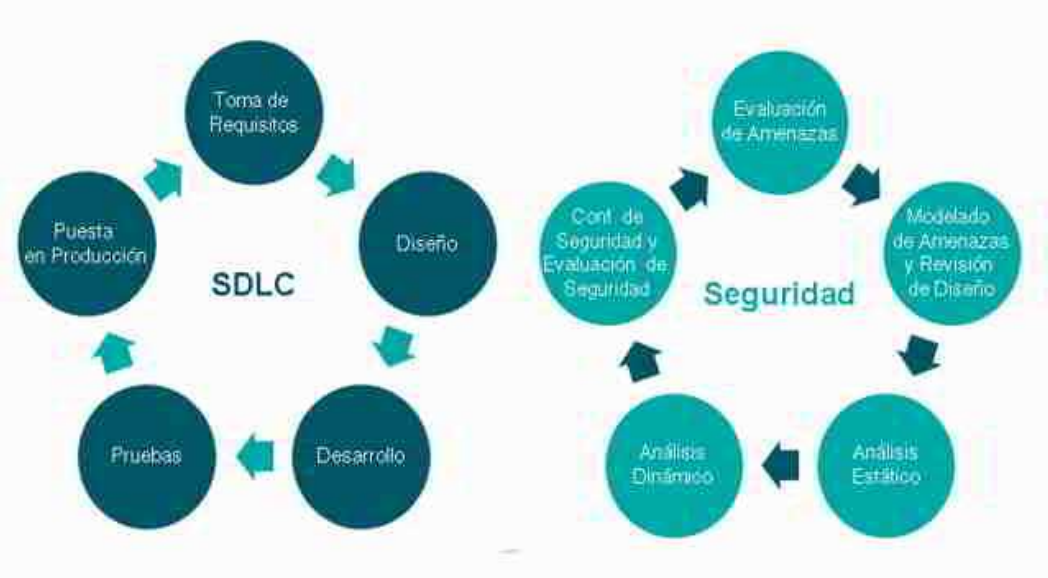
“OWASP Testing Project” (OTP), está muy orientado a realizar pruebas sobre aplicaciones Web y está en el camino de convertirse en uno de los proyectos referencia en su ámbito. OWASP, ha conseguido ser una referencia habitual para cualquier desarrollador en el ámbito de la seguridad. OTP en particular, se encuentra enfocado a responder preguntas tales como: ¿qué?, ¿por qué?, ¿cuándo?, ¿dónde? y ¿cómo? testear una aplicación web. Se cubren los siguientes puntos:

- El alcance de que testear.
- Principios del testeo.
- Explicación de las técnicas de testeo.
- Explicación general acerca del framework de testeo de OWASP.
-

OTP incorpora en su metodología de testeo, aspectos claves relacionados con el “Ciclo de Vida del Desarrollo de Software” a fin de que el “ámbito” del testeo a realizar, comience mucho antes de que la aplicación web se encuentre en producción

De este modo, y teniendo en cuenta que un programa efectivo de testeo de aplicaciones web, debe incluir como elementos a testear: Personas, Procesos y Tecnologías, OTP delinea en su primer parte conceptos claves a la vez que introduce un framework específicamente diseñado para evaluar la seguridad de aplicaciones web a lo largo de su vida.

Cerrando esta etapa de informe del trabajo de especialización, encontré un gráfico muy interesante que compara el ciclo de vida del desarrollo de software con la seguridad de la información [9]:



Cada etapa del Ciclo de Vida del Desarrollo de Software se corresponde con alguna de las acciones que implican brindarle seguridad a nuestra aplicación, comenzando desde el momento cero, que es el de la toma de requisitos.

Por otro lado, otro gráfico interesante que muestra el sitio, el que nos da una visión de los costos que nos implican las correcciones si no aplicamos la seguridad desde el inicio del Ciclo de Vida, cuanto más tarde las detectemos, más costoso nos va a resultar atacarlas:


Coste
Toma de Requisitos
Diseño
Desarrollo
Pruebas
Puesta en Producción
Fases del Ciclo de Vida

Conclusiones:

Se viene de una época en la cual se le prestaba poca atención a la seguridad en las aplicaciones, quizás se le prestaba más atención a securizar los servidores, las comunicaciones y con éso alcanzaba. Con el correr del tiempo y el uso masivo de las aplicaciones para realizar la mayoría de los trámites, consultas, etc que hacíamos personalmente, en forma online, se hace necesario que nuestras aplicaciones sean cada vez más robustas en cuanto a la seguridad de la información. Esto sucede para que puedan cumplir los tres pilares de la misma: Confidencialidad, Integridad y Disponibilidad de la Información. Información que hoy día es: personal, financiera, económica, sensible y no sensible, pero que de ninguna manera puede caer en manos de algún atacante.

Es por ello, que cada vez se hace más necesario que se piense en la seguridad desde el inicio de la concepción de las aplicaciones, desde el análisis, el relevamiento, el diseño y principalmente, en el desarrollo de la mismas, dando importancia también en la parte de testing, donde se refuerzan las verificaciones. Pero también es muy importante no olvidarnos cuando se encuentra productiva, incluyendo logs y monitoreos que nos permitan estar atentos a cualquier posible ataque y que no nos tome desprevenidos.

En fin, hay que dejar de lado las frases como: “No hay tiempo para pensar en la seguridad ahora”, “Salgamos a producción así y después lo vemos”, “Los desarrolladores no están capacitados y no es una incumbencia del desarrollo”. Hay que comenzar a capacitar a nuestros desarrolladores para que nuestras aplicaciones sean cada vez más robustas también a nivel seguridad de la información, brindarles las herramientas necesarias para poder estar capacitados.

Me ha pasado en trabajos anteriores, que la seguridad llega recién en el punto que la aplicación está por salir a producción, con lo cual, antes de que esto ocurra, se pasa por un pentesting y “si tenemos tiempo” corregimos las más críticas y después, vamos corrigiendo las demás. El “después”, muy pocas veces llega, y se termina saliendo a producción con vulnerabilidades conocidas por todos. Es una pena que en muchos lugares no se le dé la importancia necesaria a la seguridad informática, hasta que ocurre algún incidente, ya que muchas veces no basta con securizar las comunicaciones, ya que muchas veces la filtración puede ser interna, quizás por desconocimiento de uso.

Creo que un modelo muy útil para utilizar y que puede ser tomado como ejemplo, es el que utiliza Microsoft en el Ciclo de Vida del Desarrollo de Software, ya que abarca todas las etapas y la descripción que se muestra en el trabajo describe claramente cómo incluir la Seguridad en cada una de ellas. La verdad es que, en mi opinión, es un modelo que utilizaría.

Por otra parte, es de mucha utilidad el manual de metodología de testeo de aplicaciones que, si bien recopila buenas prácticas e información de otros países, tiene muchas definiciones y procedimientos a seguir que pueden ser de mucha utilidad para realizar testeos en nuestras aplicaciones.

Quiero además darle mucha importancia a la documentación de la arquitectura, es fundamental que haya una documentación, a veces no es necesario que sea extensa, sino que cubra tanto la arquitectura como la lógica de seguridad que tiene el negocio. Esto es fundamental, por ejemplo, en el caso de que ingrese una persona a trabajar. Me ha pasado ingresar a un lugar de trabajo en donde no había nada de documentación y quizás se cometían errores de seguridad de lógica de negocio por desconocimiento. Este problema se agrava aún más si la empresa tiene alta rotación de empleados.

Otro de los errores que veo habitualmente es pensar que como nuestra aplicación ya se encuentra productiva, nos olvidamos, ya está, hicimos todos los chequeos, salió todo bien y nos olvidamos. Es un grave error ya que estamos dando pie a que nos ataquen, accedan a nuestra información o bien manipulen nuestra aplicación a su gusto. Por ello es muy importante seguir monitoreando nuestra aplicación y verificando los logs continuamente.

Para finalizar, si bien creo que los tiempos han cambiado, también creo que hay muchas empresas que están comenzando a darle importancia a la seguridad de la información, porque, ninguna de ellas quiere hacerse conocida porque alguien publicó información no deseada o accedió a información que no tenía que acceder. Ojo, no sólo estoy hablando de posibles ataques, sino que también puede suceder por aplicar mal la lógica del negocio a nivel seguridad, por ejemplo, actualmente me encuentro trabajando en una empresa de recibos digitales, y uno de los fallos más graves de seguridad es que una empresa pueda acceder a recibos de sueldo de otra, o que un empleado pueda ver recibos de sueldo de otro empleado al que no tiene permisos. Por ello también remarcaba la importancia de la documentación de la arquitectura para conocer y poder aplicar correctamente las políticas de seguridad de la empresa a nivel negocio, y puedo decir, que, en mi caso particular, no se encuentran documentadas, lo cual es un grave error, porque se pueden aplicar vulnerabilidades graves solamente por desconocimiento.

Anexo/Apéndice: Manual de Metodología Abierta de Testeo de Seguridad

INSTITUTE FO R SEC URITY AND O PEN METHODOLOGIES

OSSTMM 2.1.

Manual de la Metodología Abierta de Testeo de Seguridad

Creado por Pete Herzog

Última Versión:	OSSTMM 2.1
Nota:	**Las secciones y módulos todavía están basados en la versión 2.0**. Sin embargo, esta versión tiende un puente hacia la nueva estructura de la próxima versión, 3.0. Luego de un año y medio hemos recabado más que suficiente información que permita asegurar un mejor y mas exhaustivo testeo de seguridad, aunque el formato actual no satisface la estructura deseada para procesar toda la información obtenida. El nuevo formato garantizará que la información permita al máximo la transferencia de conocimiento. **Todo el material actualizado hasta la versión 2.5 inclusive, únicamente será distribuido a nuestros subscriptores.**

Cambios:	Los siguientes cambios están incluidos: legibilidad, estructura del documento, las 6 metodologías fueron actualizadas, leyes actualizadas y prácticas recomendadas, estructura de los lineamientos de acción, reglas basadas en la experiencia, código ético de ISECOM, y cálculo de RAVs.
FECHA DE LA ÚLTIMA VERSION:	Sábado, 23 de agosto de 2003
FECHA DE LA VERSION ORIGINAL:	Lunes, 18 de diciembre de 2000

Colaboradores

Aquellas personas que han contribuido de manera valiosa y consistente han sido listadas aquí, aunque también muchas otras personas deberían recibir nuestro agradecimiento. Cada persona recibe un reconocimiento por el tipo de contribución que ha realizado, pero no se menciona lo que exactamente ha contribuido cada colaborador. La no revelación de las contribuciones personales a este documento se utiliza con el propósito de evitar prejuicios y para promover las nuevas ideas. Si UD está interesado en colaborar, por favor acceda al sitio web de ISECOM para obtener más información.

CREADO POR:	Pete Herzog	Director de ISECOM - pete<at>isecom.org
ORGANIZADORES:	Marta Barceló Robert E. Lee Rick Tucker Nigel Hedges Colby Clark Tom O'Connor Andrea Barisani Gary Axten Marco Ivaldi Raoul Chiesa	*Directora Adjunta de ISECOM* - marta<at>isecom.org *Vice Presidente de la Junta Directiva de ISECOM* - robert<at>isecom.org *Asesor de la Junta Directiva de ISECOM* - rick<at>isecom.org nigel.hedges<at>ca.com colby<at>isecom.org tom91<at>elivefree.net lcars<at>infis.univ.trieste.it gary.axten<at>lineone.net raptor<at>medíaservice.net raoul<at>medíaservice.net
ASISTENTES:	Dru Lavigne Felix Schallock Anton Chuvakin Efraín Torres Lluís Vera Rogelio M. Azorín Richard Feist Rob J. Meijer John Pascuzzi Miguel Ángel de Cara L Chris N Shepherd Darren Young Clemens Wittinger Nabil Ouchn Sean Cocat Leonardo Loro Carles Alcolea	*Gerente del OPRP de ISECOM* - dru<at>isecom.org felix.schallock<at>e-security-net.de anton<at>chuvakin.org et<at>cyberspace.org lvera<at>isecb.com rma<at>isecb.com rfeist<at>nyxtec.net rmeijer<at>xs4all.nl johnpas<at>hushmail.com miguelangel.decara<at>dvc.es chris.shepherd<at>icctcorp.com darren<at>younghome.com cwr<at>atsec.com nouchn<at>net2s.com scocat<at>remingtonltd.com leoloro<at>microsoft.com calcolea<at>menta.net claudia.kottmann<at>gmx.net

	Claudia Kottmann	
COLABORADORES:	Jaume Abella Travis Schack Andre Maxwell John Regney Peter Klee Martin Pivetta Daniel Fdez Bleda Clément Dupuis Waidat Chan Josep Ruano Bou Tyler Shields Javier Fdez. Sanguino Vicente Aguilera John Rittinghouse Kris Buytaert Xavier Caballé Brennan Hay	jaumea<at>salleurl.edu travis<at>vitalisec.com amaxwel3<at>bellsouth.net sregney<at>gedas.es klee<at>de.ibm.com martin.pivetta<at>itatwork.com dfernandez<at>isecauditors.com cdupuis<at>cccure.org waidat<at>interrorem.com jruano<at>capside.com tcroc<at>cow.pasture.com jfernandez<at>germinus.com vaguilera<at>isecauditors.com jwr<at>rittinghouse.homeip.net buytaert<at>stone-it be xavi<at>caballe.com hayb<at>ncr.disa.mil

ASISTENTES Y COLABORADORES ANTERIORES:	Rafael Ausejo Prieto Debbie Evans Daniel R. Walsh Juan Antonio Cerón Jordi Martínez Barrachina Michael S. Hines Miguel Ángel Domínguez Torres Rich Jankowski Manuel Fernando Muiños Gómez Kevin Timm Sacha Faust Ángel Luis Uruñuela José Luis Martín Mas Vincent Ip Anders Thulin Marcus M. Andersson	rafael<at>ausejo.net Debbie.Evans<at>dsnuk.com daniel.walsh<at>Total-Trust.com ja_ceron<at>terra.es jordi<at>security.gft.com mshines<at>purdue.edu mdominguez<at>security.gft.com richj<at>lucent.com mmuinos<at>dsecurity.net ktimm<at>var-log.com sacha<at>severus.org alum<at>phreaker.net jose.l.martin<at>dvc.es vincentiptingpong<at>hotmail.com anders.x.thulin<at>telia.se marcus.m.andersson<at>telia.se

TRADUCCIÓN:

COORDINACIÓN	Marta Barceló	marta<at>isecom.org
TRADUCCION/REVISIÓN	Gabriel O. Zabal Gabriel Crivelli	gabriel<at>alt126.com gcrivelli<at>femechaco.com

AGRADECIMIENTOS A	Fabián G. Chiera Xavier Carbonell Jose Nicolas Castellano Ezequiel M. Sallis Carlos Fragoso Mariscal Hernán Marcelo Racciatti Javier Fernandez-Sanguino Andres Mauricio Mujica	fabian.chiera<at>e-risk.com.ar xcarbonell<at>isecauditors.com josenicolas<at>debaleares.net ezequiel.sallis<at>e-risk.com.ar cfragoso<at>cesca.es hracciatti<at>hotmail.com jfernandez<at>germinus.com linux<at>seaq.com.co

Organizadores: Esta designación es para aquellos individuos que han aportado su tiempo y energía en crear un mejor OSSTMM. Para ello fue necesario volver a redactar secciones completas, mejorar los módulos y el desarrollo de los lineamientos de acción.

Asistentes: Esta designación es para aquellos individuos que han contribuido de modo significativo con ideas, diseños y desarrollo del OSSTMM. Esto incluye reescrituras de secciones, colaboración en los módulos y una edición significativa del documento.

Colaboradores: Esta designación es para aquellos individuos que han realizado esfuerzos significativos en la promoción y explicación del manual OSSTMM en nombre de ISECOM. Esto requirió la escritura de artículos y publicaciones, mejoras en el OSSTMM y un soporte regular de conocimiento.

Asistentes y Colaboradores Anteriores: Esta designación es para aquellos individuos cuyas ideas y trabajo aún persiste en las versiones actualizadas del OSSTMM pero que ya no contribuyen de manera regular con el mismo. Aquellos que han solicitado no continuar afiliados por razones gubernamentales o corporativas, han sido dados de baja.

Prólogo

En las versiones anteriores del OSSTMM, el enfoque principal estaba en QUÉ hacemos como testeadores de seguridad. Debido al éxito de esas ediciones y la creciente aceptación del OSSTMM en la comunidad de seguridad de TI, he tenido el prolongado placer de tratar más extensamente y en detalle el OSSTMM.

Para permitir llevar a cabo esta metodología, he creado las certificaciones de Testeador Profesional de Seguridad OSSTMM (OPST) y de Analista Profesional de Seguridad (OPSA). Además, he tenido el placer de enseñar estos cursos en numerosas ocasiones, y fue durante estas clases que he observado una creciente necesidad de definir PORQUÉ realizamos testeos de seguridad.

Cuando tratamos con seguridad y gestión de riesgos, muchos piensan con respecto a estos aspectos en términos de probabilidades y predecibilidad. Ellos preguntan: ¿Cuales son las chances de que un incidente, amenaza o ataque pueda ocurrir? ¿Cuán predecible es que este evento ocurra?

Si bien es verdadero que algunas defensas son suficientemente proactivas para identificar ataques desconocidos e impredecibles, la mayoría de las organizaciones depende de defensas que estén fortalecidas con una base de datos de los ataques conocidos. Un testeador de intrusión sabe que para contrarrestar las defensas, también debe tener una base de datos actualizada sobre los ataques conocidos. Esto ayuda en la rapidez y la efectividad de cada intento. Una y otra vez, determinados "hacks éticos" serán exitosos, y el testeador apreciará mucho estas joyas de su base de datos de ataques, registrando el índice de éxitos.

Armado de esta información, el testeador de intrusión, intentará abusar de la red de su cliente hasta que uno de sus ataques tenga éxito.

Esta técnica es de lo mejor, sin embargo en la práctica, la organización del cliente se convierte en un casino y los testeadores de intrusión están jugando contra los factores predeterminados por su cliente. Esto es muy similar al hecho de que un apostador esta a merced de los probabilidades impuestas por el casino. Para aquellos que no están familiarizados con los casinos y formas de apostar, es importante entender que los juegos de azar establecidos, como por ejemplo los que se encuentran en un casino, nunca pueden tener una proporción entre ganancia y pérdida de 50/50, porque el casino no ganaría dinero. Por consiguiente, los casinos eligen ofrecer juegos que tengan una relación mayor de pérdida que de ganancia para el apostador, de manera de poder asegurar que el casino gane dinero en un período de tiempo determinado, conocido como "establecer las probabilidades".

Los apostadores que aprenden a "hacer trampas" en los juegos de casino, usan técnicas que alteran esta proporción entre ganancia y perdida en otra dirección. Esto es muy cierto cuando un jugador sabe como jugar un juego incluso mejor que el casino mismo (lo cual es extremadamente raro, pero ocurre), en cuyo caso el casino considera como trampas habilidades que se basan en la memoria como por ejemplo contar las cartas (en blackjack), habilidades como calcular un número extremadamente enorme de variables para apostar según convenga (apostar en deportes y carreras de animales, o algo simple como reconocimiento de patrones

(ruleta).

Los testeadores de intrusión que obtienen acceso privilegiado a través de elevadas habilidades y mejor conocimiento que su cliente es algo a veces visto como "hacer trampas", aunque ellos sólo están cambiando las reglas del juego al sacar provecho de las defensas de seguridad que han sido reducidas al mínimo con la excusa de funcionalidad comercial. Cambiar las reglas del juego es muy distinto a jugar con las reglas y tomar sus propias chances en el testeo. Frecuentemente, el cliente es consciente de los riesgos que son necesarios correr para una mejor funcionalidad comercial. UD no puede abrir una tienda sin invitar a la gente a comprar.

El testeo metódico de seguridad es algo diferente del testeo de intrusión. Se apoya en una combinación de creatividad, extensas bases de conocimiento sobre las metodologías más adecuadas, cuestiones legales y las regulaciones inherentes al área de la industria del cliente, como así también las amenazas conocidas, y el alcance de la seguridad de la empresa objetivo (o puntos de riesgo) para "hacer trampas" en el casino, y por consiguiente definir las propias chances de éxito.

Hacemos esto tomando ventaja de lo predecible y de las mejores prácticas utilizables hasta su mayor alcance posible. En otras palabras, testeamos todos los extremos de lo considerado como

predecible, aprovechando al máximo las mejores prácticas para analizar los escenarios de los peores casos posibles que no son tan predecibles.

En organizaciones verdaderamente comprometidas a reducir tanto como sea posible los riesgos, no es necesario decir que es nuestra obligación como testeadores de seguridad explorar la extensión y la profundidad de los riesgos, de manera de poder identificar adecuadamente estos riesgos durante el testeo del objetivo.

Los tipos de preguntas que debemos hacernos continuamente durante el proceso de testeo son: ¿Qué bienes puedo acceder en qué momento para provocar el máximo riesgo de seguridad? ¿Bajo qué circunstancias encuentro la mayor parte de las vulnerabilidades? ¿Cuándo estoy más propenso a aplicar confidencialidad, integridad y accesibilidad al test? Manteniéndose sistemático y persistente, el efecto acumulativo de estos tests dará como resultado un panorama exacto de los riesgos, debilidades, filtraciones de información y vulnerabilidades. Esto nos ayudará tremendamente con cualquier justificación de negocio de resguardo, como así también satisfará los requisitos regulativos/legales a través de los debidos recaudos y la diligencia.

Los siguientes puntos lo ayudarán adecuadamente al crear y llevar a cabo sus tests de seguridad de altos estándares:

- ***Cuándo* testear es tan importante como *qué* testear y *porqué* testear.**

Esperar para hacer el test, esperar para reportar los problemas y esperar para solucionarlos, es un error. Cuando UD deja su casa al irse de vacaciones, ¿UD espera hasta su retorno para asegurarse de haber cerrado con llaves las puertas? Por supuesto que no. UD echó llave a la puerta y forcejeó el pomo de la misma para asegurarse de que estaba cerrada. Esperar hasta su retorno para comprobarlo requeriría también examinar la casa para verificar que cosas faltan, y no es necesario recordarle que una auditoría toma casi el mismo tiempo que un test de seguridad.

- ***Haga* las cosas pequeñas, porque en definitiva, todas son cosas pequeñas.**

Testear se refiere a los detalles, y muy a menudo los pequeños detalles llevan a las más importantes fallas de seguridad. Además, es la acumulación de las cosas pequeñas, que individualmente no representan mucho riesgo, aunque sumadas, pueden llevar a una falla de seguridad

- ***Haga* más con menos.**

Mientras los presupuestos de seguridad sigan siendo bajos, el testeador de seguridad necesita operar con eficiencia y creatividad para hacer más en menos tiempo. Si el testeo ineficiente de seguridad se vuelve demasiado costoso, es tentador para una organización ver este testeo de seguridad como un costo innecesario. Esto es algo desafortunado porque los riesgos asociados con no llevar a cabo tests de seguridad siguen siendo desconocidos. En consecuencia, cuando

balanceamos minuciosidad y eficiencia en nuestros tests de seguridad, los resultados van a hablar por sí mismos una y otra vez - y muchas otras organizaciones verán los testeos de seguridad como un arma de costo justificado en su actitud defensiva.

- **No subestime *en ninguna forma* la importancia de las Políticas de Seguridad.**

Esta política es la declaración oficial de la compañía con respecto a los objetivos que quiere lograr. Muy poca gente llega alguna vez a alguna parte sin antes desarrollar politicas de seguridad. Una política de seguridad expresa en su contenido la intención y los objetivos de seguridad de una organización. Las políticas de seguridad de una organización son con frecuencia muy complejas y con muchas personas afectadas a su desarrollo y su mantenimiento. Los errores de políticas de una sección frecuentemente derivarán en un efecto de flujo negativo que impactará en otras secciones.

Sólo se necesita unas pocas termitas en una pared para que luego aparezca una plaga en toda la casa. Por ejemplo, si la política no está implementada para especificar controles que verifiquen que la gente no se vaya llevando cajas o equipamiento, entonces una filtración de información puede ocurrir.

Las Políticas de Seguridad especifican muchos más controles que tienen un efecto directo sobre los estándares y procedimientos, tales como las reglas de salida que existen en un router de filtrado, o a cuáles correos electrónicos uno puede reenviar correos electrónicos desde dentro de la compañía.

- **Lo que los demás obtienen está relacionado directamente con *cómo* UD lo brinda.**

A pesar de todos los intentos basados en el esmero y la eficiencia, uno de los factores más importantes que determinan el éxito de una actitud de seguridad está aún basado en las finanzas. Esto es manejado muy lejos de la caja de herramientas del testeador. Se requiere cierta competencia en dirección de proyectos, discernimiento acerca de las necesidades de su cliente y excelentes destrezas comunicativas. ¿Hay tiempo suficiente para que el test sea presupuestado? ¿Habrá suficientes recursos en el presupuesto para reparar las vulnerabilidades descubiertas? ¿Qué tipos de riesgos serán considerados sin mérito suficiente por los altos directivos como para merecer ser incluídos en el presupuesto?

El resultado final del test de seguridad será entregado a su cliente o a la administración de su cliente - con todos los factores financieros previstos de antemano. Después de todo, ¿cuál es la diferencia entre un excelente test de seguridad y uno malo si el informe es ignorado?

Contenidos

Introducción

Este manual es una combinación de ambición, estudio y años de experiencia. Los tests individuales no son particularmente revolucionarios, pero la metodología en conjunto representa un estándar de referencia en el área de testeo de seguridad. A través de la minuciosidad de su utilización, UD encontrará un enfoque revolucionario hacia el testeo de seguridad.

Este manual es un estándar profesional para el testeo de seguridad en cualquier entorno desde el exterior al interior. Como cualquier estándar profesional, incluye los lineamientos de acción, la ética del testeador profesional, la legislación sobre testeo de seguridad y un conjunto integral de tests. Debido a que los testeos de seguridad continúan evolucionando en una profesión válida y respetada, el OSSTMM intenta ser el manual de referencia del profesional.

El objetivo de este manual es crear un método aceptado para ejecutar un test de seguridad minucioso y cabal. Detalles como las credenciales del testeador de seguridad, el tamaño de la empresa de seguridad, las finanzas, o el respaldo de ventas impactan en la escala y la complejidad de nuestro test - pero cualquier experto en redes o en seguridad que cumpla con los requisitos de este manual habrá completado un exitoso perfil de seguridad. UD no encontrará ninguna recomendación a seguir la metodología como si se tratase de un diagrama de flujo. En cambio, se presentan una serie de pasos que deben ser vistos y revistos (repetidas veces) durante la realización de un test exhaustivo. La gráfica de metodología brindada es la manera óptima de llevar a cabo esto, convenientemente de a dos testeadores, aunque cualquier número de testeadores tienen la posibilidad de realizar la metodología en tándem. Lo más importante en esta metodología es que los diferentes tests son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados esperados dentro de un período de tiempo determinado. Solo así el testeador habrá ejecutado el test en conformidad con el modelo OSSTMM, y por ello, el informe podrá ser considerado mínimamente exhaustivo.

Algunos testeadores de seguridad consideran que un test de seguridad es simplemente una vista de una postura defensiva en un "momento en el tiempo", y presentan los resultados de sus tests como una "instantánea de la seguridad". La denominan instantánea porque en ese momento particular, las vulnerabilidades conocidas, las debilidades conocidas y las configuraciones conocidas, no habían cambiado. ¿Es esta instantánea suficiente? La metodología propuesta en este manual proveerá más de una instantánea.

Valores de la Evaluacion de Riesgo (RAV)

Los RAV realzarán estas instantáneas agregando dimensiones de frecuencia y un contexto de tiempo a los tests de seguridad. Estas instantáneas se convierten en un perfil, abarcando un rango de variables a lo largo de un período de tiempo antes de degradarse por debajo de los niveles aceptables de riesgo. En la revisión 2.5 del OSSTMM hemos desarrollado la definición y la aplicación de los RAV para poder cuantificar con precisión los niveles de riesgo. Los RAV brindan tests específicos en períodos de tiempo determinados que se tornan cíclicos y minimizan los riesgos que uno toma en una postura defensiva.

Algunos preguntarán: "¿Vale la pena tener una metodología estándar para los tests de seguridad?" Bien, la calidad del resultado de un test de seguridad es difícil de juzgar sin una metodología estándar. Muchas variables afectan el resultado de un test, incluyendo el estilo personal y las predilecciones del testeador. Precisamente por todas estas variables, es importante definir el modo correcto de testear, basándose en las mejores prácticas y en un consenso a nivel mundial. Si UD puede reducir los prejuicios y las parcialidades en el testeo, reducirá la incidencia de muchos falsos supuestos y también evitará resultados mediocres. UD tendrá un correcto balance de la estimación de los riesgos, de los valores y la justificación de negocio del objetivo a ser testeado. El limitar y guiar nuestras suposiciones, convierte a un buen testeador de seguridad en uno excelente y brinda a los novatos la metodología apropiada para llevar a cabo los tests necesarios en las áreas correctas.

El resultado final es que como testeadores de seguridad, participamos y formamos parte de un proyecto de gran extensión. Estamos utilizando y contribuyendo con una metodología abierta a la que cualquier persona puede acceder. Cualquiera puede abrir, estudiar en sus partes, ampliar, sugerir y contribuir con el OSSTMM, donde todas las críticas constructivas continuarán ayudando al desarrollo y la evolución de esta metodología. Ésta puede ser la contribución más valiosa que alguien pudiera hacer a la disciplina del testeo profesional de seguridad.

Recibiremos con entusiasmo sus contribuciones e ideas.

Pete Herzog Director de ISECOM

Ámbito

Este es un documento de metodología de testeo de seguridad. Es un conjunto de reglas y lineamientos para CUANDO, QUE y CUALES eventos son testeados. Esta metodología cubre únicamente el testeo de seguridad externo, es decir, testear la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado. Está también dentro del alcance de este documento proveer un método estandarizado para realizar un exhaustivo test de seguridad de cada sección con presencia de seguridad (por ejemplo, seguridad física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la información, seguridad de las tecnologías de Internet, y seguridad de procesos) de una organización. Dentro de este método abierto y evaluado por expertos, para realizar exhaustivos testeos de seguridad, alcanzamos un estándar internacional en testeos de seguridad, que representa una línea de referencia para todas las metodologías de testeo de seguridad tanto conocidas como inexploradas.

La limitación al alcance del testeo de seguridad externo está dada por las diferencias considerables entre testeo externo a interno y testeo interno a interno. Estas diferencias radican fundamentalmente en los privilegios de acceso, los objetivos, y los resultados asociados con el testeo interno a interno.

El tipo de testeo que busca descubrir las vulnerabilidades inexploradas no está dentro del alcance de este documento ni dentro del alcance de un test de seguridad OSSTMM. El test de seguridad descrito a continuación es un test práctico y eficiente de vulnerabilidades conocidas, filtraciones de información, infracciones de la ley, estándares de la industria y prácticas recomendadas.

ISECOM exige que un test de seguridad solamente sea considerado un test OSSTMM si es:

- Cuantificable.
- Consistente y que se pueda repetir.
- Válido mas allá del período de tiempo "actual".
- Basado en el mérito del testeador y analista, y no en marcas comerciales.
- Exhaustivo.
- Concordante con leyes individuales y locales y el derecho humano a la privacidad.

ISECOM no asevera que el uso del OSSTMM constituya una protección legal en todos los tribunales de justicia, sin embargo, cumple el papel del más alto nivel de profesionalismo en cuanto a testeos de seguridad cuando los resultados obtenidos son aplicados al perfeccionamiento de la seguridad dentro de un espacio de tiempo razonable.

Público al que va dirigido

Este manual está pensado para profesionales del testeo de seguridad. Términos, destrezas y procesos que son mencionados aquí, pueden no ser fáciles de comprender para aquellos que no están directamente involucrados y con experiencia en los testeos de seguridad.

Diseñadores, arquitectos y desarrolladores encontrarán este manual provechoso para construir mejores defensas y herramientas de testeo. Muchos de los tests no poseen manera de ser automatizados. Muchos de los tests automatizados no siguen una metodología o siquiera siguen una en un orden óptimo. Este manual se refiere a esas cuestiones.

Acreditación

Una planilla de datos de test de seguridad es necesaria, firmada por el/los testeador(es), acompañando todos los reportes finales para obtener un test certificado de OSSTMM. Esta planilla de datos está *disponible con el OSSTMM 2.5*. Esta planilla de datos reflejará cuales módulos y táreas han sido testeados hasta su conclusión, cuáles no han sido testeados hasta su conclusión y la justificación de ello, y los tests no aplicables y la justificación de ello. La lista de comprobación debe estar firmada y acompañada del reporte final a entregar al cliente. Una planilla de datos que indique que solamente algunos módulos específicos de una Sección de OSSTMM han sido testeados debido a restricciones de tiempo, problemas en el proyecto o negativa del cliente, NO puede ser considerado como un test OSSTMM completo de la Sección en cuestión.

Las razones para el uso de las planillas de datos son las siguientes:

- Sirve como prueba de un testeo de OSSTMM minucioso.
- Responsabiliza al testeador por el test.
- Es una declaración precisa al cliente.
- Brinda una apropiada visión general.
- Suministra una lista de comprobación clara para el testeador.

La utilización de este manual en la ejecución de tests de seguridad está determinada por el informe de cada tárea y sus resultados aún cuando no fueran aplicables en el informe final.

Todos los reportes finales que incluyan esta información y las listas de comprobación asociadas y apropiadas, habrán sido ejecutados de la manera más exhaustiva y completa, y pueden incluir la siguiente declaración y un sello en el informe:

Este test ha sido ejecutado en conformidad con el OSSTMM, disponible en http://www.osstmm.org/ y mediante este sello se afirma que está dentro de las mejores prácticas de testeo de seguridad.

Todos los sellos (en color y blanco y negro) están disponibles en http://www.isecom.org/stamps.htm

Resultado Final

El objetivo principal es establecer un estándar en metodologías de testeo de seguridad que cuando es utilizado reúne condiciones de seguridad prácticas y funcionales. El resultado indirecto es forjar una disciplina que pueda hacer el papel de punto de referencia en todos los tests de seguridad sin importar el tamaño de la organización, la tecnología o las defensas.

Análisis

El alcance de este documento no incluye el análisis directo de los datos recopilados durante el uso de este manual. Tal análisis es el resultado que surge de la comprensión de las leyes relacionadas, las necesidades comerciales respectivas a cada cliente, las prácticas recomendadas y reglamentaciones de seguridad y privacidad relativas al área de operación del cliente. Sin embargo, el análisis de datos está implícito en la utilización de los "Resultados Esperados" contenido en la metodología. Es por ello que algunos análisis deben ser llevados a cabo para asegurar que como mínimo, los resultados esperados sean satisfechos.

Términos Relacionados a Internet y Redes

En todo este manual nos referimos a términos y palabras que podrían ser relacionados con otras áreas o significados. Esto es particularmente cierto con respecto a las traducciones internacionales. Para definiciones que no se encuentren presentes en este glosario, vea el glosario de ***OUSPG Terminología de Tests de Vulnerabilidad***, disponible en http://www.ee.oulu.fi/research/ouspg/sage/glossary/

Acceso Remoto	Se define como un acceso desde el exterior de la ubicación.
Acuerdo de No Divulgación	Acuerdo legal que evita la difusión de información mas allá de los prop informativos, entre las partes que mantienen dicho acuerdo de no divulgación.

Ámbito	La descripción de lo que está permitido en un test de seguridad.
Ámbito de la Red	Se refiere a lo que el testeador puede legalmente testear.
Ámbito de la Seguridad	Otra palabra que define Ámbito.
Análisis de la Competencia	Práctica legal para obtener información comercial de la competencia.
Auditoría de Seguridad	Inspección manual con privilegios de acceso del sistema operativo y de programas de aplicación de un sistema. En los Estados Unidos y Canad "Auditor" representa un vocablo y una profesión oficiales, solamente utilizado por profesionales autorizados. Sin embargo, en otros países, u "auditoría de seguridad" es un término de uso corriente que hace refer Test de Intrusión o test de seguridad.
Caja Blanca	El testeador posee conocimiento previo integral de los elementos o del entorno a ser testeados.
Caja Gris	El testeador tiene un conocimiento previo de los elementos o del entor testear.
Caja Negra	El testeador no tiene conocimiento previo de los elementos o del entor testear.
Cliente	Se refiere al receptor de las ventas con quien la confidencialidad se imp través de la firma de un acuerdo de no divulgación.
Comprador	Se refiere al receptor de las ventas con quien se la confidencialidad est éticamente implícita sin firmarse un acuerdo de no divulgación o contr alguno.
Cortafuegos	Las herramientas de software o hardware que impone una Lista de Co Acceso en un sistema o red
Entorno	Es el estado interactivo, interdependiente de una red en operación. Es también conocido como escenario.

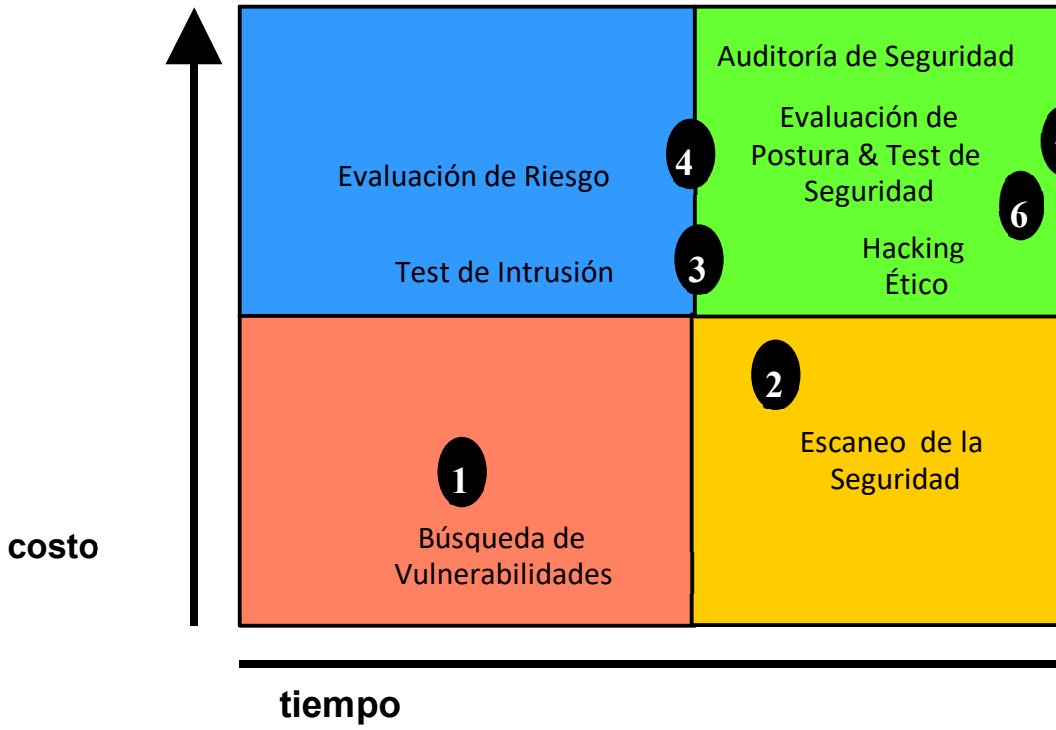
Esquema de Actividades (Plan) Agenda de actividades que deben ser sistemáticamente completadas durante un test.

Evaluación	Una visión general de la presencia de seguridad para una estimación d tiempo y horas hombre.
Evaluación de Postura	Término utilizado por el Ejército de los Estados Unidos para referirse a test de seguridad.
Evaluación de Riesgo	En el OSSTMM se emplea para describir la degradación de la seguridad marcador de comparaciones que cuantifica los niveles de seguridad de manera cronológica.
Exploración	Análisis de documentación para hallar nuevas o únicas informaciónes tendencias del curso de los negocios
Funcionalidad	Previsión que permite tornar la seguridad más comprensible y eficient manera que no sea pasada por alto de forma intencional por razones lí
Hacker	Una persona inteligente que tiene una curiosidad natural, le gusta apre como las cosas funcionan, y le interesa conocer técnicas de evasión o a de procesos para ver qué sucede.
Hacking Ético	Una forma de test de intrusión originalmente usado como táctica de mercadeo, que significa un test de intrusión en todos los sistemas - y d hay más de un objetivo, generalmente todo es un objetivo.

Horas Hombre	Trabajo realizado por una persona en el lapso de una hora. Dos horas hombres puede ser el trabajo de dos personas realizado en una hora O trabajo que una persona puede realizar en dos horas.
Ingeniería Social	Ataque activo contra los procesos.
Medidas de Contención	Es un proceso de cuarentena y validación.
Módulos	Son las perspectivas basadas en la seguridad de los negocios para cada sección individual de OSSTMM.
Objetivos	El resultado final a ser alcanzado. A veces puede ser un trofeo como es hallazgo en una red que potencialmente puede poseer valor financiero por ejemplo, una base de datos de números de tarjetas de crédito.
PBX	Representa el Conmutador Telefónico, y es el servidor central que adm las líneas telefónicas en una organización.
Presencia de Seguridad	Define cómo la seguridad es aplicada a las seis secciones de seguridad organización.
Presupuesto	Documento sobre el tiempo y las horas hombre necesarias para un tes cual puede estar explicitado el costo del mismo.
Privilegios	Credenciales y permisos.
RAV	Valores de la Evaluación de Riesgo. Es la herramienta de asesoramient riesgo de facto del OSSTMM que se basa en ciclos y factores de degrada en los módulos.
Responsabilidad Contractual	Seguridad financiera de diligencia y seriedad.
Resultados Esperados	Los hallazgos en un módulo especifico.
Router	Un programa o un dispositivo físico para enrutar paquetes.
Secciones	En el OSSTMM, se utilizan para definir perspectivas generales de segur El OSSTMM se apoya en 6 puntos de vista: TI, Información, Tecnologías Inalámbricas, Comunicaciones, Seguridad Física y Procesos.
Seguridad Práctica	Define la seguridad que puede ser empleada y que se aplica a la justific de negocios.
Semanas hombre	Es la cantidad de trabajo que una persona puede realizar en una sema trabajo de 40 horas.
Sistemas de Detección de Intrusiones (IDS)	Ya sean activos o pasivos, basados en terminales o en la red, esta herra está diseñada para monitorear y a menudo detener ataques cuando su
Sombrero Blanco	Es un hacker que no transgrede la ley y actúa con ética.
Sombrero Gris	Un hacker que es caótico, anarquista, pero no infringe la ley. Sin emba acciones a menudo carecen de integridad o etica.
Sombrero Negro	Un hacker que es caótico, anarquista e infringe la ley.
Táreas	Tests de seguridad específicos en un módulo que se utilizan para alcan o más Resultados Esperados definidos.
Test de Aplicación	Test de seguridad sobre cualquier aplicación, independientemente si e parte de la presencia en Internet.
Test de Intrusión	Test de seguridad con un objetivo definido que finaliza cuando el objet alcanzado o el tiempo ha terminado.
Testeo Automatizado	Cualquier clase de testeo automatizado que también brinda análisis.
Testeo con Privilegios	Test donde las credenciales necesarias son suministradas al usuario y permisos concedidos para testear con dichas credenciales.
Testeo de Seguridad	Un test de la presencia de seguridad. Puede ser especificado por secci
Testeo de Verificación	Un test de verificación realizado en una segunda etapa luego de que to parches han sido aplicados.

Testeo de Vulnerabilidades	Test de servicios, puertos abiertos y vulnerabilidades conocidas.
Testeo Manual	Testeo que requiere que una persona ingrese datos durante el proceso testeo y monitoree los resultados para efectuar análisis sobre ellos.
Tiempo	Tiempo físico – la cuarta dimensión – 24 horas del día.
Ubicación	Ubicación física.
Visibilidad	Componentes de la presencia de seguridad que pueden ser remotamen identificados.

Para mayor claridad, ISECOM aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de redes, basados en tiempo y costo para el Testeo de Seguridad de Internet:



1. **Búsqueda de Vulnerabilidades:** se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

2. **Escaneo de la Seguridad:** se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.

3. **Test de Intrusión:** se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.

4. **Evaluación de Riesgo:** se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

5. **Auditoría de Seguridad:** hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.

6. **Hacking Ético**: se refiere generalmente a los tests de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.

7. **Test de Seguridad y su equivalente militar, Evaluación de Postura**, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

Concordancia

Este manual fue desarrollado para satisfacer la concordancia de los testeos y las evaluaciones de riesgo para la protección de los datos personales con los siguientes cuerpos legislativos.

Los tests realizados brindan la información necesaria para analizar las cuestiones pertinentes a la privacidad de los datos en concordancia con la mayoría de las legislaciones gubernamentales y las mejores prácticas organizativas debido al alcance exhaustivo de los tests contenidos en este manual.

Aunque no todos los estatutos de los diferentes países están aquí detallados, este manual ha explorado los diferentes cuerpos legislativos para satisfacer los requisitos de derechos de los individuos y privacidad.

Legislación

Los tests de este manual incluyen en su diseño la auditoría remota y el testeo desde el exterior al interior de los siguientes cuerpos legislativos:

Austria

• Ley de Protección de Datos Austriaca, Año 2000 (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)) especialmente los requisitos mencionados en §14

Estados Unidos de América

- U.S. Gramm-Leach-Bliley Act (GLBA)
- Clinger-Cohen Act

- Government Performance and Results Act
- Government Paperwork Elimination Act
- FTC Act, 15 U.S.C. 45(a), Section 5(a)
- Children's Online Privacy Protection Act (COPPA)
- ICANN Uniform Dispute Resolution Policy (UDRP)
- Anticybersquatting Protection Act (ACPA) • Federal Information Security Management Act.
- U.S. Sarbanes-Oxley Act (SOX)
- California Individual Privacy Senate Bill - SB1386
- USA Government Information Security Reform Act of 2000 section 3534(a)(1)(A)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- OCR HIPAA Privacy TA 164.502E.001, Business Associates [45 CFR §§ 160.103, 164.502(e), 164.514(e)]
- OCR HIPAA Privacy TA 164.514E.001, Health-Related Communications and Marketing [45 CFR §§ 164.501, 164.514(e)]
- OCR HIPAA Privacy TA 164.502B.001, Minimum Necessary [45 CFR §§ 164.502(b), 164.514(d)]
- OCR HIPAA Privacy TA 164.501.002, Payment [45 CFR 164.501]

Alemania

• Deutsche Bundesdatenschutzgesetz (BDSG)-- Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes from 20. December 1990, BGBl. I S. 2954, 2955, zuletzt geändert durch das Gesetz zur Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994, BGBl. I S. 2325

España

- LOPD Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal. Art.15 LOPD -. Art. 5,
- LSSICE

Canadá

- Corporate Governance
- Provincial Law of Quebec, Canadá Act Respecting the Protection of Personal Information in the Private Sector (1993).

United Kingdom

- UK Data Protection Act 1998
- Corporate Governance

Australia

- Privacy Act Amendments of Australia-- Act No. 119 de 1988 como reformada, preparada el 2 de agosto de 2001, incorporando reformas hasta Act No. 55 de 2001. The Privacy Act 1988 (Cth) (the Privacy Act) busca equilibrar la privacidad individual con el interés público en el cumplimiento de la ley y los fines regulatorios del gobierno.
- National Privacy Principle (NPP) 6 establece que un individuo tiene derecho a acceder a la información sobre sí mismo que posea cualquier organización.
- National Privacy Principle (NPP) 4.1 establece que una organización debe tomar medidas sensatas para proteger la información personal que posee contra usos indebidos, pérdida, accesos no autorizados, modificaciones o divulgación.

Mejores Prácticas

Los tests de este manual incluyen en su diseño la auditoría remota y el testeo desde el exterior al interior de los siguientes:

Biblioteca de TI

Información disponible en http://www.ogc.gov.uk/index.asp?id=2261 publicado por British Office for Government Commerce (OGC)

Alemania: IT Baseline Protection Manual (IT Grundschutzhandbuch)

Publicado por Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security (BSI)) disponible en http://www.bsi.de/gshb/english/menue.htm

Sistemas Alemanes de TI

S6.68 (Testeo de la efectividad de los sistemas de administración para el manejo de incidentes de seguridad) y tests S6.67 (Uso de medidas de detección para incidentes de seguridad)

ISO 17799-2000 (BS 7799)

Este manual está en plena concordancia con todos los requisitos de auditoría y testeo de seguridad remotos del BS7799 (y su equivalente internacional ISO 17799) para testeos informáticos de seguridad.

GAO y FISCAM

Este manual está en concordancia con las actividades de control descritas en US General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM) donde ellas se aplican a la seguridad de redes.

SET

Este documento incorpora el testeo remoto de seguridad del SET Secure Electronic Transaction(TM) Compliance Testing Policies and Procedures, Version 4.1, 22 de Febrero de 2000

NIST

Este manual está en conformidad en su metodología de testeos y auditorías remotos de seguridad de acuerdo con las siguientes publicaciones del National Institute of Standards and Technology (NIST)

- An Introduction to Computer Security: The NIST Handbook, 800-12
- Guidelines on Firewalls and Firewall Policy, 800-41
- Information Technology Security Training Requirements: A Role- and Performance-Based Model, 800-16
- DRAFT Guideline on Network Security Testing, 800-42
- PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, 800-24
- Risk Management Guide for Information Technology Systems, 800-30
- Intrusión Detection Systems, 800-31

MITRE

Este manual es compatible con el CVE para los Valores de la Evaluación de Riesgo.

Lineamientos de Acción

Los asociados de ISECOM o quienes públicamente anuncien el uso de OSSTM para análisis y pruebas de seguridad deben seguir las siguientes reglas de uso. Estas reglas definen los lineamientos éticos de las prácticas aceptadas en el mercadeo y venta de análisis y tests de seguridad, la ejecución de dichos análisis y el manejo de los resultados obtenidos. Fallar en el cumplimiento de estas reglas puede resultar en la inhabilidad de usar el sello ISECOM en los resultados y la terminación del acuerdo de asociado con ISECOM.

1 Ventas y Mercadeo

1 El miedo infundado, la incertidumbre y la duda no pueden ser usados en presentaciones de ventas y mercadeo, sitios web, materiales de soporte, reportes o en la discusión de las pruebas de seguridad, con el propósito de vender o proveer estos servicios. Esto incluye pero no se limita a delitos, eventos, perfiles de hacker, y/o estadísticas.

2 El ofrecimiento de servicios gratuitos a cambio de fallar en el test de intrusión o entregar premios del objetivo están prohibidos.

3 Competencias de hacking, cracking y violación de sitios, para promover ventas y/o mercadeo de tests de seguridad, o productos de seguridad están prohibidos.

4 Ejecutar tests de seguridad en contra de cualquier red sin el consentimiento explícito y escrito de la autoridad correspondiente, está prohibido.
5 El uso de los nombres de clientes previos a quienes se les ha prestado servicio de seguridad (análisis, tests) está prohibido, incluso con el consentimiento de los mismos. Esto se debe a la necesidad de proteger al cliente así como a la misma empresa prestadora del servicio.
6 Es indispensable proveer una asesoría en seguridad acertada, incluso cuando dicha asesoría implique recomendar la asignación del contrato a otra compañia. Un ejemplo de este caso es cuando se requiere la verificación de una implementación de seguridad realizada por la compañía asesora. Esta implementación debe analizarse independientemente por parte de terceros.

2 Evaluación / Entrega estimada

1 Verificar posibles vulnerabilidades en determinados servicios sin autorización explícita por escrito está prohibida.
2 El análisis de seguridad de sistemas, ubicaciones y procesos inestables y obviamente inseguros está prohibido hasta que hayan sido debidamente asegurados.

3 Contratos y Negociaciones

1 Con o sin el Acuerdo de No Divulgación, el analista de seguridad esta éticamente obligado a mantener la confidencialidad y garantizar la no divulgación de la información del cliente ni los resultados del análisis.
2 El analista siempre debe asumir un monto limitado de responsabilidad. El monto aceptable de dicha responsabilidad es igual al costo del servicio. Esto incluye errores tanto intencionados como no intencionados, y un posible mal manejo del proyecto.
3 Los contratos deben explicar claramente los límites y peligros de un análisis de seguridad.
4 En el caso de análisis remoto, el contrato debe incluir el origen de las pruebas por número telefónico y/o direcciones IP.
5 Los contratos deben incluir información de contacto en caso de emergencia (nombres y números telefónicos).
6 El contrato debe incluir permisos claros y específicos para análisis que involucren fallas de supervivencia, negación del servicio, análisis de procesos o ingeniería social.
7 Los contratos deben contener los procesos para contratos futuros y cambios en las condiciones de trabajo.

4 Ámbito

1 El ámbito debe estar claramente definido contractualmente antes de verificar cualquier vulnerabilidad en los servicios de red.
2 El ámbito debe explicar claramente los límites del análisis de seguridad

5 Plan de trabajo del análisis

1 El plan de trabajo debe incluir tanto tiempo calendario como horas-hombre.
2 El Plan de trabajo debe incluir horas de análisis.

6 Entregar las reglas del contrato al cliente

1 No se permiten cambios de red inusuales durante el análisis.
2 Para prevenir incrementos repentinos en los niveles de seguridad, únicamente durante el análisis, el cliente debe notificar únicamente al personal clave acerca del proceso. Queda a juicio del cliente determinar a quién se le debe informar, sin embargo, se asume que deben ser los encargados de políticas y seguridad, administradores de procesos de aseguramiento, respuesta a incidentes y operaciones de seguridad.

3 Si es necesario para pruebas con privilegios, el cliente debe proveer dos mecanismos de acceso independientes, ya bien sean nombres de usuarios y contraseñas, certificados, números de identificación, etc. Estos deben tener los privilegios típicos de los usuarios a ser analizados. (no debe ser cuentas especiales o aseguradas)
4 Cuando se ejecuten análisis privilegiados, el analista inicialmente debe probar sin privilegios en un ambiente desconocido o de caja negra y luego probar de nuevo con privilegios en el mismo ambiente.

7 Tests

1 Los analistas deben conocer sus herramientas, de donde vienen, como trabajan, y haberlas probado en un área restringida antes de usarlas en la organización del cliente.
2 La aplicación de pruebas para la Negación del Servicio, puede realizarse únicamente con permiso explícito. Un análisis de seguridad OSSTM no requiere la explotación de vulnerabilidades de negación del servicio ni de vulnerabilidades de supervivencia . Se espera que el analista use evidencia recopilada únicamente para proveer una revisión adecuada de los sistemas y procesos de seguridad.
3 La Ingeniería Social y análisis de procesos debe ser ejecutado por medio de estadisticas anónimas obtenidas con personal sin entrenamiento o que no sea del área de seguridad.
4 La Ingeniería Social y el análisis de procesos solo puede ser ejecutado en el personal determinado en el ámbito y no debe incluir clientes, socios de negocios, asociados o entidades externas de cualquier tipo.
5 Vulnerabilidades de alto riesgo, como huecos de seguridad, vulnerabilidades con alta tasa de explotación, explotables y que permitan acceso total no monitoreado, sin dejar rastro o que puedan poner en peligro vidas y que sean descubiertas durante el análisis, deben ser reportadas al cliente con una solución práctica tan pronto sean encontradas.
6 Negación del servicio Distribuida (DDOS) por Internet esá prohibida.
7 Cualquier forma de pruebas por inundación, donde una persona, red, sistema o servicio sea saturado desde una amplia y fuerte fuente, está prohibido.
8 Notificaciones al cliente son requeridas cuando el analista cambie el plan de trabajo, cambie el origen de los análisis, obtenga resultados de alto riesgo, con antelación a la ejecución de nuevos análisis de alto riesgo y alta generación de tráfico, y en caso que hayan ocurrido problemas en el análisis. Adicionalmente el cliente debe ser notificado con reportes de progreso semanalmente.

8 Informes

1 Los Informes deben incluir soluciones prácticas orientadas a resolver los problemas de seguridad descubiertos.
2 Los Informes deben incluir todo los hallazgos desconocidos y deben ser identificados como tales.
3 Los Informes deben especificar claramente todos los estados de seguridad encontrados y no sólo las medidas de seguridad fallidas.
4 Los Informes deben usar indicadores cualitativos para medir los riesgos, basándose en los métodos aceptados por la industria. Estos valores deben basarse en fórmulas matemáticas y no en la intuición del analista.

9 Entrega de Informes

1 El cliente debe ser informado del envío del informe y debe confirmarse la recepción del mismo. 2 Todos los canales de comunicación para la entrega del reporte deben ser confidenciales.

Reglas Adicionales

Estas son las reglas adicionales para Test de Seguridad y Estimación de Tiempo

Regla de Enumeración

2 Días para una Clase C con <= 12 saltos a través de una linea digital de 64k • Agregar una hora adicional por Clase C para cada salto superior a 12.

- Mayor ancho de banda probablemente disminuiría el tiempo.
- No cuenta para sistemas protegidos por Sistemas de Detección de Intrusos o Cortafuegos a Nivel de Aplicación.

Reglas de Testeo de OSSTMM

3 Semanas-Hombre por cada 10 Sistemas Activos en una Clase C con <= 12 saltos a través de una linea digital de 64K

- Agregar ½ Hora Hombre por cada sistema activo para cada salto superior a 12.
- Mayor ancho de banda probablemente disminuiría el tiempo hasta 1MB.
- Incrementando el Numero de Testeadores disminuye el tiempo proporcionalmente. La complejidad del análisis y generación de informes aumentaría para una cantidad mayor a 5 testeadores.
- No cuenta para sistemas protegidos por Sistemas de Detección de Intrusos o Cortafuegos a Nivel de Aplicación.

Reglas de Cálculo Adicionales

- Para planear un análisis de seguridad, se deben reservar aproximadamente 2 días hombre por persona por semana calendario para la investigación y desarrollo, incluyendo en esto el mantenimiento del sistema y la verificación de nuevas herramientas.
- El tiempo total de análisis nunca debe exceder tres meses.
- El análisis puede iniciarse tempranamente, pero no antes que haya transcurrido la mitad del tiempo requerido para la enumeración.
- La mitad del tiempo invertido en tests es requerido para los Informes.
- El Informe debe ser entregado tres días antes de la última reunión con el cliente
- En la reunión final, el número de invitados no debe ser superado por el número de analistas de seguridad, a menos que, únicamente asista un invitado, caso en el cual pueden haber hasta 2 analistas por parte de la empresa prestadora del servicio.
- En una reunión de análisis siempre debe participar una persona del área comercial y otra persona del área técnica (el analista encargado del cliente).

P r o c e s o

El proceso de un análisis de seguridad, se concentra en evaluar las siguientes areas, que reflejan los niveles de seguridad presentes, siendo estos el ambiente definido para el análisis de seguridad. Estos son conocidos como las Dimensiones de Seguridad:

Visibilidad

La visibilidad es lo que puede verse, registrarse, o monitorearse en el nivel de seguridad con o sin la ayuda de dispositivos electrónicos. Esto incluye, pero no se limita a, ondas de radio, luz por encima del espectro visible, dispositivos de comunicación como teléfonos, GSM, email y paquetes de red como TCP/IP.

Acceso

El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física. Esto puede incluir, pero no se limita a, una página web, una ventana, una conexión de red, ondas de radio, o cualquier cosa cuya ubicación soporte la definición de casi-público o dinde un computador interactúa con otro por medio de una red. Limitar el acceso significa negar todo excepto lo que este expresamente permitido financieramente y por buenas prácticas.

Confianza

La confianza es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.

Autenticación

La autenticación es la medida por la cual cada interacción en el proceso está privilegiada.

No-repudio

El no-repudio provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.

Confidencialidad

La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.

Privacidad

La privacidad implica que el proceso es conocido únicamente por los sistemas o partes involucradas.

Autorización

La autorización es la certeza que el proceso tiene una razón o justificación de negocios y es administrado responsablemente dando acceso permitido a los sistemas.

Integridad

La integridad es la certeza que el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reversado sin el conocimiento de los sistemas o partes involucradas.

Seguridad

La seguridad son los medios por los cuales un proceso no puede dañar otros sistemas, o procesos incluso en caso de falla total del mismo.

Alarma

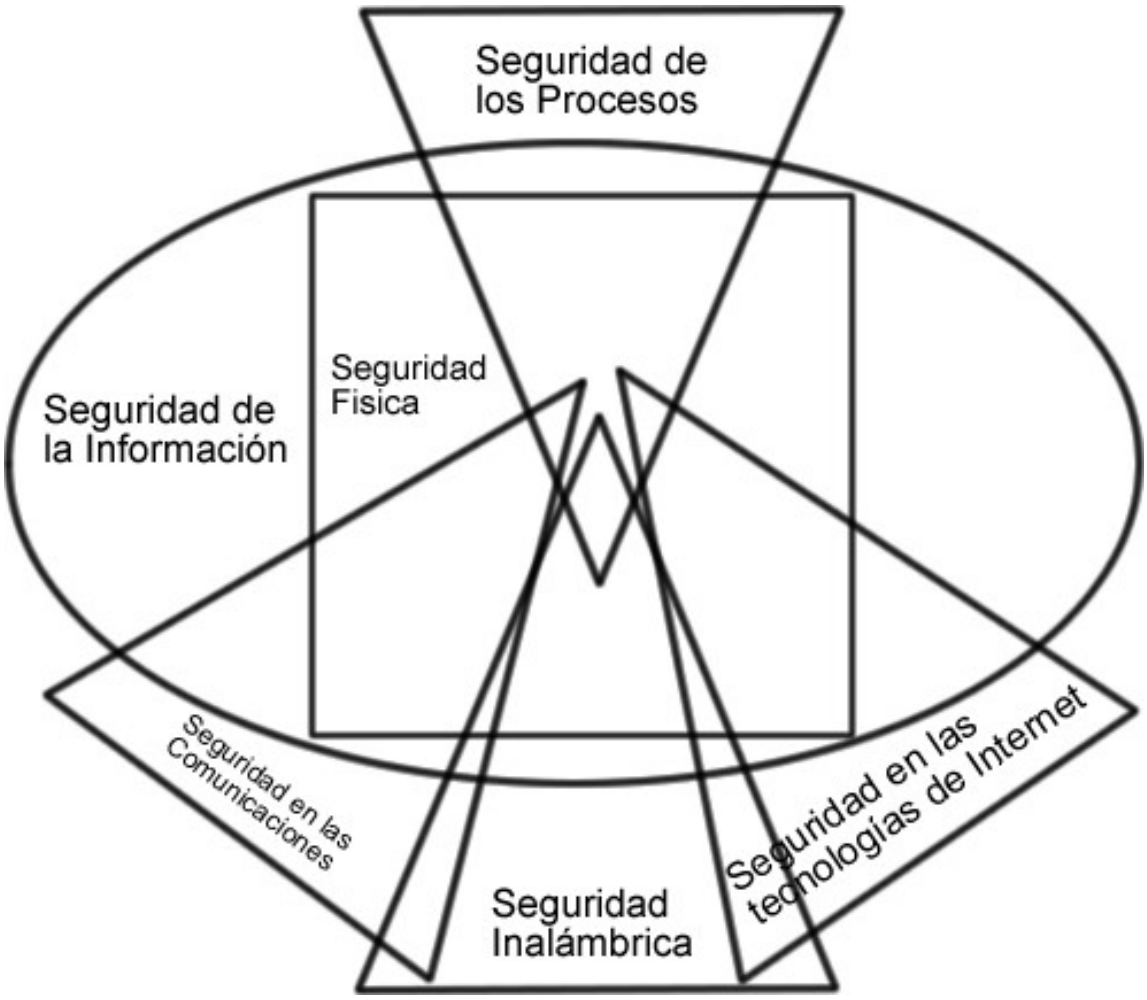
La alarma es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad. En la mayoría de violaciones de seguridad, la alarma es el único proceso que genera reacción.

Mapa de Seguridad

El mapa de seguridad es un imagen de la presencia de seguridad. Esta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones equivalentes a las de este manual. Las secciones se superponen entre si y contienen elementos de todas las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, directa o indirectamente.

Las secciones en este manual son:

1 Seguridad de la Información
2 Seguridad de los Procesos
3 Seguridad en las tecnologías de Internet
4 Seguridad en las Comunicaciones
5 Seguridad Inalámbrica
6 Seguridad Física



Lista de Módulos del Mapa de Seguridad

La lista de módulos del mapa de seguridad son los elementos primarios de cada sección. Cada módulo debe incluir todas las Dimensiones de Seguridad que estan integradas con tareas a ser desarrolladas. Para desarrollar un análisis de seguridad OSSTMM de una sección particular, todos los módulos de la sección deben ser desarrollados y aquellos para los que no exista infraestructura y no pueda ser verificada, debe definirse como NO APLICABLE en la hoja de datos OSSTM anexa al informe final.

1 Seguridad de la Información
   1 Revisión de la Inteligencia Competitiva
   2 Revision de Privacidad
   3 Recolección de Documentos
2 Seguridad de los Procesos
   1 Testeo de Solicitud
   2 Testeo de Sugerencia Dirigida
   3 Testeo de las Personas Confiables
3 Seguridad en las tecnologías de Internet
   1 Logística y Controles
   2 Sondeo de Red

3 Identificación de los Servicios de Sistemas
4 Búsqueda de Información Competitiva
5 Revisión de Privacidad
6 Obtención de Documentos
7 Búsqueda y Verificación de Vulnerabilidades
8 Testeo de Aplicaciones de Internet
9 Enrutamiento
10 Testeo de Sistemas Confiados
11 Testeo de Control de Acceso
12 Testeo de Sistema de Detección de Intrusos
13 Testeo de Medidas de Contingencia
14 Descifrado de Contraseña
15 Testeo de Denegación de Servicios
16 Evaluación de Políticas de Seguridad

4 Seguridad en las Comunicaciones
1 Testeo de PBX
2 Testeo del Correo de Voz
3 Revisión del FAX
4 Testeo del Modem

5 Seguridad Inalámbrica
1 Verificación de Radiación Electromagnética (EMR)
2 Verificación de Redes Inalámbricas [802.11]
3 Verificación de Redes Bluetooth
4 Verificación de Dispositivos de Entrada Inalámbricos
5 Verificación de Dispositivos de Mano Inalámbricos
6 Verificación de Comunicaciones sin Cable
7 Verificación de Dispositivos de Vigilancia Inalámbricos
8 Verificación de Dispositivos de Transacción Inalámbricos
9 Verficación de RFID
10 Verificación de Sistemas Infrarrojos
11 Revisión de Privacidad

6 Seguridad Física
1 Revisión de Perímetro
2 Revisión de monitoreo
3 Evaluación de Controles de Acceso
4 Revisión de Respuesta de Alarmas
5 Revisión de Ubicación
6 Revisión de Entorno

Evaluación de Riesgo

La evaluación de Riesgo es mantenida por el analista, todos los datos que sean recopilados sirven de soporte para una evaluación válida por medio de tests no privilegidos. Esto implica que si se recopila muy poca información o esta no es apropiada, puede no ser posible proveer una evaluación de riesgos correcta y el analista debe basarse en las mejores prácticas, las regulaciones correspondientes a la industria del cliente, la justificación de negocios del cliente, la política de seguridad del mismo, y las cuestiones legales para el cliente y su ambiente de negocios.

Evaluación de Riesgo

El riesgo significa que los límites de la presencia de seguridad tendrán un efecto perjudicial en la gente, la cultura de información, los procesos, negocios, imagen, propiedad intelectual, derechos legales o capital intelectual. Este manual mantiene cuatro dimensiones durante el análisis para minimizar cualquier estado de riesgo en el ambiente.

1 **Seguridad**

Todos los tests deben ejecutarse con la precaución necesaria para evitar los peores escenarios posibles, que impliquen grandes pérdidas. Esto implica que el analista mantenga por encima de cualquier cosa, el respeto por la seguridad humana, en la salud física y emocional y ocupacional.

2 Privacidad

Todos los análisis deben ejecutarse manteniendo el derecho a la privacidad personal sin importar la ley regional. La ética y el entendimiento de la privacidad son a menudos más avanzados que la legislación actual.

3 Practicidad

Todos los tests deben ser diseñados buscando la mínima complejidad, la máxima viabilidad y una profunda claridad.

4 Usabilidad

Todos los tests deben permanecer dentro del marco de seguridad util. Es decir, lo más seguro es lo menos bienvenido y perdonable. Los tests dentro de este manual son desarrollados para encontrar un nivel de seguridad útil (tambien conocido como seguridad práctica).

Seguridad Perfecta

En evaluación de riesgos, el OSSTM aplica la técnica de "Seguridad Perfecta", en seguridad perfecta los analistas calibran con el cliente que se puede considerar seguridad perfecta. Esto se

logra con la revisión de postura, que corresponde a las mejores practicas, las regulaciones en la industria del cliente, las justificaciones del negocio, la política de seguridad del cliente y los asuntos legales para el cliente y las regiones donde el mismo tenga negocios. El resultado es "Seguridad Perfecta" para el cliente. Los analistas pueden proveer un análisis comparativo entre el estado actual de seguridad y la "Seguridad Perfecta"

Mejores prácticas definidas dentro de la teoría hacia una "Seguridad Perfecta".

Servicios y acceso a Internet

- No usar Acceso Remoto no encriptado.
- No usar Acceso Remoto no autenticado.
- Las restricciones deniegan todo y permiten específicos.
- Monitorearlo y registrarlo todo.
- Descentralizar.
- Limitar la confianza entre sistemas.
- Poner en cuarentena las entradas y validarlas.
- Instalar únicamente las aplicaciones / servicios requeridos.
- Dividir capas de seguridad.
- Es mejor ser invisible - mostrar únicamente el servicio, nada más.
- La simplicidad previene los errores de configuración.

Computación Mobil

- Poner en cuarentena todas las redes entrantes y trafico de Internet.
- No usar Acceso Remoto no encriptado.
- No usar Acceso Remoto no autenticado.
- Encriptación acorde a las necesidades.
- Instalar las aplicaciones y/o servicios necesarios.
- Es mejor invisible - sin servicios ejecutándose.
- Exigir contrasseñas en BIOS.
- Entrenamiento en seguridad para aplicar las mejores prácticas y reconocer los eventos de seguridad es requisito para usuarios y personal de soporte.

Aplicaciones

- El uso de las características de seguridad debe ser una obligación.
- Asegurar las justificaciones de negocio para todas las entradas y salidas en una aplicación.
- Validar todas las entradas.
- Limitar confianzas (a sistemas y usuarios).
- Encriptar datos.
- Encriptar los componentes.
- Todas las acciones ocurren del lado del servidor.
- Definir capas de seguridad.

- Es mejor invisible - mostrar únicamente el servicio.
- Accionar alarmas.

Personal

- Autoridad Descentralizada.
- Responsabilidad Personal.
- Seguridad Personal y controles de privadad.
- Accesible únicamente por medio de gateway personales.
- Entrenamiento en definiciones legales y ética de las políticas de seguridad.
- Acceso al conocimiento de informacion e infraestructura limitado.

Valores de la Evaluación de Riesgo

Integrados a cada modulo, se encuentran los Valores de la Evaluación de Riesgo (RAVs). Estos se definen como la degradación de la seguridad (o elevación del riesgo) sobre un ciclo de vida específico, basándose en mejores prácticas para tests periódicos. La asociación de niveles de riesgo con ciclos ha probado ser un procedimiento efectivo para las métricas de seguridad.

Los conceptos de métrica de seguridad en este manual son para:

- Establecer un ciclo estándar de tiempo para testear y verificar con el fin de
- Mantener un nivel cuantificable de riesgo basado en
- La degradación de la seguridad (o elevación del riesgo) que ocurre naturalmente, con el tiempo y
- La habilidad de medir el riesgo con consistencia y detalle
- Ambos antes y después del análisis

A diferencia de la administración de riesgos convencional, los RAVs operan puramente en la aplicación de seguridad dentro de una organización. Estos toman en cuenta los controles tales como procesos, políticas, y procedimientos al operar en paralelo con la metodología de análisis. Mientras que la metodología de análisis examina estos controles, algunas veces de manera indirecta, los controles actuales no le interesan al analista, debido a que es la aplicación de estos controles la que determina los resultados de un análisis de seguridad. Una política bien escrita que no sea seguida no tendrá efecto alguno en la seguridad actual.

Los RAV están definidos matemáticamente por los siguientes factores:

1. Los grados de degradación de cada módulo por separado, según un nivel óptimo medido de un máximo teórico del 100% para propósitos de administración de riesgos.
2. El ciclo que determina la máxima longitud de tiempo que se requiere para que la degradación sea total (llegue a su máximo porcentual) basándose en prácticas recomendadas de seguridad y consenso.
3. La influencia de otros módulos ejecutados o no.
4. Pesos establecidos por las Dimensiones de Seguridad

5 El tipo de riesgo tal y como se designa por los Tipos de Riesgo OSSTM y si este ha sido a ***Identificado***, pero no investigado o con resultados no concluyentes. b ***Verificado***, con un positivo absoluto o una vulnerabilidad explotada, o
c ***No aplicable***, debido a que no existe porque la infraestructura o mecanismo de seguridad no se encuentra presente.

Tipos de Riesgos

A pesar que los tipos de riesgo parezcan ser subjetivos, la clasificación de riesgos en los siguientes tipos, es bastante objetiva al seguir el marco de trabajo del OSSTMM. Versiones futuras asegurarán su compatibilidad con CVE.

Vulnerabilidad

Una falla inherente en el mecanismo de seguridad mismo o que pueda ser alcanzada por medio de protecciones de seguridad, permitiendo el acceso privilegiado a la ubicación, gente, procesos del negocio, y personal o acceso remoto a los procesos, gente, infraestructura generando datos corruptos o eliminados. Una vulnerabilidad puede ser un metal en una puerta que se torna frágil a temperaturas bajo 0º C, un lector de huellas digitales que permite el acceso con dedos de goma, un dispositivo infrarojo que no tiene mecanismos de autenticación para realizar cambios en la configuración, o un error de traducción en un servidor web que permite la identificación del propietario de una cuenta bancaria por medio del número de esta.

Debilidad

Una falla inherente a la plataforma o ambiente en el que el mecanismo de seguridad reside, una mala configuración, falla de sobrevivencia, falla de usabilidad, o falla al cumplir los requerimientos de una Política de Seguridad. Una debilidad puede ser un proceso que no almacena datos transaccionales durante el tiempo límite legal, tal y como se establezca en las leyes locales, una alarma de ingreso que no suena si la puerta ha quedado abierta por un período de tiempo específico, un cortafuegos que devuelve mensajes ICMP de host inalcanzable para sistemas de red internos, un servidor de base de datos que permite consultas sin filtrar, una entrada sin monitoreo a un edificio considerado " seguro".

Filtrado de Información

Una falla inherente en el mecanismo de seguridad mismo, o que puede ser alcanzada por medio de medidas de seguridad que permiten el acceso privilegiado a información sensitiva o privilegiada acerca de datos, procesos de negocio, personal o infraestructura. Una fuga de información puede ser una cerradura con la combinación disponible por medio de señales audibles de cambio dentro de los mecanismos de la misma, un enrutador que brinda información SNMP

acerca de la red objetivo, una hoja de cálculo con los salarios de ejecutivos en una compañía privada, el teléfono celular privado del personal de marcadeo, un sitio web con información acerca de la próxima revisión del elevador de la compañía.

Preocupación

Un evento de seguridad que puede resultar al no seguir las practicas recomendadas de seguridad, y que por el momento no se presente como un peligro actual. Una preocupación puede ser el servicio FINGERD corriendo en un servidor de la organización que no requiere el servicio FINGER, una puerta de entrada vigilada que requiere que el celador deje la puerta para perseguir a un intruso y no se disponga de un nuevo celador haciendo presencia en la misma puerta, o empleados que se sientan con sus monitores y tableros visibles desde el exterior del perimetro de seguridad.

Desconocidos

Un elemento desconocido o sin identificación en el mecanismo de seguridad mismo, o que puede ser alcanzado a través de las medidas de seguridad y actualmente no tiene impacto conocido en la seguridad ya que tiende a no tener sentido o servir ningún propósito con la información limitada que el analista posea. Un desconocido puede ser una respuesta inesperada posiblemente de un enrutador en una red, indicando problemas en la misma, una frecuencia de radio no natural que proviene del perimetro de seguridad sin ofrecer información o identificación,o una hoja de cálculo con información privada acerca de la competencia.

La siguiente tabla provee los parámetros para los Valores de la Evaluación de Riesgos (RAVs)

	Verificado	Identificado	No Aplicable
Vulnerabilidad	3.2	1.6	0.4
Debilidad	1.6	0.8	0.3
Preocupación	0.8	0.4	0.2
Filtrado de Información	0.4	0.2	0.1
Desconocidos	0.2	0.1	-

Secciones y Módulos

La metodología está dividida en *secciones, módulos y tareas* . Las secciones son puntos específicos en el mapa de seguridad que se sobreponen entre si y comienzan a descubrir un todo que es mucho mayor a la suma de sus partes. Los módulos son el flujo de la metodología desde un punto de presencia de seguridad hacia el otro. Cada módulos tiene una salidad y una entrada. La entrada es la información usada en el desarrollo de cada tarea. La salidas es el resultado de las

tareas completadas. La salida puede o no ser datos analizados (también conocido como inteligencia) para servir como entrada para otro módulo. Incluso puede ocurrir que la misma salida sirva como entrada para más de un módulo o sección.

Algunas tareas no brindan resultados, esto significa que existen módulos para los cuales no hay entrada. Los módulos que no tienen entrada pueden ser ignorados durante el análisis. El hecho de ignorar módulos no indica necesariamente un análisis inferior, al contrario indica un nivel de seguridad superior.

Los módulos que no tienen salida como resultado, pueden significar una de tres cosas:

- Las tareas no fueron ejecutadas apropiadamente.
- Las tareas no se aplicaban.
- Las tareas revelaron niveles superiores de seguridad.
- Los datos resultantes de la tarea se analizaron inapropiadamente.

Es vital que la imparcialidad exista al ejecutar las tareas de cada módulo. Buscar algo que usted no tenga intención de encontrara puede llevarlo a encontrar exactamente lo que quiere. En esta metodología cada módulo inicia como una entrada y una salida exactamente por la necesidad de mantener la imparcilidad. Cada módulo brinda una guia de lo que puede ser revelado para profundizar mas aún en el flujo.

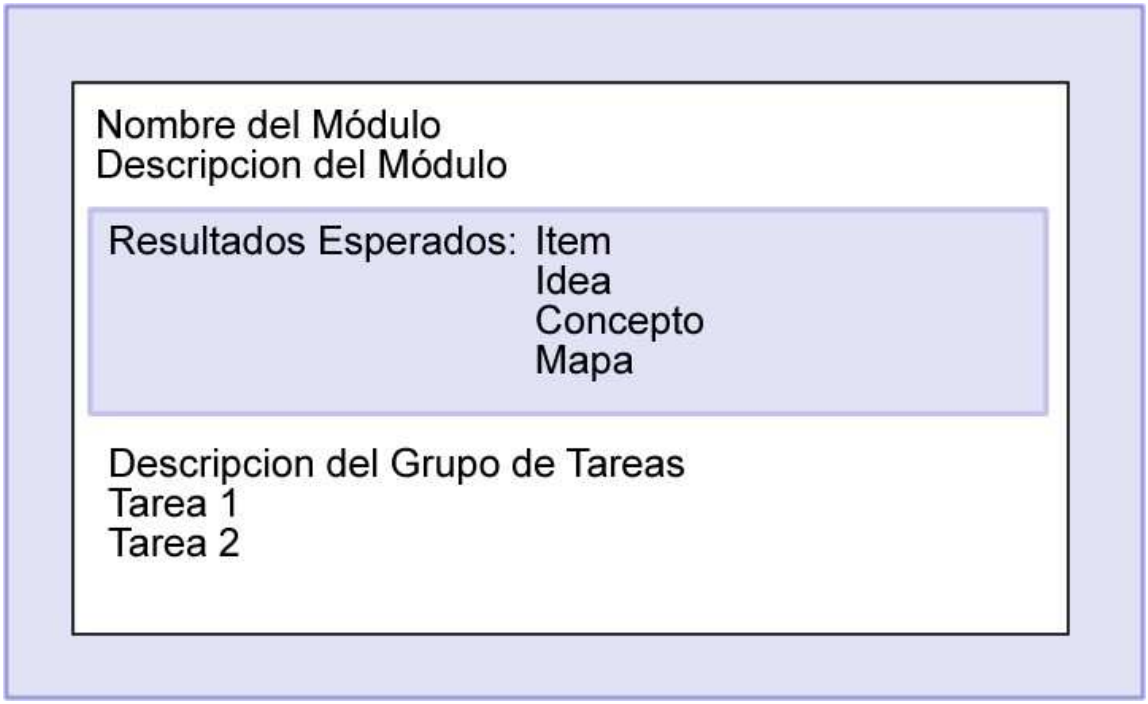
El tiempo es relativo. Grandes ambientes de test significan más tiempo gastado en cada sección, módulo o tarea. La cantidad de tiempo permitido antes de obtener resultados, depende del analista, el ambiente, y el ámbito del análisis. Un análisis adecuado es un balance del tiempo y energía dedicados al proyecto. El tiempo es dinero, y la energía es el límite del hombre y la capacidad de la máquina.

Identificar las tareas que puedan ser vistas como innecesarias y por lo tanto retiradas tranquilamente del análsiis es vital, cuando se definen los módulos a analizar para un sistema objetivo, donde el ámbito del proyecto o restricciones así lo requieran. Estas tareas omitidas, sin embargo, deben documentarse claramente y deben ser aceptadas previo al proceso de análisis.

Con la disposición del análisis como un servicio, es altamente importante indicarle al equipo encargado exactamente que no ha sido, o no será analizado, de tal forma que se pueda administrar la expectativa y la potencialmente inapropiada fe en la seguridad del sistema.

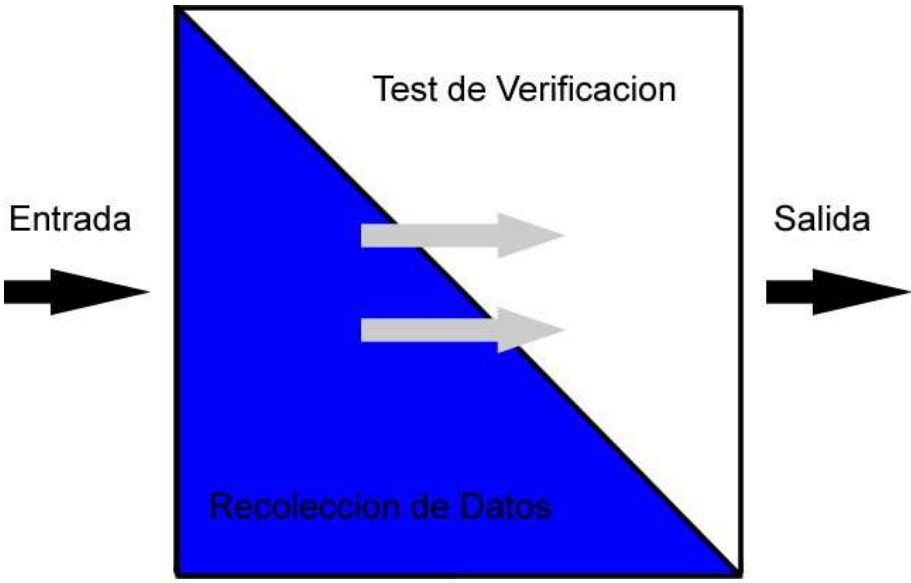
Módulos de Tests y Tareas

Módulo Ejemplo


Nombre del Módulo
Descripcion del Módulo
Resultados Esperados: Item
Idea
Concepto
Mapa
Descripcion del Grupo de Tareas
Tarea 1
Tarea 2

Metodología

La metodología fluye desde el módulo inicial hasta completar el módulo final. La metodología permite la separación entre recolección de datos y tests de verificación de y sobre los datos recolectados. El flujo tambien determina los puntos precisos de cuando extraer e insertar estos datos.



Al definir la metodología de análisis, es importante no restringir la creatividad del analista introduciendo estandares excesivamente formales e inflexibles que la calidad de los tests sufran. Adicionalmente, es importante dejar tareas abiertas a alguna interpretacion donde la definición exacta causará problemas a la metodología cuando una nueva tecnología sea introducida.

Cada módulo tiene una relación con el inmediatamente anterior y con el inmediatamente posterior. Cada sección tiene aspectos interrelacionados a otros módulos y algunos se interrelacionan con todas las otras secciones. Normalmente, los análisis de seguridad comienzan con una entrada que corresponde a las direcciones de los sitemas a ser analizados. El análisis de seguridad finaliza con el inicio de la fase de análisis y la construcción del informe final. Esta metodología no afecta la forma, tamaño, estilo o contenido del informe final ni especifica como los datos deben ser analizados. Esto es responsabilidad del analista de seguridad o la organización.

La secciones son el modelo total de seguridad dividido en porciones manejables y analizables. El módulo requiere una entrada para ejecutar las tareas del módulo y de otros módulos en otras secciones. Las tareas son los tests de seguridad a ejecutarse dependiendo de la entrada del módulo. Los resultados de las tareas pueden ser inmediatamente analizados para actuar como un resultado procesado o se pueden dejar en bruto (sin analizar). De cualquier modo, estos son considerados la salida del modulo. Esta salida es a menudo la entrada para el siguiente módulo o en algunos casos, como equipos recién descubiertos; pueden ser la entrada para un módulo anterior.

El modelo de seguridad completo puede ser dividido en secciones administrables para las pruebas. Cada sección puede a su vez ser vista como una colección de módulos de test con cada módulo dividido en un conjunto de tareas.

Sección A – Seguridad de la Información

Valores de la Evaluación de Riesgo

Módulo	Ciclo (dias)	Degradacion (%)	Influencia (x)
Análisis de Postura	No disponible	No disponible	No disponible
Revision de la Integridad de la Información	No disponible	No disponible	No disponible
Estudio de Inteligencia	No disponible	No disponible	No disponible

Recolección de Documentos en Internet	No disponible	No disponible	No disponible
Revision de Recursos Humanos	No disponible	No disponible	No disponible
Revisión del Análisis de la Competencia	No disponible	No disponible	No disponible
Revisión de los Controles de Privacidad	No disponible	No disponible	No disponible
Revisión de los Controles de la Información	No disponible	No disponible	No disponible

Módulos

1. Revisión de la Inteligencia Competitiva

La IC es la informacion recolectada a partir de la presencia en Internet que puede ser analizada con inteligencia de negocio. A diferencia del robo de propiedad intelectual encontrada en el hacking o el espionaje industrial, es que la IC tiende a no ser invasiva y mucho mas discreta. Este es un buen ejemplo de cómo la presencia en Internet se extiende mas alla de los hosts de la DMZ. Utilizar IC en un Test de Intrusión da valor de negocio a los componentes y puede ayudar a encontrar justificaciones de negocio para implementar distintos servicios.

Resultados Esperados:	Una medicion de las justificaciones de negocio de la red de la organizacion Tamano y alcance de la presencia en Internet Una medicion de la política de seguridad a planes futuros de la red

1. Realizar un mapa y medir la estructura de directorio de los servidores web.
2. Realizar un mapa y medir la estrutura de directorio de los servidores de FTP.
3. Examinar la base de datos WHOIS para los servicios de negocio relacionando los nombre de hosts registrados.
4. Determinar el costo de TI de la infraestructura de Internet basados en SO, Aplicaciones y Hardware.
5. Determinar el costo de soporte de la infraestructura basado en requerimientos salariales de los profesionales de TI, puestos de trabajo, cantidad de personal, curriculums publicados y responsabilidades.
6. Medir el entusiasmo (respuesta) de la organizacion basandose en grupos de noticias, tableros web, y los sitios de respuesta de la industria.
7. Grabar el numero de productos que se estan vendiendo electronicamente (para download)
8. Grabar el numero de productos encontrados en origenes P2P, sitios wares, cracks disponibles para las versiones, y la documentacion tanto interna como de terceras partes de los productos.

2. Revision de Privacidad

La revision de privacidad es el punto de vista legal y etico del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente y del empleado. El uso de estos datos es la preocupación de muchas personas privadas y la legislación no da reglas especificas considerando la privacidad. Aunque algunas de estas leyes son locales, todas ellas se aplican a la Internet y por lo tanto afecta a los auditores de seguridad internacionalmente.

Resultados Esperados:	Lista de cualquier revelacion Lista de las fallas de conformidad entre la politica publica y la practica actual Lista de los sistemas involucrados en la recoleccion de datos Lista de las tecnicas de obtencion de datos Lista de los datos obtenidos

1. Comparar publicamente la politica accessible con la practica actual
2. Comparar la practica actual con el fraude regional y las leyes de privacidad o cumplimiento
3. Identificar el tipo y tamano de la base de datos para el almacenamiento de los datos
4. Identificar los datos conseguidos por la organizacion
5. Identificar la ubicacion de almacenamiento de los datos
6. Identificar los tipos de cookies
7. Identificar las fechas de expiracion de las cookies
8. Identificar la informacion almacenada en las cookies
9. Verificar los metodos de encripcion de la cookie
10. Identificar la ubicacion del servidor de errors del web
11. Identificar web bug data gathered and returned to server

3. Recolección de Documentos

En este modulo es importante la verificación de la información testeada y perteneciente a varios niveles de lo que se considera seguridad de la información. La cantidad de tiempo otorgado para la búsqueda y extracción de la información es dependiente del tamano de la organización, el ámbito del proyecto, y de la longitud de tiempo planeado para el test. No obstante, mucho tiempo no siempre significa mas información pero puede eventualmente llevar a partes claves del rompecabezas de la seguridad.

Resultados Esperados:	Un perfil de la organizacion Un perfil de los empleados Un perfil de la red de la organizacion Un perfil de las tecnologias de la organizacion Un perfil de los socios, alianzas y estrategias de la organizacion

1. Examinar las bases de datos web y los caches pertencientes a objetivos y personal clave de la organización.
2. Investigar personas claves via paginas personales, curriculums publicados, afiliaciones organizacionales, información de directorios, datos de compañías, y el registro electoral.
3. Recopilar direcciones de email de la organización y direcciones personales de personas claves.
4. Buscar en las bases de datos laborales por niveles tecnológicos requeridos necesarios que tiene la organización.
5. Buscar en los grupos de noticias referencias y publicaciones de la organización y personas claves.
6. Buscar en los documentos codigos ocultos o revisions de datos.
7. Examinar referencias y publicacion de redes P2P de la organizacion y personas claves.

Sección B – Seguridad de los Procesos

Valores de la Evaluación de Riesgo

Modulo	Ciclo (dias)	Degradacion (%)	Influencia (x)
Revisión de la Postura	No disponible	No disponible	No disponible
Testeo de Solicitud	No disponible	No disponible	No disponible

Testeo de Solicitud Reversa	No disponible	No disponible	No disponible
Testeo de Sugerencia Dirigida	No disponible	No disponible	No disponible
Testeo de Personas Confiables	No disponible	No disponible	No disponible

Módulos

1. Testeo de Solicitud

Este es un metodo de obtener privilegios de acceso a una organización y sus activos preguntando al personal de entrada usando las comunicaciones como un teléfono, e-mail, chat, boletines, etc desde una posición “privilegiada” fraudulenta. El personal de entrada son quienes tienen la autoridad para dar privilegios de acceso a otros.

Resultados Esperados:	Lista de los metodos de código de acceso Lista de los códigos validos Nombres de las personas de entrada Métodos de obtención de esta información Lista de la información obtenida

1. Seleccionar una persona de entrada desde la información ya obtenida sobre el personal
2. Examinar los métodos de contacto con la persona de entrada desde el objetivo de la organizacion
3. Obtener información acerca de la persona de entrada (posición, hábitos, preferencias)
4. Contactar la persona de entrada y solicitar información desde una autoridad o posición privilegiada
5. Obtener información desde la persona de entrada
6. Enumerar cantidad de información privilegiada obtenida

2. Testeo de Sugerencia Dirigida

Este es un método de enumeración y enumeracion de puntos de acceso privilegiados a una organización y sus activos provocando a hablar mediante los medios de comunicaciones tal como el telefono, e-mail, chat, boletines, etc. a una ubicación fuera la orgnizacion desde una posición "privilegiada" fraudulenta. Esta tecnica requiere una "ubicación" para la persona a provocar a hablar tal como una pagina web, una direccion de e-mail,

Resultados Esperados:	Lista de los puntos de acceso Lista de las direcciones IP internas Métodos de obtención de esta información Lista de la información obtenida

1. Seleccionar una persona o personas a partir de la información ya obtenida sobre el personal
2. Examinar los métodos de contacto a las personas de la organización objetivo
3. Invitar a las personas a usar / visitar una ubicación
4. Obtener información de los visitantes
5. Enumerar los tipos y cantidad de informacion privilegiada obtenida

3. Testeo de las Personas Confiables

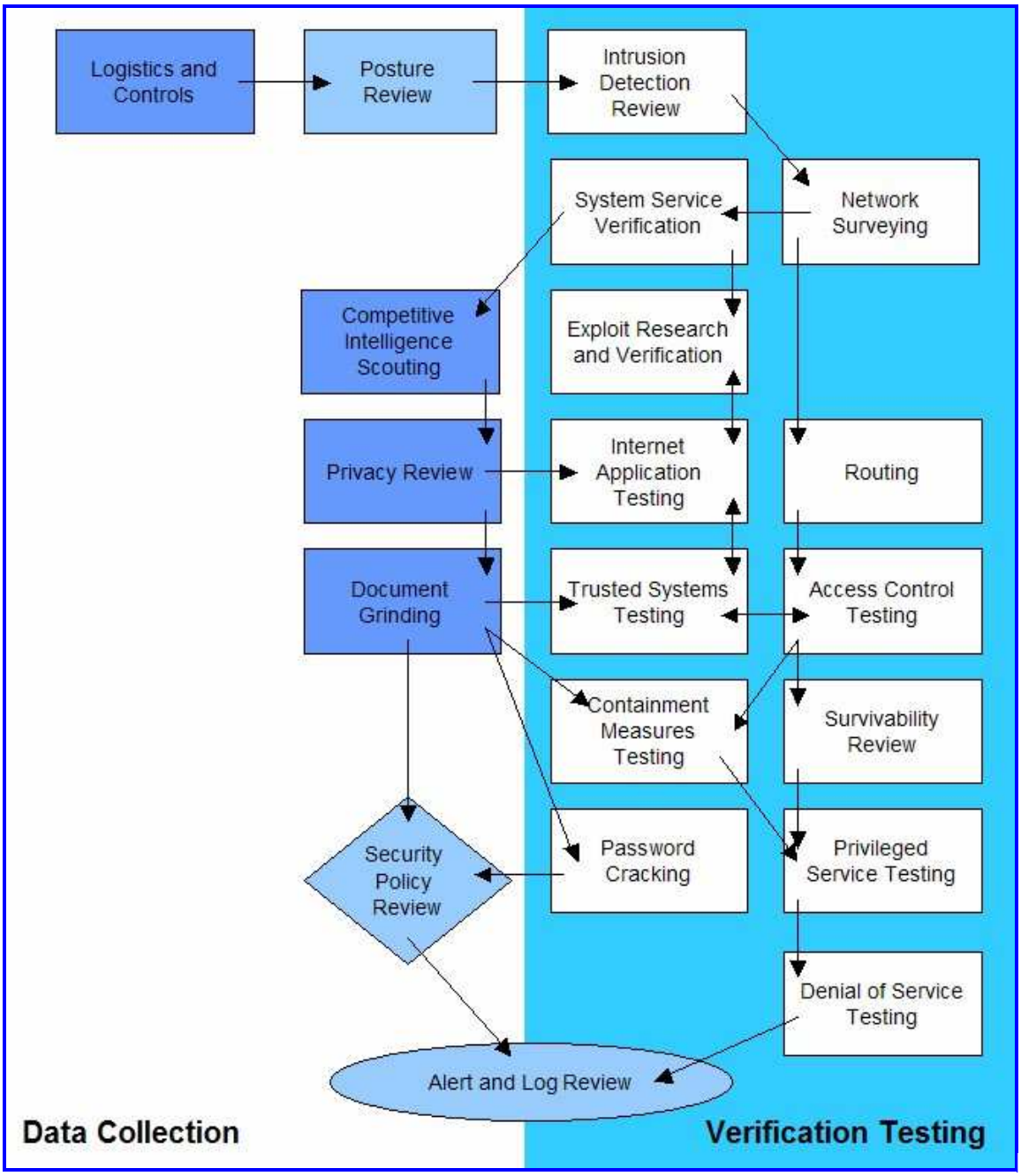
Este es un método de usar la posición de confianza tales como las de un empleado, vendedor, socio o hija de un empleado para inducir a la persona interna a la revelación de información concerniente a la organización objetivo.

Este modulo puede ser realizado mediante cualquier forma de comunicación o en persona.

Resultados Esperados:	Lista de las personas de confianza Lista de las posiciones de confianza Metodos de obtención de esta información Lista de la información obtenida

1. Seleccionar una persona o personas a partir de la información ya obtenida sobre el personal
2. Examinar los métodos de contacto a las personas de la organización objetivo
3. Contactar a la persona interna desde una posición de confianza
4. Obtener información de la persona interna
5. Enumerar los tipos y cantidad de información privilegiada obtenida

Sección C – Seguridad en las tecnologías de Internet



Valores de la Evaluación de Riesgo

Módulo	Ciclo (días)	Degradación (%)	Influencia (x)
Logística y Controles	0	0	1.6

Revisión de Configuración de Seguridad	178	12	
Revisión del Sistema de Detección de Intrusiones (IDS)	25	2.3	
Sondeo de Red	30	3	
Identificación de Servicios y Sistemas	7,19,54	1.7,3.9,2.15	
Obtención de Información Competitiva	17	7.3	
Revisión de la Política de Privacidad	96	2.9	
Obtencion de Documentos	96	8.7	
Testeo de Aplicaciones de Internet	67	5.8	
Búsqueda y Verificación de Vulnerabilidades	3	3.6	
Enrutamiento	34	3.2	
Testeo de Sistemas Confiados	42	4.1	
Testeo del Control de Acceso	34	2.9	
Descifrado de Contraseñas	21	7.8	
Testeo de Medidas de Contención	96	3.9	
Revisión de Supervivencia	178	9	
Testeo de Servicios Privilegiados	25	2.3	
Testeo de Denegación de Servicios	4	5.4	
Revision de la Política de Seguridad	124	6.7	
Revision de Registros y Alertas	0	0	

Subconjuntos de Protocolos

Protocolo	Subconjunto A	Subconjunto B
TCP	1,21,22,23,25,53,80,110,111,161,443	1,7,19,21,22,23,25,53,80,110, 111,137,139,161,389,443,445, 1433,1434,10001,12001,33580, 65535
UDP	1,20,53,65,67,68,69,139,161,445,1433,1434	1,7,13,19,20,53,65,67,68,69,139,16 1,445,1433,1434,1812,10001,12001 33580,65535

ICMP	0/0,3/3,3/4,8/0,11/0,13/0,15/0	0/0,3/0,3/1,3/2,3/3,3/4,3/5,3/6,3/ 0,8/0,11/0,13/0,15/0,30,33,34,40/1
IPv4	No disponible	No disponible
IPv6	No disponible	No disponible
OSPF	No disponible	No disponible
ISAKMP	No disponible	No disponible
IPSec	No disponible	No disponible
BGP	No disponible	No disponible
RTP	No disponible	No disponible
RSVP	No disponible	No disponible
IGMP	No disponible	No disponible
IOTP	No disponible	No disponible
L2TP	No disponible	No disponible

Diseño del Mapa

Enrutamiento
Confianzas
Puntos de Acceso
Segmentos de ID de Alarmas
Servicios
Control de Acceso
Supervivencia

INCOMPLETO

Módulos

1. Logística y Controles

El propósito de este módulo es reducir los falsos positivos y negativos realizando los ajustes necesarios en las herramientas de análisis.

Resultados Esperados:	Discrepancias por el Ancho de Banda usado en el Testeo Paquetes TCP perdidos Paquetes UDP perdidos Paquetes ICMP perdidos Problemas de enrutamiento Trafico de Enrutamiento del ISP y Vendedores de Tráfico

Comprobaciones de Error

1. Examinar la ruta a la red objetivo en busca de paquetes TCP perdidos.
2. Examinar la ruta a la red objetivo en busca de paquetes UDP perdidos.
3. Examinar la ruta a la red objetivo en busca de paquetes ICMP perdidos.
4. Medir el tiempo utilizado en el recorrido TCP de los paquetes.
5. Medir la latencia TCP a través de conexiones TCP.
6. Medir el porcentaje de paquetes aceptados y respondidos por la red objetivo.
7. Medir la cantidad de paquetes perdidos o rechazos de conexión en la red objetivo.

Enrutamiento

8. Examinar el camino de enrutamiento al objetivo desde los sistemas de ataque.
9. Examinar el camino de enrutamiento para el ISP del objetivo.
10. Examinar el camino de enrutamiento para el Vendedor de Trafico Principal del ISP objetivo
11. Examinar el uso de Ipv6 para cada uno de los sistemas activos en la red.

2. Sondeo de Red

El sondeo de red sirve como introducción a los sistemas a ser analizados. Se podría definir mejor como una combinación de recolección de datos, obtención de información y política de control. A pesar que a menudo es recomendable desde un punto de vista legal el definir exactamente y contractualmente los sistemas a analizar si usted es un auditor externo o aun si es el administrador de sistemas, puede ser que no pueda empezar con los nombres de sistema o IPs en concreto. En ese caso es necesario sondear y analizar. La clave es encontrar el número de sistemas alcanzables que deben ser analizados, sin exceder los limites legales de lo que se quiere analizar. Por lo tanto, el sondeo de red es simplemente una forma de empezar un test; otra forma sería recibir el

rango de direcciones IP a comprobar. En este módulo, no se realiza ningún tipo de intrusión directamente en los sistemas, excepto en los sitios considerados un dominio cuasi-público.

En términos legales, un dominio cuasi-público es una tienda que invita a realizar compras. La tienda puede controlar el acceso y puede denegar la entrada a ciertos individuos, aunque la mayor parte de la tienda esté abierta al público en general (incluso en aquellos casos en que se monitoree a los usuarios). Este es el paralelismo al e-business o a un sitio web.

A pesar de no ser realmente un módulo en la metodología, el sondeo de red es un punto de partida. Muy a menudo se detectan más hosts durante el test. Hay que tener en cuenta que los hosts descubiertos posteriormente pueden ser añadidos en las pruebas como un subconjunto de los sistemas definidos y a menudo solamente con el permiso o colaboración del equipo de seguridad interna de la organización a analizar.

Resultados esperados:	Nombres de Dominio Nombres de Servidores Direcciones IP Mapa de Red Información ISP / ASP Propietarios del Sistema y del Servicio Posibles limitaciones del test

Respuestas del Servidor de Nombres.

1. Examinar la información del registro de dominio en busca de servidores.
2. Encontrar el propietario del bloque de direcciones IP.
3. Consultar los servidores de nombres primario, secundario y del ISP en busca de hosts y subdominios.
4. Encontrar bloques de IPs Ipv6 utilizados a través de consultas a los DNS.

Examinar la pared externa de la red.

5. Usar múltiples trazas a la puerta de enlace para definir los routers y segmentos externos de la red.

Examinar pistas de la organización a analizar.

6. Inspeccionar los logs del servidor web y los logs de intrusión en busca de eventos de los sistemas de la organización a analizar.
7. Inspeccionar mensajes de grupos de noticias y listas de distribución en busca de eventos de los sistemas de la organización a analizar.

Filtración de información

8. Examinar el código fuente y scripts del servidor web en busca de servidores de aplicación y enlaces internos.
9. Examinar las cabeceras de los correos electrónicos, los mensajes devueltos y los destinatarios de las alertas y eventos del sistema de los servidores.
10. Buscar información sobre la organización a analizar en los grupos de noticias.

11. Buscar en bases de datos de empleos y en periódicos ofertas de puestos de trabajo en Tecnologías de la Información dentro de la organización a analizar, referencias a hardware y software.
12. Buscar en servicios P2P conexiones dentro de la red objetivo y datos referentes a la organización.

3. Identificación de los Servicios de Sistemas

El escaneo de puertos es la prueba invasiva de los puertos del sistema en los niveles de transporte y red. También se incluye aquí la validación de la recepción del sistema a protocolos tunelizados, encapsulados o de enrutamiento. En este módulo se deben enumerar los servicios de Internet activos o accesibles así como traspasar el cortafuegos con el objetivo de encontrar más máquinas activas. La pequeña cantidad de protocolos empleados aquí tiene el objetivo de resultar en una definición clara de los objetivos. Es por esto que algunos de los protocolos no aparecen. El testeo de diferentes protocolos dependerá del tipo de sistema y servicios que ofrecen los sistemas. En la sección Referencias de Testeo aparece una lista más completa de protocolos.

Cada servidor activo en Internet dispone de 65.536 puertos TCP y UDP posibles (incluido el Puerto 0). En cualquier caso, no siempre es necesario comprobar todos estos puertos en cada sistema. Esto se deja a la libre elección del equipo que realiza los tests. Los puertos que son importantes para el testeo según el servicio que ofrecen se listan con las tareas del módulo. Otros números de puertos empleados en los escaneos se deben obtener de bases de datos consensuadas en webs de proyectos de intrusión tales como www.dshield.org.

Una vez los puertos abiertos han sido identificados, es necesario llevar adelante un análisis de la aplicación que escucha tras dicho servicio. En algunos casos, más de una aplicación puede encontrarse detrás de un servicio donde una aplicación es la que realmente escucha en dicho puerto y las otras se consideran componentes de la aplicación que escucha. Un buen ejemplo de esto es PERL que se instalo para ser usado por las aplicaciones web. En este caso, el servicio que escucha es el demonio HTTP y el componente es PERL.

Tras la identificación de los servicios, el siguiente paso es identificar el sistema mediante las pruebas sobre el sistema con el fin de obtener respuestas que puedan distinguir su sistema operativo y su versión.

Resultados Esperados:	Puertos abiertos, cerrados y filtrados Direcciones IP de los sistemas activos Direccionamiento de los sistemas de la red interna Lista de los protocolos descubiertos de tunelizado y encapsulado Lista de los protocolos descubiertos de enrutado soportados Servicios activos Tipos de Servicios Tipo y nivel de parcheado de las Aplicaciones de los Servicios Tipo de Sistema Operativo Nivel de parcheado Tipo de Sistema Lista de sistemas activos Mapa de la red

Enumeración de sistemas

1. Recoger respuestas de broadcast desde la red
2. Intentar traspasar el cortafuegos con valores estratégicos de TTLs (Firewalking) para todas las direcciones IP.
3. Emplear ICMP y resolución inversa de nombres con el objetivo de determinar la existencia de todos los sistemas en la red.
4. Emplear paquetes TCP con puerto origen 80 y el bit ACK activo en los puertos de destino 3100-3150, 1001-10050, 33500-33550 y 50 puertos aleatorios por encima del 35000 para todos los sistemas de la red.
5. Emplear paquetes TCP fragmentados en orden inverso mediante escaneos FIN, NULL y XMAS en los puertos destino 21, 22, 25, 80 y 443 para todos los servidores de la red.
6. Usar escaneos TCP SYN sobre los puertos 21, 22, 25, 80 y 443 para todos los servidores de la red.
7. Emplear intentos de conexión a DNS para todos los servidores de la red.
8. Emplear FTP y Proxies para relanzar los escaneos al interior de la DMZ para los puertos 22, 81, 111, 132, 137 y 161 para todos los servidores de la red.

Enumeración de Puertos

9. Usar escaneos SYN TCP (Half-Open) para enumerar puertos abiertos, cerrados o filtrados para aquellos puertos TCP utilizados por defecto en el test, en todos los servidores de la red.
10. Usar scaneos TCP full connect para escanear todos los puertos por encima del 1024 en todos los servidores de la red.
11. Usar escaneos TCP fragmentados en orden inverso para enumerar puertos y servicios para el conjunto de puertos definidos en el Apéndice B por defecto para todos los servidores de la red.
12. Usar escaneos UDP para enumerar puertos abiertos o cerrados para los puertos UDP por defecto si UDP no está siendo filtrado. [Recomendación: primero comprobar el sistema de filtrado para un subconjunto de puertos UDP.]

Verificación de Respuestas para Varios Protocolos

13. Verificar y examinar el uso de tráfico y protocolos de enrutamiento.
14. Verificar y examinar el uso de protocolos no estándar.
15. Verificar y examinar el uso de protocolos cifrados.
16. Verificar y examinar el uso de TCP e ICMP sobre IPV6.

Verificación de Respuestas a Nivel de Paquete

17. Identificar la predictabilidad de las secuencias TCP.
18. Identificar la predictabilidad de los números de secuencia TCP ISN.
19. Identificar la predictabilidad de la Generación de Secuencia IPID.
20. Identificar el up-time del sistema.

Identificación de Servicios

21. Relacionar cada puerto abierto con un servicio y protocolo.
22. Identificar el nivel de parcheado del sistema a partir de su up-time.
23. Identificar la aplicación tras el servicio y su nivel de parcheado empleando los banners o la identificación de huellas.
24. Verificar la aplicación y su versión en el sistema.
25. Localizar e identificar el remapeo de servicios o la redirección de sistemas.

26. Identificar los componentes de los servicios en escucha.
27. Usar peticiones propias de Troyanos y servicios UDP en todos los sistemas de la red.

Identificación de Sistemas

28. Examinar las respuestas de los sistemas para determinar el tipo de sistema operativo y su nivel de parcheado.
29. Examinar las respuestas de las aplicaciones para determinar su sistema operativo y su nivel de parcheado.
30. Verificar la predicción de secuencia TCP para todos los servidores de la red.
31. Busque ofertas de trabajo donde obtener información sobre los servidores y aplicaciones del objetivo.
32. Buscar en boletines técnicos y grupos de noticias información sobre los servidores y las aplicaciones del objetivo.
33. Relacionar la información recopilada con las respuestas de los sistemas para ajustar los resultados.

4. Búsqueda de Información Competitiva

La Búsqueda de IC es la búsqueda de información útil a partir de la presencia que se tiene en Internet y que puede ser tratada como información sobre el negocio. A diferencia del robo de propiedad intelectual que se da en el espionaje industrial o el hacking, la IC tiende a ser no invasiva y mucho más sutil. Es un buen ejemplo de cómo la presencia en Internet se extiende mucho más allá de los sistemas que se disponen en una DMZ. Usando la IC en un test de intrusión le da un valor añadido a sus diferentes componentes y puede ayudar para encontrar justificaciones a nivel de negocio para implementar determinados servicios.

Resultados Esperados:	Una medida de las justificaciones de negocio sobre la red de la organización Tamaño y alcance de la presencia en Internet Una medicion de la politica de seguridad a planes futuros de la red

Información del Negocio

1. Realizar un mapa y medir la estructura de directorio de los servidores web.
2. Realizar un mapa y medir la estrutura de directorio de los servidores de FTP.
3. Examinar la base de datos WHOIS en busca de servicios relacionados con los nombres de los servidores.
4. Determinar el coste de la infraestructura en Sistemas de Información a partir de sus Sistemas Operativos, Aplicaciones y Hardware.
5. Determinar el coste de mantenimiento de la infraestructura a partir del salario de la zona para profesionales de TI, ofertas de trabajo, cantidad de personal, curriculums publicados y cargos.
6. Medir el entusiasmo (respuesta) de la organizacion basandose en grupos de noticias, tableros web, y los sitios de respuesta de la industria.
7. Registrar el número de productos que se venden electrónicamente (para descargar).

8. Registrar el número de productos encontrados en fuentes P2P, sitios de software pirata, cracks disponibles para versiones específicas y documentación tanto interna como de terceras partes sobre los productos.
9. Identificar socios del negocio.
10. Identificar los clientes a partir de organizaciones de los mismos sectores industriales.
11. Verificar la claridad y facilidad de uso del proceso de compra de productos.
12. Verificar la claridad y facilidad de uso del proceso y política de devoluciones.
13. Verificar que todos contratos realizados a través de Internet desde la firma digital a la pulsación del botón que implica la aceptación de las cláusulas por parte del cliente final pueden ser repudiadas inmediatamente y durante un período de 7 días.

5. Revisión de Privacidad

La revisión de privacidad se centra en como se gestiona, desde un punto de vista ético y legal, el almacenamiento, transmisión y control de datos de información privada perteneciente a empleados y clientes. La utilización de estos datos supone una gran preocupación para muchas personas y es por esto que la legislación está definiendo reglas específicas con relación a la privacidad. Aunque muchas de estas leyes son locales, todas son aplicables a Internet y por tanto afectan de forma internacional a todos los auditores de seguridad.

Para estas pruebas es necesario entender la diferencia entre información privada e información personal: por información privada entendemos aquella información que generalmente sólo es conocida por la persona a la que pertenece y la autoridad que ha recopilado dichos datos. Algunos ejemplos de información privada podrían ser transcripciones de Universidad, cantidades de dinero donadas a la Iglesia, nombres de ex-novias o exnovios, y quizás un diario de la infancia un tanto embarazoso. Por otro lado, información personal es aquella información que describe una persona o su estilo de vida, como por ejemplo la fecha de nacimiento, color de pelo, ojos, nombre de los miembros de su familia, banco que utiliza, nombre de sus mascotas, preferencias sexuales, religión, o color favorito.

Adicionalmente, la información de identificación personal es aquella información que permite derivar la identidad de una persona por sí sola o en conjunto. Podría ser un nombre de persona o un número de identificación.

Resultados Esperados:	Listado de cualquier revelación Listado de las inconsistencias entre la política que se ha hecho pública y la práctica actual que se hace de ella Listado de los sistemas involucrados en la recolección de datos Listado de las técnicas de recolección de datos Listado de los datos recolectados

Política

1. Identificar la política de privacidad pública

2. Identificar los formularios web
3. Identificar el tipo y la localización de la base de datos donde se almacenan los datos recolectados
4. Identificar los datos recolectados por la organización
5. Identificar la localización de los datos almacenados
6. Identificar los tipos de cookies
7. Identificar el tiempo de expiración de las cookies
8. Identificar la información guardada en las cookies
9. Verificar los métodos de cifrado de las cookies
10. Identificar la claridad de la informacion relacionada con opt-out
11. Identificar la facilidad de usar opt-out
12. Identificar los gifs de publicidad y bugs web en los servicios web y en los correos electrónicos
13. Identificar la localización de los gifs de publicidad
14. Identificar los bugs de web recogidos y devueltos al servidor

Difamacion y Falsa Divulgacion

15. Identificar las personas, organizaciones e instituciones reales a las que corresponden realmente las ficticias.
16. Identificar personas u organizaciones retratadas de forma negativa.

Apropiación

17. Identificar personas, organizaciones o materiales que por ellos mismos o por similitud son utilizados comercialmente en sitios web o anuncios publicitarios.

Revelación de Datos Privados

18. Identificar información de empleados, organizaciones o materiales que contienen información privada.

6. Obtención de Documentos

Este módulo es importante para la verificación de gran cantidad de la información probada y pertenece a muchos de los niveles de lo que se considera seguridad de la información. La cantidad de tiempo concedida a la búsqueda y extracción de información depende del tamaño de la organización, el ámbito del proyecto y el tiempo planificado para la auditoría. La dedicación de más tiempo no siempre significa la obtención de más información pero puede conducir a piezas claves del rompecabezas de seguridad.

Resultados Esperados:	Un perfil de la organización Un perfil de los empleados Un perfil de la red de la organización Un perfil de las tecnologías utilizadas por la organización Un perfil de los partners, alianzas y estrategias de la organización

1. Examinar bases de datos de webs y caches buscando la organización objetivo y personas clave.
2. Investigar personas claves via paginas personales, resumenes publicados, afiliaciones organizacional, información de directorios, datos de compañías, y el registro electoral.
3. Recopilar direcciones de e-mail corporativas y personales de las personas clave.
4. Buscar en bases de datos de trabajo conjuntos de perfiles tecnológicos requeridos por la organización objetivo.
5. Buscar en grupos de noticias referencias y mensajes enviados desde dentro de la organización y por personas claves de la organización.
6. Buscar documentos que contengan códigos ocultos o datos de revisión.
7. Examinar redes P2P (Peer-to-Peer) con referencias o envíos desde dentro de la organización y por personas claves de la organización.

7. Búsqueda y Verificación de Vulnerabilidades

La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red.

La investigación concerniente a la búsqueda de vulnerabilidades es necesaria hasta prácticamente el momento de la entrega del informe. Esta investigación incluye la búsqueda en bases de datos online y listas de correo relativas a los sistemas y redes que se están auditando. No se debe limitar la búsqueda a la web, también se debe considerar la utilización del IRC, grupos de noticias, y sitios FTP underground.

La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. Aunque muchos escáneres automáticos están actualmente tanto en el mercado como en el mundo underground, es imporante para los auditores identificar e incorporar en las pruebas que realizan los scripts y exploits que existen actualmente en el mundo underground. No obstante, es necesaria la verificación manual para eliminar falsos positivos, expandir el ámbito de hacking y descubrir el flujo de datos de entrada y salida de la red. La búsqueda manual de vulnerabilidades hace referencia a las personas que delante del ordenador utilizan la creatividad, la experiencia y la ingenuidad para probar la red objetivo.

Resultados Esperados:	Tipo de aplicación o servicio por vulnerabilidad Niveles de parches de los sistemas y aplicaciones Listado de posibles vulnerabilidades de denegación de servicio Listado de áreas securizadas a través de ocultación o acceso visible Listado de vulnerabilidades actuales eliminando falsos positivos Listado de sistemas internos o en la DMZ Listado de convenciones para direcciones de e-mail, nombres de servidores, etc.. Mapa de red

1. Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.
2. Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.
3. Intentar determinar vulnerabilidades por tipo de aplicación y sistema.
4. Intentar ajustar vulnerabilidades a servicios.
5. Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.
6. Realizar pruebas redundantes al menos con 2 escáneres automáticos de vulnerabilidades.
7. Identificar todas las vulnerabilidades relativas a las aplicaciones.
8. Identificar todas las vulnerabilidades relativas a los sistemas operativos.
9. Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los sistemas objetivo.

10. Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.
11. Verificar todos los positivos (Se debe tener en cuenta el contrato firmado con la organización objetivo en el caso de estar intentando penetrar o si se puede llegar a provocar una denegación de servicio).

8. Testeo de Aplicaciones de Internet

Un test de Aplicaciones de Internet emplea diferentes Tècnicas de testeo de Software para encontrar “fallos de seguridad” en aplicaciones cliente/servidor de un sistema desde Internet. En este módulo, nos referimos a aplicaciones cliente/servidor que sean desarrolladas por los administradores de sistema con propositos de la empresa y programadas con cualquier tecnología y lenguaje de programación. E.j. Aplicaciones web para transacciones entre empresas es un objetivo en este módulo. Tests como "Caja Negra" y/o "Caja Blanca" pueden ser utilizados en este módulo.

Resultados Esperados:	Lista de Aplicaciones Lista de los Componentes de las Aplicaciones Lista de las Vulnerabilidades de las Aplicaciones Lista de los Sistemas Confiados por las Aplicaciones

Re-Ingenieria

1. Descomponer o Deconstruir los códigos binarios, si es posible.
2. Determinar las Especificaciones de Protocolo de la Aplicación Cliente/Servidor
3. Adivinar la lógica del programa de los mensajes de error/debug en las salidas del programa y en el rendimiento y comportamiento del programa.

Autenticacion

4. Buscar las posibles combinaciones de contraseñas por fuerza bruta en las aplicaciones.
5. A ser posible, buscar credenciales de cuentas válidas por fuerza bruta.
6. Saltarse el sistema de autenticación con una validación cambiada.
7. Saltarse el sistema de autenticación reproduciendo informacion de la autenticacióna
8. Determinar la lógica de la aplicación para mantener las sesiones de autenticación - número (consecutivo) de intentos fallidos, intentos fuera de tiempo, etc.
9. Determinar las limitaciones de control de acceso en las aplicaciones - permisos de acceso, duración de las sesiones, tiempo inactivo.

Administracion de Sesiones

10. Determinar la Informacion de Administracion de Sesiones – numero de sesiones concurrentes, Autenticaciones basadas en IP, Autenticacion basada en roles, Autenticacion basada en Identidad, uso de Cookies, ID de sesión dentro de las secuencias de codificación de la URL, ID de sesión en campos HTML ocultos, etc.
11. Adivinar la secuencia y formato de la ID de sesión.

12. Determinar si la ID de sesión esta formada con información de direcciones IP; mirar si la misma información de sesión puede ser recuperada y reutilizada en otra máquina.
13. Determinar las limitaciones de mantenimiento de sesión - uso del ancho de banda, limitaciones de bajadas/subidas de archivos, limitaciones en transacciones, etc.
14. Reunir bastante informacion con URL's exactas, instrucciones exactas, secuencias de accion / saltos de secuencia y/o omisiones de las páginas.
15. Reunir información sensible a partir de ataques Hombre-en-el-Medio.
16. Inyectar excesa/falsa información con técnicas de Hijacking.
17. Reproducir la información reunida para engañar a las aplicaciones.

Manipulación de la información de entrada.

18. Encontrar las limitaciones de las variables definidas y de los protocolos - longitud de datos, tipo de datos, formato de la estructura.etc.
19. Usar cadenas largas de caracteres para encontrar vulnerabilidades de desbordamientos de memoria en las aplicaciones.
20. Concatenar comandos en las cadenas de entrada de las aplicaciones.
21. Inyectar comandos SQL en las entradas de cadenas de caracteres de aplicaciones web basadas en bases de datos.
22. Examinar vulnerabilidades "Cross-Site Scripting" en las aplicaciones web del sistema.
23. Examinar accesos a directorios/ficheros no autorizados con directorios/rutas traversales en las entradas de cadenas de caracteres de las aplicaciones.
24. Usar cadenas específicas de codificación URL y/o codificación Unicode para saltarse los mecanismos de validación de las aplicaciones.
25. Ejecutar comandos remotos a traves de "Server Side Include".
26. Manipular el estado de las cookies (session/persistent) para tirar o modificar la lógica dentro de las aplicaciones web "server-side".
27. Manipular los campos variables (ocultos) en los formularios HTML para tirar o modificar la lógica en las aplicaciones web "server inside".
28. Manipular las variables "Referrer", "Host", etc. del protocolo HTTP para tirar o modificar la lógica en las aplicaciones web "server inside".
29. Usar información de entrada ilógica/ilegal para testear las rutinas de error de la aplicación y encontrar mensajes de error/depuración que sean útiles.

Manipulación de la Información de salida

30. Recuperar información importante/comprometedora guardadas en las cookies.
31. Recuperar información importante/comprometedora en la caché de la aplicacion cliente.
32. Recuperar información importante/comprometedora guardada en los objetos con número de serie.
33. Recuperar información importante/comprometedora guardada en los archivos temporales y objetos.

Filtración de información

34. Buscar información utilizable en campos ocultos de variables en formularios HTML y comentarios en los documentos HTML.
35. Examinar la información contenida en los banners de la aplicación, instrucciones de uso, mensajes de bienvenida, mensajes de despedida, mensajes de ayuda, mensajes de error/depuración, etc.

9. Enrutamiento

Las Protecciones de un Router son unas defensas que se encuentran a menudo en una red donde se restringe el flujo del tráfico entre la red de la empresa e Internet. Opera en una política de seguridad y usa ACL's (Access Control Lists o Lista de Control de Acceso) que acepta o deniega paquetes. Este módulo está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede puede ser aceptado en la red; todo lo demás debe ser denegado. La protección también debe estar diseñada para restringir el flujo de salida de ciertos tipos de tráfico. Los Router estan siendo cada vez más complejos y algunaos tienen propiedades desconocidas para el auditor y aveces para la organización auditada. El papel del auditor es en parte determinar la función del router dentro de la DMZ.

Resultados Esperados:	Tipo de Router y Propiedades implementadas Información del router como servicio y como sistema Perfil de la política de seguridad de una red a partir de la ACL Lista de los tipos de paquetes que deben entrar en la red Mapa de las respuestas del router a varios tipos de tráfico Lista de los sistemas vivos encontrados

El Router y sus características

1. Verificar el tipo de router con información reunida de la obtencion de Inteligencia.
2. Verificar si el router está dando servicio de traducción de direcciones de red (NAT).
3. Verificar las intrusiones con opciones TTL estratégicas en los paquetes ,(Firewalking) hecho en el módulo de escaneo de puertos.

Verificar la configuración de las ACL's del router

4. Testear la ACL del router en contrade las políticas de seguridad y en contra de la regla "Deny All".
5. Verificar si el router está filtrando el tráfico de la red local hacia afuera.
6. Verificar que el router esté haciendo detección de direcciones falsas.
7. Verificar las intrusiones desde un escaneo inverso en el módulo de escaneo de puertos.
8. Testear las capacidades externas del router desde el interior.
9. Cuantificar la habilidad que tiene el router para manejar fragmentos de paquetes muy pequeños.
10. Cuantificar la habilidad del router para manejar paquetes grandes.
11. Cuantificar la habilidad del router para manejar fragmentos coincidentes como los usados en ataques del tipo TEARDROP.

10. Testeo de Sistemas Confiados

El propósito de los testeos de sitemas confiados es afectar la presencia en Internet planteandose como una entidad confiada en la red. El escenario de testeo es a veces más teoria que práctica, y en realidad mas que oscurecer la frontera entre un Test de Vulnerabilidad y un Testeo de Cortafuefos / ACLS, es dicha frontera.

Resultados Esperados:	Mapa de los sistemas dependientes de otros sistemas Mapa de las aplicaciones con dependencias a otros sistemas Tipos de vulnerabilidades que afectan a los sistemas de confianzas y aplicaciones

1. Verificar las relaciones determinadas en la obtencion de Inteligencia, Testo de Aplicaciones y Testeo de Servicios.
2. Testear las relaciones entre varios sistemas a traves de provocación de eventos "event triggering" o engaño de origen.
3. Verificar que los sistemas puedan ser engañados. 4. Verificar qué aplicaciones pueden ser engañados.

11. Testeo de Control de Acceso

El cortafuegos controla el flujo del tráfico de la red corporativa, la DMZ, e Internet. Opera en una política de seguridad y usa ACL's (Listas de Control de Acceso). Este módulo está diseñado para segurar que solo lo que debe estar expresamente permitido puede ser aceptado dentro de la red, todo lo demás debe ser denegado. De manera adicional, el auditor debe entender la configuración del cortafuegos y cartografia que se provee entre los servidores y los servicios que hay detrás. Repasando los logs necesarios de los servidores para verificar los tests desempeñados en presencia de Internet, especialmente en casos donde los resultados de los tests no son inmediatamente evidentes para el auditor. Algunos que son desconocidos son destinados para el analista, quien no ha revisado los logs.

Resultados Esperados:	Información en el firewall como servicio y como sistema Información de las características implementadas en el firewall Perfil de la política de seguridad de la red a partir de la ACL Lista de los tipos de paquetes que deben entrar en la red Lista de tipos de protocolos con acceso dentro de la red Lista de los sistemas "vivos" encontrados Lista de paquetes, por número de puerto, que entran en la red Lista de protocolos que han entrado en la red Lista de rutas sin monitorizar dentro de la red

El Cortafuegos y sus características.

1. Verificar el tipo de router con información reunida de la Obtención de Inteligencia.
2. Verificar si el router está dando servicio de traducción de direcciones de red (NAT).
3. Verificar las intrusiones con opciones TTL estratégicas en los paquetes ,(Firewalking) hecho en el módulo de escaneo de puertos.

Verificación de la configuración de las ACL

4. Testear la ACL del cortafuego en contra de las políticas de seguridad y en contra de la regla "Denegar Todo".
5. Verificar si el cortafuegos está filtrando el tráfico de la red local hacia afuera.
6. Verificar que el cortafuegos esté haciendo detección de direcciones origenes falsas.
7. Verificar las intrusiones desde un escaneo inverso en el módulo de Escaneo de Puertos.
8. Testear las capacidades externas del cortafuegos desde el interior.
9. Determinar el éxito de los métodos de identificación de cortafuegos a traves de las distintos paquetes de respuesta.
10. Verificar la posibilidad de escanear usando tecnicas ocultas SYN para enumeración a través del cortafuegos.
11. Verificar la posiblidad de escanear para enumeración usando puertos origenes especificos.
12. Cuantificar la habilidad del cortafuegos para manejar fragmentos superpuestos como los usados en ataques del tipo TEARDROP.
13. Cuantificar la habilidad del cortafuegos para manejar fragmentos de paquetes diminutos.

14. Testear la habilidad del cortafuegos para manejar series de paquetes SYN entrantes (inundación) 15. Testear la respuesta del cortafuegos a paquetes con la bandera RST activada.
16. Testear el mantenimiento del cortafuegos con paquetes UDP estándar.
17. Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando paquetes ACK.
18. Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando paquetes FIN.
19. Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando paquetes NULL.
20. Verificar la habilidad del cortafuegos para protegerse de varias técnicas midiendo el tamaño de ventana en el paquete (WIN).
21. Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando todas las banderas activadas (XMAS).
22. Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando IPIDs.
23. Verificar la habilidad del cortafuegos para protegerse de varias técnicas usando protocolos encapsulados.
24. Cuantificar la robustez del cortafuegos y su susceptibilidad a los ataques de denegación de servicios con conexiones TCP ininterrumpidas.
25. Cuantificar la robustez del cortafuegos y su susceptibilidad a los ataques de denegación de servicios con conexiones TCP temporales.
26. Cuantificar la robustez del cortafuegos y su susceptibilidad a los ataques de denegación de servicios con datagramas UDP.
27. Cuantificar la respuesta del cortafuegos a todos los tipos de paquetes ICMP.

Revisión de Registros del Cortafuegos

28. Testear el proceso de registro del cortafuegos.
29. Verificar escaneos TCP y UDP en los registros del servidor.
30. Verficiar escaneos de vulnerabilidades automatizados.
31. Verificar deficiencias de registros de servicios.

12. Testeo de Sistema de Detección de Intrusos

Este test está enfocado al rendimiento y susceptibilidad de un IDS. La mayor parte de este test no puede ser llevada a cabo adecuadamente sin acceder a los registros del IDS. Algunos de estos tests estan relacionados con ataques de ancho de banda, saltos distantes, y latencia que afectan al resultado de estos tests.

Repasar los registros del servidor es necesario para verificar que los tests realizados en presencia en Internet, especialmente en los casos donde el resultado de éstos no es inmediatamente evidentes para el auditor. Algunos que son desconocidos son destinados para el analista, quien no ha revisado los registros y alertas.

Resultados Esperados:	Tipo de IDS Nota del rendimiento de los IDS bajo una sobrecarga Tipo de paquetes eliminados o no escaneados por el IDS Tipo de protocolos eliminados o no escaneados por el IDS Nota del tiempo de reacción y tipo del IDS Nota de la susceptibilidad del IDS Mapa de reglas del IDS Lista de falsos positivos del IDS Lista de alarmas perdidas del IDS Lista de rutas no monitorizadas en la red

El IDS y sus características

1. Verificar el tipo de IDS con información recogida de la Inteligencia

de Informacion 2. Determinar la esfera de protección o influencia.

3. Testear los estados de alarma del IDS.
4. Testear los parámetros de sensibilidad de las firmas pasado 1 minuto, 5 minutos, 60 minutos, y 24 horas.

Testeo de configuración IDS

5. Testear la configuración del IDS para reacciones múltiples, ataques variados (inundación).
6. Testear la configuración del IDS para reacciones como URLs manipuladas y rutinas de explotación.
7. Testear la configuración del IDS para reacciones ante cambios de velocidad al enviar paquetes.
8. Testear la configuración del IDS para reacciones ante cambios aleatorios de velocidad durante un ataque.
9. Testear la configuración del IDS para reacciones ante cambios aleatorios de protocolos durante un ataque.
10. Testear la configuración del IDS para reacciones ante cambios aleatorios de origen durante un ataque.
11. Testear la configuración del IDS para reacciones ante cambios de puerto de origen.
12. Testear en el IDS, la habilidad de manejar paquetes fragmentados.
13. Testear en el IDS, la habilidad de manejar metodos de ataques de sistemas específicos.
14. Testear los efectos y reacciones del IDS. Una dirección IP contra varias direcciones.

15. Encontrar alertas de IDS sobre escaneos de vulnerabilidades.
16. Encontrar alertas de IDS sobre descifrado de contraseñas.
17. Encontrar alertas de IDS de testeos de sistemas confiados.

13. Testeo de Medidas de Contingencia

Las medidas de contingencia dictan el manejo de lo atravesable, programas maliciosos y emergencias. La identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados. Debe ser necesario responder primero a una nueva cuenta de correo electrónico de pruebas o al sistema de escritorio donde el administrador pueda monitorizar.

Resultados Esperados:	Definición de las capacidades Anti-Troyano Definición de las capacidades Anti-Virus Identificación de las Medidas de Contingencia de Escritorio Identificación de las Debilidades de Contingencia de Escritorio Lista de recursos de contingencia

1. Medir el mínimo de recursos necesarios que senecesitan en el susbistema para realizar las tareas.
2. Verificar los recursos disponibles a este subsistema que necesiten realizar estas tareas, y que recursos estan protegidos desde este subsistema.
3. Verificar la detección de medidas presentes para la deteccion de intentos de acceso a los recursos protegidos.
4. Verificar recursos innecesarios.
5. Verificar las propiedades del sistema de contingencia.
6. Verificar la detección de medidas presentes para la detección de accesos 'no comunes' a los recursos 'necesarios'.
7. Medidas de respuestas y procesos contra el "sap 27" (ver página 132 de la lista)
8. Medidas de configuración del sistema.

14. Descifrado de Contraseñas

Descifrar las contraseñas es el proceso de validar la robustez de una contraseña a traves del uso de herramientas de recuperación de contraseñas automatizados, que dejan al descubierto la aplicación de algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas debiles debido a factores humanos. Este módulo no debe ser confundido con el de recuperación de contraseñas via escucha de de texto por canales libres, es más sencillo de entender que un transtorno del sistema de seguridad, pero solo que tiene mecanismos de autenticacion sin cifrar, nada de debilidades en contraseñas [Nota: Este módulo puede incluir técnicas para averiguar manualmente las contraseñas, que explote los usuarios y contraseñas por defecto en aplicaciones o sistemas operativos (p.ej. Usuario: System Contraseña: Test) o fácilmente predecible por parte del error de un usuario (p.ej. Usuario: joe Contraseña: joe). Este puede ser un sistema para obtener acceso a un sistema inicialmente, quizá sea siempre con acceso de administrador o root, pero solo con fines educativos. Más allá de la predictibilidad manual de las contraseñas, a través de combinaciones por defecto o simples, se puede hacer fuerza bruta de contraseñas para aplicaciones como Telnet, usando scripts o programas personalizados, almenos no es viable por valores de espera agotados, siempre con aplicaciones de fuerza bruta con multiconexión (simulando el multihilo).]

Una vez entrado con privilegios de root o administrador en un sistema, el descifrado de contraseñas consiste en obtener acceso a sistemas o aplicaciones adicionales (gracias a los usuarios cuyas contraseñas sean coincidentes en múltiples sistemas) y es una técnica válida que puede ser usada por influencia del sistema a traves de un test de seguridad. Descifrados de contraseñas minuciosos pueden ser realizados como un ejercicio de simple y debe ser subrayada la necesidad de algoritmos criptográficos fuertes para contraseñas de almacenamiento de sistemas de llave, tambien subrayar la necesidad del refuerzo de una política estricta de contraseñas de usuario, generación automática, o módulos del tipo PAM.

Resultados Esperados:	Ficheros de Contraseñas descifrados o no descifrados Lista de cuentas, con usuario o contraseña de sistema Lista de sistemas vulnerables a ataques de descifrado de contraseñas Lista de archivos o documentos vulerables a ataques de descifrado de contraseñas Lista de sistemas con usuario o cuenta de sistema que usan la s mismas contraseñas

1. Obtener el fichero de contraseñas desde el sistema que guarda nombres de usuario y contraseña
   - Para sistemas Unix, ha de estar en /etc/passwd o/y /etc/shadow.
   - Para sistemas Unix que tienen que realizar autenticaciones SMB, puede encontrar las contraseñas de NT en /etc/smbpasswd.

- Para sistemas NT, ha de estar en /winnt/repair/Sam._ (u otra, más dificil de obtener variantes)

2. Arranque un ataque automatizado de diccionario al fichero de contraseñas.
3. Arranque un ataque de fuerza burta al fichero de contraseñas.
4. Usar contraseñas obtenidas o sus variaciones para acceder a sistemas o aplicaciones adicionales.
5. Arranque Programas automatizados de descifrado en ficheros cifrados que haya encontrado (como documentos PDF o Word) como intento de recopilar más datos y subrayar la necesidad de un cifrado del sistema o de documentos más fuerte.
6. Verificar la edad de las contraseñas.

15. Testeo de Denegación de Servicios

La Denegación de Servicios (DoS) es una situación donde una circunstancia, sea intencionada o accidental, previene el sistema de tal funcionalidad como sea destinada. En ciertos casos, el sistema debe funcionar exactamente como se diseñó, nunca fue destinado para manejar la carga, alcance, o parámetros que abusen de ellos.

Es muy imporante que los tests de DoS reciban ayuda adicional de la organización y sea monitorizada a nivel privado. Inundación y ataques DoS Distribuidos (DDoS) estan especificamente no comprobados y prohibidos por este manual. Los ataques de inundación y los ataques DDoS SIEMPRE causarán ciertos problemas y a veces no solamente al objetivo sino también a los enrutadores y sistemas entre el auditor y el objetivo.

Resultados Esperados:	Lista de puntos débiles en presencia de Internet incluidos los puntos individuales por averías Establecer un punto de referencia para un uso normal Lista de comportamientos de sistema por un uso excesivo Lista de sistemas vulnerables a DoS

1. Verificar que las cuentas administrativas y los archivos y recursos del sistemas estan securizados aporpiadamente y todos los accesos estan concedidos con "Mínimo Privilegio".
2. Comprobar las restricciones de sistemas expuestas a redes sin confianza.
3. Verificar que los puntos de referencian estan establecidos a partir de un actividad normal del sistema.
4. Verificar que los procedimientos estan en un lugar que responde a una actividad irregular. 5. Verificar la respuesta a una información negativa SIMULADA (ataques propaganda)
6. Testear cargas de red y de servidor excesivas.

16. Evaluación de Políticas de Seguridad

La política de seguridad resaltada aquí es el documento escrito legible que contiene las políticas que delinean la reducción de riesgos en una organización con la utilización de tipos específicos de tecnologías. Esta política de seguridad puede ser también una forma legible de Listas de Controles de Acceso. Existen dos funciones a llevar a cabo: primero, el testeo de lo escrito contra el estado actual de las conexiones de la presencia en Internet y de otras conexiones no relacionadas a Internet; y segundo, asegurar que la política este incluida dentro de las justificaciones de negocio de la organización, y de los estatutos legales locales, federales e internacionales, en especial en referencia a los derechos y responsabilidades tanto del empleador como de los empleados y la ética de privacidad personal.

Esta tareas exigen que el testeo y verificación de vulnerabilidades sea hecho en su totalidad y que todas las otras revisiones técnicas hayan sido llevadas a cabo. A menos que esto sea realizado, no es posible comparar los resultados con los lineamientos a lograr especificados por las políticas de seguridad, traducidos en medidas de protección del entorno operativo.

1. Comparar la política de seguridad contra el estado actual de la presencia en Internet.
2. *Aprobación de la Gerencia* – Busque cualquier signo que revele que la política está aprobada por la gerencia. Sin esta aprobación, la política no tiene valor porque el personal no tiene la obligación de seguir las reglas establecidas en la política. Desde un punto de vista formal, UD puede detener las investigaciones de la política de seguridad si ésta no es aprobada por la gerencia. Sin embargo, el testeo debería continuar para determinar cuán efectivas son las medidas de seguridad en el estado actual de la presencia en Internet.
3. Cerciórese de que la documentación está adecuadamente almacenada, ya sea electrónicamente o en otros medios, y que la política ha sido leída y aceptada por el personal incluso antes de que ellos obtengan acceso a los sistemas informáticos.
4. Identifique los procedimientos de manejo de incidentes, para asegurarse de que las brechas de seguridad son manejadas por las personas adecuadas y que son reportadas de manera apropiada.
5. *Conexiones entrantes* – Verifique los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet (Internet -> DMZ, Internet -> red interna), y las medidas que son necesarias implementar para reducir o eliminar dichos riesgos. Estos riesgos pueden ser permitidos en conexiones entrantes, típicamente SMTP, POP3, HTTP, HTTPS, FTP, VPNs y las correspondientes medidas como esquemas de autenticación, encriptación y Listas de Control de Acceso. Específicamente, las reglas que niegan el acceso con estado a la red interna generalmente no son alcanzadas por la implementación.
6. *Conexiones salientes* – Las conexiones salientes pueden producirse entre la red interna y DMZ, así como también entre la red interna e Internet. Busque cualquier regla de conexiones salientes que no se corresponda con la implementación. Las conexiones salientes no pueden ser usadas para introducir código malicioso o revelar las especificaciones de la red interna.
7. *Medidas de seguridad* – Las reglas que exigen la implementación de medidas de seguridad, deben ser cumplidas. Aquellas pueden hacer uso de AVS, IDS, cortafuegos, DMZs, routers y las configuraciones/implementaciones adecuadas de acuerdo con los riesgos a contrarrestar.
8. Comprobar la política de seguridad contra el estado actual de las conexiones no relacionadas a Internet.
9. *Modems* – Debe existir una regla que indique que el uso de modems que no están especialmente asegurados está prohibido o al menos sólo permitido si los modems están desconectados cuando no se encuentran en uso, y configurados para no permitir el marcado. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.
10. *Máquinas de Fax* – Debe existir una regla que indique que el uso de las máquinas de fax que pudiera permitir acceso desde el exterior a la memoria de las máquinas, está prohibido o al menos sólo permitido si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.
11. *PBX* – Debe existir una regla que indique que la administración remota del sistema PBX está prohibida o al menos sólo permitida si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.
12. Verifique que la política de seguridad establezca las medidas de contención y los tests de ingeniería social basados en el uso indebido de Internet por parte de los empleados, de acuerdo con la justificación de negocios y las mejores prácticas de seguridad.

Sección D – Seguridad en las Comunicaciones

Valores de la Evaluación de Riesgo

Modulo	Ciclos (días)	Degradación (%)	Influencia (x)
Revisión de Configuración de Seguridad	No Disponible	No Disponible	No Disponible
Revisión de la PBX	No Disponible	No Disponible	No Disponible

Testeo del Correo de Voz	No Disponible	No Disponible	No Disponible
Testeo del FAX	No Disponible	No Disponible	No Disponible
Inspección de Modems	No Disponible	No Disponible	No Disponible
Testeo de Controles de Acceso Remoto	No Disponible	No Disponible	No Disponible
Testeo de Voz sobre IP	No Disponible	No Disponible	No Disponible
Testeo de Red de Paquetes Conmutados X.25	No Disponible	No Disponible	No Disponible

Módulos

1. Testeo de PBX

Este es un método para lograr acceso privilegiado a la central telefónica de la organización objetivo.

Resultados Esperados:	Lista de sistemas PBX que permitan ser administrados remotamente Lista de los sistemas que permitan acceso desde cualquier lugar del mundo a la terminal de mantenimiento. Lista de todos los sistemas telefónicos que estén en modo de escucha y de manera interactiva.

1. Revisar los detalles de llamadas en busca de indicios de abuso.
2. Asegurarse que las cuentas administrativas no tengan contraseñas por defecto, ni que las mismas puedan ser fácilmente adivinadas.
3. Verificar que el sistema operativo se encuentre actualizado y con los últimos parches aplicados.
4. Verificar el acceso remoto para el mantenimiento del sistema.
5. Testear la autenticación de las llamadas entrantes.
6. Verificar la autenticación remota de las llamadas entrantes.

2. Testeo del Correo de Voz

Este es un método para lograr acceso privilegiado a los sistemas de correo de voz de la organización objetivo y de su personal interno.

Resultados Esperados:	Lista de las casillas de correo de voz que son accesibles desde cualquier ubicación en el mundo. Lista de los códigos de llamadas entrantes a las casillas de correo de voz y sus correspondientes Números de Identificación Personal (PINs).

1. Verificar el tamaño del PIN y su frecuencia de cambio.
2. Identificar información de usuarios y de la organización.
3. Verificar el acceso remoto para el mantenimiento del sistema.
4. Testear la autenticación de las llamadas entrantes.
5. Verificar la autenticación remota de las llamadas entrantes.

3. Revisión del FAX

Este es un método para enumerar maquinas de FAX y lograr acceso privilegiado a los sistemas en los que estos quizás se encuentren.

Resultados Esperados:	Lista de los sistemas de FAX. Lista de los tipos de sistemas de FAX y sus posibles programas operativos. Recopilación de información alojada en la memoria de los sistemas de FAX. Mapa del manejo de protocolos de FAX dentro de la organización.

1. Asegurarse que las cuentas administrativas no tengan las contraseñas por defecto, ni que las mismas sean fácilmente adivinables.
2. Testear FAX poling.
3. Verificar el acceso remoto para el mantenimiento del sistema.
4. Testear la autenticación de las llamadas entrantes.
5. Verificar la autenticación remota de las llamadas entrantes.

4. Testeo del Modem

Este es un método para enumerar módems y lograr acceso privilegiado a los sistemas de modems habilitados en los sistemas de la organización objetivo.

Resultados Esperados:	Lista de los sistemas con módems que se encuentren a la escucha. Lista de los tipos modem y sus programas operativos. Lista de los esquemas de autenticación de los módems. Lista de usuarios y contraseñas de acceso vía modem Mapa del manejo de protocolos de modem dentro de la organización.

1. Escanear la central para módems.
2. Asegurarse que las cuentas no tengan las contraseñas por defecto, ni que las mismas sean fácilmente adivinables.
3. Asegurarse que el sistema operativo y las aplicaciones del modem estén actualizados y con los últimos parches aplicados.
4. Verificar el acceso remoto para el mantenimiento del sistema.
5. Testear la autenticación de las llamadas entrantes.
6. Verificar la autenticación remota de las llamadas entrantes.

Sección E – Seguridad Inalámbrica

Valores de la Evaluación de Riesgo

Módulo	Ciclo (días)	Degradación (%)	Influencia (x)
Revisión de Postura			

Verificación de Radiación Electromagnética (EMR)	Debería ser realizada en nuevas instalaciones o cada vez que se añada un nuevo dispositivo a una configuración segura existente.		
Verificación de Redes Inalámbricas 802.11	28 días	1.3%	
Verificación de Redes Bluetooth	28 días	1.3%	
Verificación de Dispositivos de Entrada Inalámbricos	60 días	2.8%	
Verificación de Dispositivos de Mano Inalámbricos	60 días	2.8%	
Verificación de Comunicaciones sin Cables	60 días	2.8%	
Verificación de Dispositivos de Vigilancia Inalámbricos	Debería ser realizada en nuevas instalaciones o cada vez que se añada un nuevo dispositivo a una configuración segura existente.		
Verificación de Dispositivos de Transacción Inalámbricos	Debería ser realizada en nuevas instalaciones o cada vez que se añada un nuevo dispositivo a una configuración segura existente.		
Verificación de RFID	365 días		
Verificación de Infrarrojos	120 días	.6%	
Revisión de Privacidad	70 días	2.1%	

Módulos

1. Verificación de Radiación Electromagnética (EMR)

Este es un método para verificar la Seguridad de las Emisiones (Emsec) perteneciente a la verificación remota de radiaciones electromagnéticas emitidas por dispositivos de las Tecnologías de la Información. Se puede capturar la radiación electromagnética de los dispositivos tales como CRTs, LCDs, impresoras, módems, teléfonos móviles, entre otros y utilizarse para reconstruir los datos mostrados en la pantalla, impresos, transmitidos…El abuso de esta vulnerabilidad es conocido como 'Van Eck phreaking'.

El equipamiento para verificar o abusar esta vulnerabilidad puede ser prohibitivamente caro. Sin embargo existen algunas soluciones de bajo coste utilizando receptores de televisión, sintonizadores VCR, equipos de sincronización, y otras piezas. Encontrar la fuente correcta de una

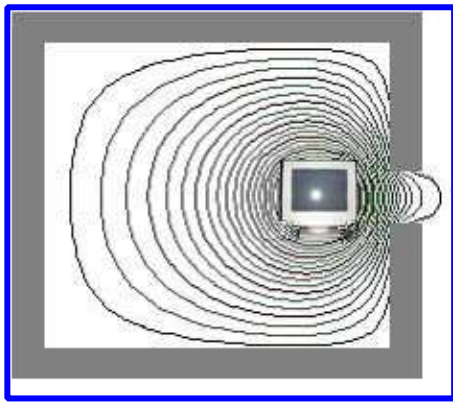
EMR puede requerir una persona cualificada sentada durante horas. Por esta razón este tipo de verificación se reserva a instalaciones de alta seguridad donde la protección de la propiedad intelectual es absolutamente vital. Además, debido a que estos datos puede ser obtenidos desde cualquier dispositivo con capacidad de emitir EMR, es mejor verificarlo en implementaciones diseñadas específicamente para protegerse contra ellas.

Protegerse ante este tipo de intrusiones se realiza habitualmente comprando equipamiento de tipo “Tempest” y colocando todas las maquinas y periféricos dentro de algún tipo de sala blindada, como por ejemplo una Jaula de Faraday y utilizando únicamente fibra o conexiones filtradas o alámbricas hacia y entre todos los dispositivos internos y desde el exterior. Por dicha razón este tipo de protección puede ser prohibitivamente cara.

Para protecciones de bajo coste ante este tipo de intrusiones, ‘PGP Security’ tiene una opción preventiva de supervisión “Tempest” en su ‘secure viewer’ (utilizado en la visualización de ficheros de texto cifrados). Consiste en una pantalla de bajo contraste donde se visualiza el texto. Esto probablemente ofusque el texto en el caso de espionaje desde una furgoneta. También se puede generar ‘ruido blanco’ para hacer mucho más difícil a un intruso la obtención de datos nítidos.

* Nota – Es un mito bastante extendido el hecho de que los CRTs son los grandes culpables de la filtración de información mediante EMR. Esto no es cierto. Emiten una cantidad significativa de EMR pero aunque es potente no es tan legible como las emitidas por módems e impresoras. Más aún, para la obtención de datos desde CRTs una persona altamente cualificada necesitaría filtrar, reconstruir y organizar los datos cuando en módems e impresoras simplemente hay que interceptarlas.

Resultados Esperados:	



Evaluar las Necesidades de Negocio, Prácticas, Políticas y Ubicaciones de las Áreas Sensibles

1. Verificar que la organización disponga de una política de seguridad en uso que trate las EMR.

Evaluar el Equipamiento y Ubicación

2. Verificar que todos los dispositivos de las Tecnologías de la Información que deben ser protegidos están ubicados apropiadamente en una Jaula de Faraday o habituación blindada de metal.

Evaluar y Verificar el Cableado y Emisiones

3. Verificar que todo el cableado de entradas o salida la sala blindada, donde sea posible, sean de fibra

2. Verificación de Redes Inalámbricas [802.11]

Este es un método para la verificación del acceso a redes WLAN 802.11, las cuales se están popularizando cada vez más. Sin embargo existen algunos problemas bastante comunes y alarmantes en la implantación de estas tecnologías. Se debe principalmente a que estas redes se crean rápida y fácilmente pero las medidas de seguridad no forman parte de la configuración por defecto. Existen algunas medidas básicas para mejorar la seguridad y algunas más drásticas a aplicar para conseguir unas WLANs bastante seguras.

Especificaciones 802.11:

Capa Física	Secuencia Directa en Espectro Ensanchado (DSSS), Saltos de Frecuencia en Espectro Ensanchado (FHSS), infrarrojos (IR)
Cifrado por defecto	Algoritmo de cifrado basado en flujo RC4 para confidencialidad, autenticación, y integridad. Gestión de Claves limitada.
Rango de Operación	Unos 150 pies en interiores y 1500 en exterior.

Implementaciones:

802.11a

- Opera en el rango de frecuencias de 5Ghz
- Incompatibilidad con equipamiento 802.11b o 802.11g
- Máxima velocidad de 54MBps

802.11b

- Opera en el rango de frecuencias de 2.4Ghz
- Es la tecnología más extendida actualmente
- Máxima velocidad de 11Mbps

802.11g

- Opera en el rango de frecuencias de 2.4Ghz
- Máxima velocidad estándar de 54MBps
- Se espera compatibilidad con equipamiento 802.11b existente

Resultados Esperados:	

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

1. Verificar que la organización disponga de una adecuada política de seguridad en uso que trate la utilización de tecnologías inalámbricas, incluyendo el uso de 802.11

Evaluar Equipamiento, Firmware y Actualizaciones.

6. Realizar un inventario completo de todos los dispositivos inalámbricos de la red.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

7. Determinar el nivel de control de acceso físico a los puntos de acceso y dispositivos que los controlan (cerrojos, lectores de tarjetas, cámaras...).

Evaluar el Acceso Administrativo a los Dispositivos Inalámbricos:

8. Determinar si los puntos de acceso son apagados durantes los momentos del día en los que no son utilizados.

Evaluar la Configuración, Autenticación y Cifrado de las Redes Inalámbricas:

9. Verificar el cambio de los 'Service Set Identifier' (SSID) por defecto de los puntos de acceso.

Evaluar los Clientes Inalámbricos:

10. Verificar que todos los clientes inalámbricos poseen un antivirus instalado.

3. Verificación de Redes Bluetooth

Este es un método para la verificación de redes Bluetooth de tipo ad-hoc (piconets), las cuales son populares en las redes inalámbricas de área personal (PANs) pequeñas y de poco ancho de banda. De igual modo que con otras estrategias inalámbricas, existen vulnerabilidades inherentes que plantean problemas de seguridad significativos.

Especificaciones Bluetooth:

Capa Física	Frequency Hopping Spread Spectrum (FHSS)
Banda de Frecuencia	2.4 – 2.45 GHz (ISM band)
Salto de Frecuencia	1,600 hops per second
Tasa Bruta de Transmisión	1Mbps
Ancho de Banda	Hasta 720 Kbps
Seguridad de Datos y Red	• Tres modalidades de seguridad (ninguna, a nivel de enlace y a nivel de servicio) • Dos niveles de confianza de dispositivo y 3 niveles de seguridad del servicio. • Algoritmo de cifrado de flujo para confidencialidad y autenticación. • Claves derivadas del PIN y gestión de claves limitada
Rango de Operación	Sobre 10 metros (30 pies); puede ser ampliado a 100 metros (328 pies).

Resultados Esperados:	

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

1. Verificar que existen políticas de seguridad organizativas que traten el uso de la tecnología inalámbrica, incluyendo la tecnología Bluetooth.

Evaluar Equipamiento, Firmware y Actualizaciones.

2. Realizar un inventario completo de todos los dispositivos inalámbricos de tipo Bluetooth.

Pruebas de Vulnerabilidades Comunes (especialmente en el Red-M 105AP):

3. Realizar ataques de fuerza bruta contra puntos de acceso Bluetooth para comprobar la fortaleza de la contraseña. Verificar que las contraseñas contengan números y caracteres especiales. Los Puntos de Acceso Bluetooth utilizan contraseñas sin diferenciación de

mayúsculas lo que facilita a los atacantes la realización de ataques de fuerza bruta al haber un espacio más pequeño de posibles contraseñas por adivinar.

Evaluar el Control de Acceso, la Seguridad Perimetral y la Habilidad para Interceptar o Interferir las Comunicaciones:

4. Verificar el perímetro actual de la red Bluetooth.

Evaluar la Configuración de Dispositivo (Autenticación, Contraseñas, Cifrado...):

5. Verificar que los dispositivos Bluetooth son configurados con los niveles más bajos de potencia para operar suficientemente y mantener las transmisiones dentro de los límites seguros de la organización.

4. Verificación de Dispositivos de Entrada Inalámbricos

Esta sección trata de los dispositivos de entrada inalámbricos tales como ratones y teclados. Estos dispositivos se están popularizando aunque presentan profundas vulnerabilidades y compromisos en privacidad y seguridad.

Resultados Esperados:	

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

1. Analizar la política de seguridad organizativa que trata el uso de tecnologías inalámbricas tales como la de los dispositivos de entrada inalámbricos.

Evaluar Equipamiento, Firmware y Actualizaciones:

2. Realizar un inventario completo de todos los dispositivos de entrada inalámbricos en la red.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

3. Realizar una inspección del lugar para medir y establecer el alcance de los dispositivos de entrada inalámbricos para la organización.

5. Verificación de Dispositivos de Mano Inalámbricos

Debido a la increíble variedad y ubicuidad de los dispositivos de mano inalámbricos es prácticamente imposible tratar cada tipo. Esta sección pretende incorporarlos de forma agregada. Existen medidas básicas que se deberían tomar y verificar en todos ellos. Los siguientes pasos proporcionan un método de verificación de seguridad en todos los dispositivos.

El aspecto más significativo para verificar estos dispositivos no reside en su configuración sino en la educación del usuario. La mayoría de estos pasos comprueba los conocimientos del usuario respecto al uso más seguro del dispositivo.

Resultados esperados:	

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

1. Verificar que existe una política de seguridad organizativa que trata el uso de los dispositivos de mano.

Evaluar Equipamiento, Firmware y Actualizaciones:

2. Realizar un inventario completo de todos los dispositivos inalámbricos de la red.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

3. Verificar que existe una protección de los limites externos alrededor del perímetro de los edificios o de las redes inalámbricas.

Evaluar la Configuración del Dispositivo (Autenticación, Contraseñas, Cifrado...):

4. Verificar que los dispositivos utilizan cifrado fuerte para proteger los ficheros sensibles y las aplicaciones.

6. Verificación de Comunicaciones sin Cable

Este es un método para la verificación de dispositivos de comunicación sin cables que puedan sobrepasar los límites físicos y monitorizados de una organización. Esto incluye la verificación de interferencia entre tipos diferentes o similares de comunicación dentro de una organización y sus organizaciones vecinas.

Resultados Esperados:	

Evaluar las Necesidades de Negocio, Prácticas y Políticas

1. Verificar que la organización disponga de una política de seguridad que trate el uso de tecnologías de comunicación sin cables.

Evaluar Equipamiento, Firmware y Configuración:

2. Realizar un inventario de todos los dispositivos de comunicación sin cables.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

3. Verificar la distancia en la que las comunicaciones sin cables sobrepasa el límite físico de la organización.

7. Verificación de Dispositivos de Vigilancia Inalámbricos

Esta sección pertenece a los dispositivos de vigilancia inalámbricos que han empezado recientemente a reemplazar los alámbricos – tales como cámaras, micrófonos, etc. Estos dispositivos permiten a las compañías instalar equipamiento de monitorización en áreas en las que no era anteriormente factible y a un bajo coste. Estos equipos de monitorización están a menudo completamente escondidos sean por su pequeño tamaño o bien siendo camuflados por otros objetos tales como alarmas de incendio, cuadros o relojes. Debido a que gran parte de estos equipos son inalámbricos son más susceptibles a interferencia triviales, intencionadas, monitorización y reproducción que las equivalentes alámbricas. El verificador de la seguridad debe ser también la última línea de defensa para asegurar que el equipamiento esta instalado y funcionando apropiadamente.

Resultados Esperados:	

Evaluación de Necesidades de Negocio, Prácticas y Políticas:

1. Verificar que existe una política de compañía que trate efectivamente el equipamiento de vigilancia inalámbrico.

Evaluación de Dispositivos y Ubicación:

2. Verificar que los equipos de vigilancia están realmente camuflados o no visibles, si es una de las cosas que pretende el equipamiento.

Evaluación del Control de Acceso, Seguridad Perimetral y Habilidad de Interceptar y Interferir las Comunicaciones:

3. Verificar el perímetro actual de la transmisión del dispositivo de vigilancia inalámbrico.

8. Verificación de Dispositivos de Transacción Inalámbricos

Esta sección cubre los dispositivos de transacción inalámbricos instalados en numerosas tiendas. Este equipamiento se esta utilizando para proporcionar conexión con cajas registradoras y otros dispositivos de punto de venta a lo largo de los comercios. Esta tecnología ha demostrado un tremendo beneficio de negocio para las compañías aunque algunas veces se instalan sin tener en cuenta la seguridad y protección de la información confidencial.

Resultados Esperados:	

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

1. Verificar que existe una política corporativa que trate efectivamente el equipamiento de transacción inalámbrico.

Evaluar Equipamiento, Firmware y Actualizaciones:

2. Realizar un inventario completo de todos los dispositivos de transacción inalámbricos.

Evaluar la Configuración de Dispositivo:

3. Verificar que los datos enviados sean cifrados y el nivel utilizado.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir con las Comunicaciones:

4. Determinar la habilidad de un tercero no intencionado de interceptar los datos transmitidos.

9. Verficación de RFID

Las etiquetas de RFID (Radio Frequency Identifier) se componen de un circuito integrado (IC), a menudo del tamaño de medio grano de arena, y una antena – habitualmente una espiral de cables. La información está almacenada en el IC y se transmite mediante la antena. Las etiquetas RFID pueden ser pasivas (sin batería utilizando la transmisión de energía del lector de etiquetas RF) o activa (autoalimentadas por batería). La velocidad y alcance de la transmisión de datos depende de la potencia de salida, tamaño de la antena, sensibilidad del receptor, frecuencia y interferencia. Las etiquetas RFID pueden ser de solo lectura, de lectura y escritura, o una combinación de ambas donde una parte es de solo lectura (tal como el número de serie) y el resto modificable para la posterior codificación o actualización.

Además las etiquetas RFID no requieren línea directa de visión para ser leídas y pueden trabajar bajo diversas condiciones ambientales – algunas son resistentes al agua y lavables. Cada etiqueta contiene un identificador único de 64 bits y una cantidad variable de memoria – gran parte de ellas 1024 bits. Por esta razón pueden proporcionar un alto nivel de funcionalidad e integridad de datos.

Algunas de ellas proporcionan medidas de seguridad. Gran parte de las que utilizan cifrado tienen una clave secreta escondida de 40 bits. Algunos transponedores integran firma digital y protocolo de cifrado que incluye una autenticación de desafío/respuesta. Dependiendo del diseño de la etiqueta RFID y del transpondedor, la autenticación puede ser de una o dos caras.

Las frecuencias exactas utilizadas en sistemas RFID pueden por ello variar en cada país o región, sin embargo los sistemas RFID utilizan típicamente los siguientes rangos de frecuencia:

- Baja frecuencia: rango de frecuencias de 30 a 300 kHz, sobretodo en la banda de 125 kHz;
- Alta frecuencia: rango de frecuencias de 13.56 MHz;
- Frecuencia Ultra-Alta (UHF): rango de frecuencias de 300 MHz a 1 GHz; y
- Frecuencia Microondas: rango de frecuencias superior a 1 GHz, sobretodo las bandas de 2.45 GHz y
  5.8 GHz

Las etiquetas RFID son totalmente esenciales en logística aunque temidas y cuestionadas por los defensores de la privacidad debido a la calidad y cantidad de información que proporcionan. Por esta razón, se deben tomar algunos pasos para asegurar que la logística no incapacita mientras que las restricciones de seguridad no se pisotean.

Existen una legislación inminente que podría afectar a las compañías que las utilizan y es mejor ser proactivo y realizar una aproximación con visión de futuro de las mejores prácticas. Para ello hay que verificar la lectura de las etiquetas de RFID en todos los pasos del recorrido logístico y su desactivación en el destino (tales como el punto de venta) y que no puedan ser reactivadas de manera alguna. Esta desactivación ayuda a proteger ante futuras legislación así como de intenciones maliciosas.

Sin embargo también se necesita asegurar que las etiquetas RFID no pueden ser desactivadas por aquellos que intentan robar los artículos. Por esta razón la desactivación de la etiqueta de RFID solo debería poder ser realizada en la caja registradora y cualquier otro lugar especifico requerido por el negocio.

Resultados Esperados:	

Evaluación de Necesidades de Negocio, Prácticas y Políticas:

1. Verificar que la organización tiene una política de seguridad que trata adecuadamente el uso de RFIDs inalámbricas.

Evaluar los Atributos RFID (Autenticación, Cifrado, Propiedades…):

2. Verificar que el número de serie en la etiqueta ID no puede ser cambiado.

Evaluar la Ubicación, Scanners y Equipamiento de Seguimiento:

3. Para un seguimiento completo de los productos etiquetados en un almacén o en un medio de almacenamiento, hay que asegurar la ubicación de lectores de etiquetas en todas las entradas y salidas, no solo en las zonas de llegada y salida de cargas. Esto ayudará a reducir el robo causado por empleados.

Evaluar el Control de Accesos, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

4. Verificar que las etiquetas RFID y los transmisiones con los lectores no interfieren las redes inalámbricas y los equipos de comunicaciones.

10. Verificación de Sistemas Infrarrojos

Este es el método de verificación de dispositivos de comunicaciones infrarrojas que pudieran sobrepasar los limites físicos y monitorizados de la organización.

Las comunicaciones infrarrojas son mucho menos accesibles desde el exterior de la organización en comparación con 802.11 y Bluetooth. Sin embargo la seguridad en los dispositivos infrarrojos suele descuidarse debido a su relativa inaccesibilidad.

Resultados Esperados:	

Evaluar las Necesidades de Negocio, Prácticas, Políticas y Ubicaciones de las Áreas Sensibles:

1. Verificar que la organización dispone de una política de seguridad que trata el uso de las tecnologías inalámbricas tales como dispositivos infrarrojos.

Evaluar Equipamiento, Firmware y Actualizaciones:

2. Realizar una auditoria completa de todos los dispositivos con capacidad infrarroja.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir con las Comunicaciones:

3. Verificar la distancia sobrepasada en las comunicaciones infrarrojas más alla de los límites físicos de la organización.

Evaluar la Configuración de Dispositivo (Autenticación, Contraseñas, Cifrado..):

4. Verificar el método de autenticación de los clientes.

11. Revisión de Privacidad

La privacidad de los dispositivos de comunicación inalámbricos pueden sobrepasar los limites físicos y monitorizados de una organización. La revisión de la privacidad es el punto central, desde un punto de vista legal y ético, del almacenamiento, transmisión y control de los datos en base a la privacidad de empleados y clientes. El uso de estos datos es una inquietud para bastantes particulares y la legislación está mostrando reglas especificas respecto a la privacidad. Aunque algunas de estas leyes son locales, todas aplican a la Internet y por tanto afectan internacionalmente a todos los auditores de seguridad.

Resultados Esperados:	Enumerar cualquier revelación Enumerar las anomalías en el cumplimiento entre la política pública y la práctica actual Enumerar las comunicaciones inalámbricas involucradas en la obtención de datos Enumerar las técnicas de obtención de datos Enumerar los datos obtenidos

1. Verificar el método de autenticación de los clientes
2. Verificar si están en uso de forma apropiada contraseñas robustas
3. Verificar que existe una política de expiración de contraseñas
4. Verificar si el cifrado está en uso y correctamente configurado
5. Verificar que los clientes no pueden ser forzados a volver al modo sin cifrado
6. Comparar la política públicamente accesible a la práctica actual
7. Compara la práctica actual a las leyes u obediencias regionales de fraude y privacidad
8. Identificar el tipo y tamaño de la base de datos para almacenar información
9. Identificar la información recogida por la organización
10. Identificar la ubicación de la información almacenada
11. Identificar los momentos de expiración de la información

Sección F – Seguridad Física

Valores de la Evaluación de Riesgo

Módulo	Ciclo (días)	Degradación (%)	Influencia (x)
Revisión de Configuración de Seguridad	No disponible	No disponible	No disponible
Testeo de Controles de Acceso	No disponible	No disponible	No disponible
Revisión de Perímetro	No disponible	No disponible	No disponible
Revisión de Monitoreo	No disponible	No disponible	No disponible

Revisión de Respuesta de Alarmas	No disponible	No disponible	No disponible
Revisión de Ubicación	No disponible	No disponible	No disponible
Revisión de Entorno	No disponible	No disponible	No disponible

Módulos

1. Revisión de Perímetro

Este es un método para evaluar la seguridad física de una organización y sus bienes, verificando las medidas de seguridad de su perímetro físico.

Resultados Esperados:	Mapa del perímetro físico Tipos de medidas de protección física Lista de áreas desprotegidas o insuficientemente protegidas

1. Trazar mapa del perímetro físico
2. Trazar mapa de las medidas de protección físicas (cercas, puertas, luces, etc.)
3. Trazar mapa de las rutas de acceso y/o métodos físicos
4. Trazar mapa de las áreas no monitoreadas

2. Revisión de monitoreo

Este es un método para descubrir puntos de acceso monitoreados, a una organización y sus bienes, por medio del descubrimiento de custodia y monitoreo electrónico.

Resultados Esperados:	Lista de puntos de acceso monitoreados Tipos de monitoreo Lista de puntos de acceso estándar y privilegiados, no monitoreados Lista de disparadores de alarmas

1. Enumerar los dispositivos de monitoreo
2. Trazar mapa de sitios protegidos y rutas recorridas
3. Trazar mapa de áreas monitoreadas y no monitoreadas
4. Examinar los dispositivos de monitoreo en búsqueda de limitaciones y vulnerabilidades
5. Examinar posibles ataques de denegación de servicio sobre los dispositivos de monitoreo

3. Evaluación de Controles de Acceso

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos.

Resultados Esperados:	Lista de puntos de acceso físicos Tipos de autenticación Tipos de sistemas de alarmas Lista de disparadores de alarmas

1. Enumerar áreas de control de acceso
2. Examinar dispositivos y tipos de control de acceso
3. Examinar tipos de alarmas
4. Determinar el nivel de complejidad en un dispositivo de control de acceso
5. Determinar el nivel de privacidad en un dispositivo de control de acceso
6. Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades
7. Examinar posibles ataques de denegación de servicio sobre los dispositivos de control de acceso

4. Revisión de Respuesta de Alarmas

Este es un método para descubrir procedimientos y equipos de alarmas en una organización por medio del descubrimiento de custodia y monitoreo electrónico.

Resultados Esperados:	Lista de tipos de alarmas Lista de disparadores de alarmas Mapa de procedimiento en caso de alarma Lista de personas involucradas en el procedimiento en caso de alarma Lista de medidas de contención y precauciones de seguridad activadas por alarmas

1. Enumerar los dispositivos de alarmas
2. Trazar mapa de procedimientos de detonación de alarmas
3. Trazar mapa de precauciones de seguridad activados por alarmas
4. Descubrir las personas involucradas en un procedimiento de alarma
5. Evaluar el incremento de alarma
6. Examinar la activación y desactivación de alarmas
7. Examinar los dispositivos de alarmas en búsqueda de limitaciones y puntos débiles
8. Examinar posibles ataques de denegación de servicio sobre los dispositivos de alarma
9. Examinar posibles ataques de denegación de servicio sobre los procedimientos de alarma

5. Revisión de Ubicación

Este es un método para obtener acceso a una organización o a sus bienes, a través de puntos débiles en su ubicación y en su protección contra elementos externos.

Resultados Esperados:	Mapa de ubicación física de los bienes Lista de ubicación física de los puntos de acceso Lista de puntos de acceso vulnerables en la ubicación Lista de la ubicación de los accesos de terceras partes

1. Enumerar las áreas de la organización que son visibles (Línea de visión)
2. Enumerar las áreas dentro de la organización que son audibles (Escuchas electrónicas, con láser y otros dispositivos)
3. Examinar las áreas de la ubicación referentes a las entradas por abastecimiento en búsqueda de puntos débiles y vulnerabilidades
4. Listar las empresas y empleados de abastecimiento
5. Listar las empresas y empleados de limpieza
6. Listar días y horarios de los ciclos de entregas
7. Listar días y horarios de los ciclos de visitantes

6. Revisión de Entorno

Este es un método para ganar acceso o dañar a una organización o sus bienes, a través de puntos débiles en su entorno.

Resultados Esperados:	Mapa físico de bienes en cada ubicación Lista de ubicaciones vulnerables Lista de leyes, costumbres, y ética locales Lista de leyes, costumbres, y ética operativas

1. Examinar las condiciones de la región respecto de los desastres naturales
2. Examinar las condiciones del entorno político
3. Examinar los procedimientos de resguardo y recuperación
4. Identificar puntos débiles y vulnerabilidades en los procedimientos de resguardo y recuperación
5. Identificar posibles ataques de denegación de servicio en los procedimientos de resguardo y recuperación
6. Examinar impedimentos físicos y electrónicos frente a distintas condiciones climáticas
7. Comparar procedimientos operacionales con las leyes, costumbres y ética regional

Requisitos de las Plantillas de Informes

Las siguientes plantillas son un breve ejemplo de los requisitos de los informes, indicando la información que se debe mostrar en un informe como condición necesaria para calificar y ser certificado en conformidad con el OSSTMM. Sobre éstas plantillas se aplican restricciones de ámbito y alcance pertinentes.

Plantilla de Perfil de Red

Rangos de IP que serán testeados y detalle de dichos rangos

Información de los dominios y su configuración

Información destacada de la transferencia de zonas

LISTA DE SERVIDORES

Dirección IP	Nombre(s) de dominio	Sistema operativo

Plantilla de Datos del Servidor

Dirección IP	Nombre de dominio

Puerto	Protocolo	Servicio	Detalles del servicio

MENSAJES DE BIENVENIDA:

Puerto	Protocolo	Mensaje de bienvenida

SECUENCIAS TCP:

Predicción de secuencia TCP:
Números de secuencia ISN TCP:
Generación de secuencias IPID:
Tiempo operacional

PREOCUPACIONES Y VULNERABILIDADES:

Preocupación o Vulnerabilidad
Ejemplo
Solución

Plantilla de Análisis del Cortafuegos

identificación

Este test permite determinar el exito de las respuestas a los paquetes con metodos de identificacion a traves del cortafuegos.

Método	Resultado

sigilo

Este test determina la viabilidad de realizar un escaneo SYN sigiloso a través del cortafuegos y obtener una enumeración de servicios.

Resultado

control de puerto origen

Este test mide el uso de escaneo de puertos usando puertos de origen especificos a traves del cortafuegos para enumerar los servicios.

Protocolo	Origen	Resultado
UDP	53	
UDP	161	
TCP	53	
TCP	69	

superposicion de paquetes

Este test determina la capacidad del cortafuegos para manipular fragmentos de paquetes como los usados en un ataque TEARDROP

Protocolo	Resultado

fragmentos de paquetes

Este test determina la habilidad del cortafuegos para manipular pequeños paquetes fragmentados.

IP	Resultado

inundación Syn

Este test mide la capacidad del cortafuegos de gestionar un flujo constante de paquetes SYN entrantes.

IP	Resultado

bandera rst

Este test exige respuesta del cortafuegos a paquetes enviados con la opción RST activada

IP	Resultado

UDP

Este test mide la capacidad de gestión de paquetes UDP estándar.

IP	Resultado

ack

Este test descubre la capacidad del cortafuegos para bloquear técnicas de enumeración que utilizan paquetes ACK.

IP	Resultado

fin

Este test descubre la capacidad del cortafuegos para bloquear técnicas de enumeración que utilizan paquetes FIN.

IP	Resultado

null

Este test descubre la capacidad del cortafuegos para bloquear técnicas de enumeración que utilizan paquetes NULL.

IP	Resultado

win

Este test descubre la capacidad del cortafuegos para bloquear técnicas de enumeración que utilizan paquetes WIN.

IP	Resultado

xmas

Este test descubre la capacidad del cortafuegos para bloquear técnicas de enumeración que utilizan paquetes que tienen todas las opciones del protocolo habilitadas.

IP	Resultado

Plantilla de Testeo Avanzado del Cortafuegos

Conexiones TCP sostenidas

Este test mide la robustez del cortafuegos y su sensibilidad a ataques de denegación de servicio. (DoS attacks)

Conexión	Descripción	Número máximo de conexiones	Tiempo máximo de inactividad

Conexiones TCP de corta duración

Este test mide la robustez del cortafuegos y su sensibilidad a ataques de denegación de servicio. (DoS attacks)

Conexión	Descripción	Número máximo de conexiones	Tiempo máximo de inactividad

Rendimiento de flujo UDP

Este test mide la robustez del cortafuegos y su sensibilidad a ataques de denegación de servicio. (DoS attacks)

Conexión	Descripción	Número máximo de conexiones

Respuestas ICMP

Este test mide la respuesta del cortafuegos a distintos tipos de paquetes ICMP.

Tipo	Descripción del tipo de paquete	Respuesta	RTT

Respuestas a falsificación (spoof)

Este test mide la Lista de Control de Accesos del cortafuegos por direccion IP.

Conexión	Descripción de la respuesta	De	a

Protocolo

Este test descubre la capacidad del cortafuegos de filtrar puertos de diversos protocolos.

Protocolo	Resultado

Plantilla de Testeo de Sistemas de Detección de Intrusiones (IDS)

Tipo de IDS

Este test determina el tipo de IDS y su alcance de proteccion o influencia.

Tipo de IDS	Rango de direcciones IP protegidas

Ataque de inundación

Este test mide las capacidades de respuesta del IDS cuando ocurren eventos de varios ataques de diversas prioridades entrando en simultáneo.

Tipo de inundación	Descripción del ataque	Duración	Resultado

URL enmascaradas

Este test apunta a la habilidad del IDS para detectar las URLs enmascaradas de los servidores web atacantes.

Tipo de codificación	URL enviada	Resultado

Ajustes de velocidad

Este test mide la sensibilidad del IDS a escaneos con diferente duracion de tiempo.

	Descipción de paquetes	Retardo	Resultado
1 minuto			
5 minutos			
60 minutos			
24 horas			

Ataques de comportamiento

Este test mide la sensibilidad del IDS a los escaneos de tipo aleatorio.

	Descripción	Resultado
Ataque de velocidad aleatoria		
Ataque con protocolos aleatorios		
Ataque con fuentes aleatorias		

Comprobación de método

Este test mide la sensibilidad del IDS a escaneos de servidores web que utilizan métodos desconocidos.

	Resultado
HEAD	
POST	
PUT	
DELETE	
PATCH	
PROPFIND	
PROPPATCH	
MKCOL	
COPY	
MOVE	
LOCK	
UNLOCK	

control de puerto origen

Este test mide el uso de escaneo de puertos usando puertos de origen especificos a traves del IDS y sin alarma.

Protocolo	Origen	Resultado
UDP	53	
UDP	161	
TCP	443	
TCP	22	

Respuestas falseadas

Este test mide las reglas de las Listas de Control de Acceso del IDS por direcciones IP.

Conexión	Descripción de la respuestas	De	A

Fragmentos

Este test mide la habilidad del IDS para manipular pequeños paquetes fragmentados.

Resultado

Plantilla de Ingeniería Social sobre el Objetivo

Definición del Objetivo

Nombre	Correo electrónico	Teléfono	Descripción

Plantilla de Ataque Telefónico usando Técnicas de Ingeniería Social

Escenario de ataque	
Número de teléfono:	
Persona	
Descripción	
Resultados	

Escenario de ataque	
Número de teléfono:	
Persona	
Descripción	
Resultados	

Plantilla de Ataque por Correo Electrónico usando Técnicas de Ingeniería Social

Escenario de ataque	
Correo electrónico:	
Persona	
Descripción	
Resultados	

Escenario de ataque	
Correo electrónico:	
Persona	
Descripción	
Resultados	

Plantilla de Análisis de Confianza

Dirección IP	Nombre de dominio
Descripción de confianza	

Dirección IP	Nombre de dominio
Descripción de confianza	

Dirección IP	Nombre de dominio
Descripción de confianza	

Plantilla de Revisión de Políticas de Privacidad

Dirección IP	Nombre de dominio
Política de privacidad	
Violaciones de la política de privacidad:	

Dirección IP	Nombre de dominio
Política de privacidad	
Violaciones de la política de privacidad:	

Plantilla de Revisión de Medidas de Contención

Dirección IP	Nombre de dominio
Mecanismos de anti-virus / anti-trojanos de servidor	
Respuesta del servidor a “SAP 27” y 42.zip	

Mecanismos de anti-virus / anti-trojano de cliente

Tipos de clientes de correo
Vulnerabilidades de clientes de correo

Tipos de navegadores de web del cliente

Vulnerabilidades de los navegadores de web del cliente

Plantilla de Correo Electrónico falseado

Intentos Conexiones internas

Muestra el resultado de un conexión vía telnet al servidor de correo y el envío de correo desde una dirección interna a otra dirección interna

Saliente

Muestra los resultados de enviar correo desde una dirección interna a otra dirección interna utilizando un servidor POP externo, de terceros.

Reenvío externo de correo

Muestra los resultados de enviar correo desde una dirección de correo externa a otra dirección de correo externa utilizando el servidor de correo objetivo.

Reenvío interno de correo

Muestra los resultados de enviar correo desde una dirección de correo interna a otra externa utilizando el servidor de correo objetivo.

Plantilla de Informacion Competitiva

Dirección IP	
Nombres de dominio	
Nombres de dominio similares	
Tamaño total de contenido	
Número de documentos	
Número de productos	
Lista de productos	
Número de servicios	
Lista de servicios	
Métodos de venta	
Areas restringidas	

Plantilla de Ataques a Contraseñas

Archivo protegido

Nombre de archivo	
Tipo de archivo	
Tiempo de duración del ataque	
Nombre de usuario	
Contraseña	

Archivo de contraseñas codificado

Dirección IP	
Puerto de servicio	
Tipo de servicio	
Protocolo	
Nombre de fichero	
Tipo de fichero	
Tiempo de ataque	
Nombres de usuarios	
Contraseñas	

Servicio en línea protegido

Dirección IP	
Puerto de servicio	
Tipo de servicio	
Protocolo	
Nombres de usuario	
Contraseñas	

Plantilla de Denegación de Servicio (Denial of Service)

Testeo del sistema

Dirección IP	
Puerto de servicio	
Tipo de servicio	
Protocolo	
Descripción del test	
Respuesta al test	

Dirección IP	
Puerto de servicio	
Tipo de servicio	
Protocolo	
Descripción del test	
Respuesta al test	

Testeo de procesos

Proceso	
Personas	
Ubicación	
Hora/Fecha	
Descripción del test	
Respuesta al test	

Proceso	
Personas	
Ubicación	
Hora/Fecha	
Descripción del test	

Respuesta al test	

Plantilla de Análisis de Documentos

Contactos principales	
Método de contacto	

Información de la organización	
Nombre del trabajo	
Dirección de trabajo	
Teléfono de trabajo	
Fax de trabajo	
Modelo jerárquico	
Jerarquía de la oficina	
Línea de negocio	
Operaciones	
Estructura legal	
Año de inicio	
Historia de la compañía	

Departamentos y responsabilidades	
Información de telecomunicaciones	
Números registrados de teléfonos de la oficinas	
Bloque de número de teléfonos	
Tipo de número de teléfonos	
Cantidad de módems	
Números de teléfono de módems	
Velocidad de conexión de los módems	
Número de equipos de fax	
Números de teléfono de fax	
Números de teléfono no habituales	

Datos de empleados	
Nombres de empleados y posición	
Páginas personales de empleados	
Información de empleados	

Subcontratistas	
Diseñadores Web	
Correo electrónico	
Soporte técnico	
Cortafuegos	
Sistema de detección de intrusiones	

Mesa de ayuda	
Socios	
Revendedores	
Proveedor de Internet	
Proveedores de Servicios de Aplicaciones	

Información IP	
Nombres de dominio	
Bloques de red	
Propietario de los bloques de red	
Fecha de creación de los registros	
Última fecha de modificación de los registros	

Información de red interna

Número de cuentas de red	
Estándar de cuentas de red	
Estándar de creación de cuentas internas	
Clientes web utilizados	
Tamaño de pantalla	
Configuración de seguridad en el navegador web	

Información interna de sistemas	
Número de Sistemas	
Estándar de nombres de sistema	
Nombres de Sistemas	
Tipos de sistemas	
Sistemas operativos	
Servicios ofrecidos	

Información de correo	
Dirección del servidor de correo	
Tipo de servidor de correo	
Clientes de correo	
Sistema de correo	
Estándar de direcciones de correo	

Pie de correos	
Estándar de cifrado	
Correos rebotados	
Ruta del servidor de SMTP	
Respuestas automáticas de vacaciones	
Listas de correo	

Información Web	
Dirección de servidor web	
Tipo de servidor web	
Ubicación del servidor	
Fechas mostradas	
Fecha de última modificación	
Enlaces de web internos	
Capacidades de búsqueda en el servidor	
Enlaces de web externos	
Árbol de directorios del servidor de web	

Tecnologías utilizadas	
Estándares de cifrado	
Lenguajes de programación web	
Campos de formulario	
Variables de formulario	
Método de publicación de formularios	
Palabras claves utilizadas	
Forma de contacto con la compañía	
Meta tags	
Comentarios detectados	
Capacidades de comercio electrónico	
Servicios ofrecidos en Internet	
Productos ofrecidos en Internet	

Características	
Motores de búsqueda detectados	
Puntuación en motores de búsqueda	
Número de accesos diarios / semanales / mensuales	
Popularidad de los enlaces	
Cultura de los enlaces	

Información de administración de archivos	
Dirección del servidor FTP	
Dirección del servidor SMB	
Ubicación de los servidores	
Tipo de servidores	
Árbol de directorios	
Ubicación de los archivos	
Servicios de nombres	
Servidor primario (autorizado) de nombres	
Servidor secundario	
Ultima actualización	
Servidores de nombre adicionales	

Información de cortafuegos	
Dirección del cortafuegos	
Tipo de cortafuegos	
Tipo de sistema de detección de intrusiones (IDS)	

Información de enrutamiento	
Direcciones de los routers	
Tipos de routers	
Capacidades de los routers	

Información de redes privadas virtuales (VPN)	
Capacidades de las redes privadas virtuales	
Tipo de redes privadas virtuales	

Servicios de red	
Servicios de red detectados	

Información de presencia en Internet	
Publicaciones en grupos de noticias	
Publicación en áreas de mensajes	
Publicación en sistemas de información de negocios	
Oferta de trabajo	
Archivos P2P	
Número de software ilegal encontrado	
Números de serie encontrados	

Análisis de la competencia	
Lista de clientes	
Franja de Mercado	
Lista de productos	

Plantilla de Ingeniería Social

Compañía	
Nombre de la compañía	
Dirección de la compañía	
Teléfono de la compañía	
Fax de la compañía	
Página web de la compañía	
Productos y Servicios	
Contactos Principales	
Departamentos y Responsabilidades	
Ubicación de las oficinas	
Historia de la Compañía	
Socios	
Revendedores	
Regulaciones de la compañía	
Información sobre políticas de seguridad	

Tradiciones de la compañía	
Publicación de ofertas de trabajo	
Disponibilidad de empleos temporales	
Riesgos típicos de IT	

Personas	
Información de empleados	
Nombre y cargos de empleados	
Posición del empleado en la jerarquía	
Páginas personales del empleado	
Métodos de contacto del empleado	
Pasatiempos del empleado	
Datos en Internet del empleado (listas de correo, usenet)	
Opiniones que ha expresado el empleado	
Familiares y amigos del empleado	
Historial del empleado (incluyendo historia laboral)	
Rasgos del carácter del empleado	
Valores y prioridades del empleado	
Hábitos sociales del empleado	
Patrones de habla y forma de hablar del empleado	
Gestos y maneras del empleado	

Equipamiento	
Equipamiento utilizado	
Servidores, número y tipo	
Estaciones de trabajo, número y tipo	
Programas utilizados (y versiones)	
Nombres de host utilizados	
Topología de red	
Capacidades anti-virus	
Recursos usados para la protección de la red (con sus versiones de software)	
Recursos usados para acceso remoto (incluyendo conexión por modem)	
Routers utilizados (con sus versiones de software)	
Tecnología usada para el control de acceso físico	
Ubicación de los vertederos de desechos utilizados	

Lista de Comprobación de Tests de Seguridad Legales

ASPECTOS A CONSIDERAR	LEY APLICABLE
PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN	
Obtención y uso de información personal. La información personal sobre personas vivas puede ser obtenida y utilizada solo si es necesaria para las pruebas de seguridad realizadas y si esto esta legalmente permitido. Ciertas condiciones deben ser tenidas en consideración cuando se obtenga o utilice información personal. Estas condiciones varían de acuerdo a los países y podrían incluir: o Obtener el consentimiento del individuo cuya información va a ser obtenida y utilizada. o Si la información es necesaria para la prevención o detección de un crimen.	Existen diferentes variaciones internacionales en relación a la obtención y proceso de datos personales. Existe un cierto nivel de consistencia entre los paises de la Comunidad Europea que han implementado la Directiva 95/46/EC del Parlamento Europeo y del Consejo sobre la protección de datos personales con respecto al proceso de dichos datos y el libre movimiento de éstos (OJ [1995] L281/31). El Acta de Protección de Datos (Computer Proteccion Act) de 1998 del Reino Unido, que está basada parcialmente en la Directiva 95/46/EC exige expresamente que los datos personales sólo pueden ser obtenidos y procesados legalmente y fielmente. Se deben satisfacer una serie de condiciones para demostrar que se está acatando Acta de Protección de Datos.
Copia, almacenamiento, retención y destrucción de información. La información perteneciente a terceros puede ser copia y retenida por los Auditores de Seguridad cuando sea relevante y necesaria para realizar un análisis o generar un informe. A menos que dichas actividades estén prohibidas expresamente por contrato o por la legislación vigente. La información perteneciente a terceros sólo debería mantenerse tanto y como fuera necesario para los objetivos de pruebas y generación de informes. La información legalmente obtenida y estimada necesaria para los propósitos de la prueba debe ser destruida de forma apropiada cuando ya no sea necesaria su utilización.	Los requisitos legales para el tratamiento de la información varían de país a país. Existe cierta consistencia en los países de la Comunidad Europea que están sujetos a la Directiva 95/46/E El Acta de Protección de Datos de 1998 del Reino Unido, parcialmente basada en la Directiva 95/46/EC requiere de forma expresa que los dato personales no deben mantenerse más allá de lo estrictamente necesario y que se deben tomar medidas de seguridad adecuadas para proteger la información personal. Cuando una compañía de Estados Unidos desea compartir información con una compañía sujeta a la Directiva 95/46/EC, la compañía estadounidens debe seguir los requisitos proteccion de datos personales.

Revelación de información • No se debe revelar información a individuos no autorizados.	Existen varias reglas en vigor para la protección d información de revelación no autorizada. Estas reglas pueden ser necesarias para proteger la confidencialidad comercial o la privacidad de los individuos.
• El Auditor de Seguridad debe asegurarse de que se respetan los derechos de privacidad de un individuo en todos los casos necesarios. • El Auditor de Seguridad no debería actuar en ninguna forma que podría resultar en la ruptura de la confidencialidad o la contravención de cualquier ley o contrato.	- Los países integrantes de la Comunidad Europea han adoptado la Convención Europea de los Derechos Humanos a sus leyes nacionales. - El Acta de Derechos Humanos del Reino Unido de 1998 incorpora el derecho de privacidad definido en el artículo 8 de la Convención. También exige que se utilic al menos un nivel de protección mínimo - El artículo 12 de la Declaración de Derechos Humanos de las Naciones Unidas determina que todo individuo tiene derecho a su privacidad.

INTEGRIDAD DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN	
Interferencia no autorizada en sistemas de información. • Los Auditores de Seguridad no tiene permitido causar interferencia a la operación de los sistemas de información de sus clientes de forma intencionada, a no ser que le esté permitido por la legislación vigente o por el propio cliente. • Puede ser necesario el consentimiento por escrito del cliente previo a la realización de una Prueba de Seguridad.	La interferencia con los sistemas de información está gobernada por un conjunto de normas internacionales. Aunque es una función que puede estar incorporada como un elemento en los términos d contrato. En el Reino Unido, es necesario observar los acto de la persona que interfiere en un sistema, el cua puede ser castigado según define la legislación: e Acta de Uso Inapropiado de Ordenadores (*Computer Misuse Act*), el Acta de Robo (*Theft Act*) o el Acta de Daños Criminales (*Criminal Damages Act*)
Daño y Modificación de la información o de sistemas de información • Los Auditores de Seguridad deben poner recaudos en no alterar o dañar la información o los sistema de información durante las pruebas, a excepción del o legalmente permitido por ley o por las partes contratantes.	La alteración, modificación o daño de la información por los Auditores de Seguridad pueden ser considerados como delitos civiles o penales, dependiendo del país. En el Reino Unido, está establecido en el Acta de Uso Inapropiado de Ordenadores (Computer Misuse Act) y en el Acta de Daños Criminales (Criminal Damages Act).

Uso no autorizado de la información o de sistemas de información. • No se debe permitir el uso no autorizado de la información o sistemas de información con las limitaciones que considere la ley vigente o la otra parte contractual.	Tanto la información como los sistemas de información necesitan ser protegidos de terceros por una amplia gama de razones; tales como mantener la confidencialidad del cliente o proteger las tareas de investigación y desarrollo de las compañías.

COMUNICACIÓN Y AUTORIZACIÓN	

Notificación de intenciones y acciones. • Se debe poner en conocimiento al cliente y a todos aquellos con el derecho legal de saber el impacto y las implicancias de una Prueba de Seguridad. • Los Auditores de Seguridad deben poner a disposición del cliente la información detallada asociada a las acciones que se tomarán como parte de la Prueba de Seguridad. • Si se descubre la presencia de atacantes (hackers) en el sistema de un cliente durante la Prueba de Seguridad, los Auditores deben informar al cliente tan pronto como sea posible. • Cualquier tercera entidad a la que pudiera afectar la Prueba de Seguridad debería ser informada de la naturaleza de éste cuando sea legalmente necesario.	Puede ser un requisito legal en algunos países el entregar notificaciones de intenciones y acciones referidas a la Prueba de Seguridad. En el Reino Unido, los auditores son responsable por una variedad de razones si no proveen dicha notificaciones. Esto supone una violación de los acuerdos contractuales, un acto de negligencia o una infracción a la legislación vigente, como el Acta de Uso Inapropiado de Ordenadores de 199
Notificación de Responsabilidades: • Los Auditores de Seguridad deberían asegurarse que los clientes son conscientes de sus responsabilidades incluyendo: - Realizar copias de seguridad de la información previa a las pruebas. - Informar a aquellos empleados que deban conocer la prueba, por razones legales u operativas.	Éste es generalmente un requisito de diligencia necesario que puede ser aplicado internacionalmente.

Autorización: • Puede ser necesario un permiso escrito del cliente para el Auditor antes de realizar las Pruebas de Seguridad. • Puede ser necesario obtener el consentimiento de individuos u organizaciones distintas del cliente antes de realizar la Prueba de Seguridad.	La realización de una Auditoria de Seguridad sin autorización debida es considerada un delito civ dependiendo del país en el que se lleva a cabo la Auditoria. El Acta de Uso Inapropiado de Ordenadores de 1990 del Reino Unido convierte en delito el acce a un sistema sin la autorización debida.
Suspensión de la Prueba de Seguridad • Si se descubre un intruso en un sistema de información del cliente durante la Prueba de Seguridad, la prueba debe ser suspendida y el incidente reportado al cliente. Tras la suspensión, la Prueba de Seguridad sólo debería comenzar de nuevo tras la aprobación del cliente.	Cualquier Auditor de Seguridad debe actuar con cautela o podrían ser punibles por una variedad de delitos menores. En particular se debe tener cuidado cuando se descubren intrusos de seguridad y el Auditor no desea ser acusado de l acciones del intruso.

CONTRATO	
Creación del contrato, términos y condiciones • Asegúrese de que el contrato se ajusta a las normas legales vigente. • Los términos y condiciones de la realización de una Prueba de Seguridad deben estar suficientemente detallados para establecer los derechos y responsabilidades del cliente y del auditor.	El uso de contratos es una práctica reconocida internacionalmente. Existen diferencias entre los países con leyes contractuales y éstas deberían s tenidas en cuenta si se realizan contratos con organizaciones de otros países. - En el Reino Unido se pueden tomar información de la realización de contrato en el Acta de Oferta de Servicios y Productos de 1982 (*Supply of Goods ar Services Act*). Este acta indica la existencia de términos implícitos en los contratos como el término implícito que indica que un contacto será realizado los cuidados necesarios y las habilidades requeridas.

Responsabilidades • Asegúrese de que las cláusulas legales apropiadas con relación a la limitación de responsabilidad están presentes en el contrato. Por ejemplo, una cláusula que debe existir es la de limitar la responsabilidad del Auditor en el caso de que ocurran daños o pérdidas como resultado de la incapacidad del cliente de implementar las medidas de protección adecuadas en los sistemas de información o cualquiera de los elementos que estén conectados a ellos.	Existen variaciones internacionales en el conten de las cláusulas de responsabilidad. - El Reino Unido define las limitaciones de responsabilidad que están sujetas a legislación en el Acta de Términos Injust de Contratos de 1977 (*Unfair Contract Terms Act*).
Contenidos: • Debe ser necesario asegurar que la información específica para la auditoria de seguridad se incluye en cualquier documento contractual, como pudiera ser: - Una lista de todas las direcciones de IP asignadas que deben ser expresadas como una dirección IP individual y un rango.	Proveer de detalles acerca del alcance y los parámetros de la Prueba de Seguridad protege tanto al cliente como al auditor.

Referencias de Testeo

Las siguientes son referencias clave para la utilización de este manual durante el Testeo. **sap 27**

Sap o *sucker* 27 son diversas extensiones que se utilizan para hacer llegar código malicioso a diversos sistemas de correo electronico y navegadores.

EXT.	DESCRIPCIÓN
.ade	Extensión de Microsoft Access Project
.adp	Microsoft Access Project
.bat	Archivo Batch
.chm	Archivo de ayuda de HTML compilado
.cmd	Comandos de Microsoft Windows NT
.com	Programa de Microsoft MS-DOS
.cpl	Extensión del Control Panel
.crt	Certificado de Seguridad
.eml	Correo de Outlook Express
.exe	Programa

.hlp	Archivo de ayuda
.hta	Programa HTML
.inf	Información de Configuracion
.ins	Servicio de Nombres de Internet
.jpg	Imagen JPEG
.isp	Configuración de comunicaciónes de Internet
.js	Archivo Jscript
.jse	Archivo de JScript codificado
.mdb	Programa Microsoft Access
.mde	Base de datos Microsoft Access MDE
.msc	Documento de Microsoft Common Console
.msi	Paquete instalador de Microsoft Windows
.msp	Parche del Instalador de Microsoft Windows
.mst	Archivos de código fuente de Microsoft Visual Test
.pcd	Codigo compilado de MS Visual, Imagen de Photo CD
.pif	Acceso directo a un programa de MS-DOS
.reg	Entradas de registro
.scr	Protector de pantalla
.sct	Componente de Windows Script
.shb	Objeto Shell Scrap
.shs	Objeto Shell Scrap
.url	Página HTML
.vb	Archivo VBScript
.vbe	Archivo de VBScript codificado
.vbs	Archivo VBScript
.wav	Archivo de sonido
.wsc	Componente de Windows Script
.wsf	Archivo de Windows Script
.wsh	Archivo de configuración de Windows Script Host

Protocolos

Como una extensión de la lista de protocolos de Internet del OSSTMM original, el OPRP es un recurso unico de información de los protocolos, información de transporte y especificaciones de Internet. Este recurso es esencial para la realización de tests de seguridad completos.

Puede obtenerse de ISECOM en la siguiente dirección:

http://www.isecom.org/projects/protocolresource.htm

Licencia de Metodología Abierta (OML)

PREÁMBULO

Una metodología es una herramienta que detalla QUIÉN, QUÉ, CUÁL Y CUÁNDO. Una metodología es capital intelectual y está a menudo enérgicamente protegido por instituciones comerciales. Las metodologías abiertas son actividades comunitarias que transforman todas las ideas en un solo documento de propiedad intelectual que está disponible sin cargo para cualquier individuo.

Con respecto a la GNU General Public License (GPL), esta licencia es similar con la excepción del derecho de los desarrolladores de software a incluir las metodologías abiertas que están bajo esta licencia en los programas comerciales. Esto hace que esta licencia sea incompatible con la licencia GLP.

La principal preocupación de los desarrolladores de metodologías abiertas que esta licencia tiene en cuenta, es que ellos recibirán el debido reconocimiento por su contribución y desarrollo, así como también el reservarse el derecho de permitir las publicaciones y distribuciones gratuitas cuando las metodologías abiertas no sean utilizadas en material comercial impreso del cual las ganancias se deriven ya sea de su publicación o distribución.

Agradecimientos especiales a la Free Software Foundation y a la GNU General Public License por los conceptos legales y la redacción.

TÉRMINOS Y CONDICIONES

1. Esta licencia se aplica a cualquier metodología o cualquier herramienta intelectual (por Ej., matriz, lista de comprobación, etc.) que contenga un aviso colocado por el titular de los derechos de autor diciendo que está protegido bajo los términos de esta Licencia sobre Metodologías Abiertas.
2. Esta Metodología se refiere a cualquier metodología, herramienta intelectual o cualquier trabajo basado en la Metodología. Un "trabajo basado en la Metodología" significa tanto la Metodología como cualquier trabajo derivado protegido por leyes de derechos de autor que se aplique al trabajo que contiene la Metodología o una porción de la misma, ya sea literalmente o con modificaciones y/o traducida a otro idioma.
3. Cualquier persona puede copiar y distribuir copias literales de la Metodología en la misma forma en que dichas copias fueron recibidas, y a través de cualquier medio, con la condición de que sea visible y apropiadamente publicado en cada copia el aviso de derechos de autor y la mención explícita del creador o creadores de la Metodología, y se mantengan intactos todos los avisos que ser refieren a esta Licencia y a la ausencia de cualquier garantía, y dar a cualquier receptor de la Metodología una copia de esta Licencia junto con la Metodología así como también la ubicación de donde pueden obtener una copia original de la Metodología directamente del titular de los derechos de autor.
4. Está terminantemente prohibida la venta de la Metodología, el cobro por la distribución de la misma o por cualquier medio del cual la Metodología forme parte sin el consentimiento expreso del titular de los derechos de autor.

5. Está permitida la inclusión total o parcial de esta Metodología en ofrecimientos de servicios comerciales, para usos privados o no comerciales, o para propósitos educativos sin el consentimiento explícito del titular de los derechos de autor, con la condición de que los servicios comerciales, privados o de uso interno ofrecidos cumplan con los requisitos de los ítems 3 y 4 de esta Licencia.

6. Está terminantemente prohibida la modificación o cualquier cambio en esta Metodología para su republicación sin el consentimiento explícito del titular de los derechos de autor.

7. Está permitido utilizar la Metodología o cualquier parte de ella para desarrollar o mejorar programas comerciales o de distribución gratuita, y copiar y distribuir esos programas bajo cualquier término, con la condición de que se respeten las siguientes condiciones:

a) Los ítems 3, 4, 5, y 6 de esta Licencia deberán ser estrictamente cumplidos.
b) Cualquier reducción o uso incompleto de estas Metodologías en los programas debe estricta y explícitamente declarar cuáles partes de la Metodología fueron utilizadas en los programas y cuáles partes no fueron utilizadas.
c) Cuando los programas que utilizan la Metodología sean ejecutados, deben mostrar un aviso que indique el uso de la Metodología, incluyendo un aviso de los derechos de autor y un aviso de garantía y de como acceder a una copia de esta licencia o tomar otras medidas específicas, como proveer documentación, o mostrar el código abierto utilizado.

8. Si, como consecuencia de una sentencia judicial o una alegación de infracción de patente o por cualquier otra razón (no limitada a cuestiones de patentes), se imponen condiciones a una persona (ya sea por orden de la corte, por acuerdo o de otras maneras) que contradicen las condiciones de esta Licencia, ello no lo exime del cumplimiento de las condiciones de esta Licencia. Si dicha persona no puede satisfacer simultáneamente sus obligaciones bajo esta Licencia y otras obligaciones pertinentes, entonces, como consecuencia de ello, dicha persona no puede usar, copiar, modificar o distribuir la Metodología en absoluto. Si cualquier porción de esta sección es considerada no válida o inexigible bajo cualquier circunstancia particular, el equilibrio de la sección se intentará aplicar y esa sección como un todo será aplicada a cualquier otra circunstancia.

9. Si la distribución y/o uso de la Metodología está restringido en ciertos países ya sea por patentes o por interfaces con derechos de autor, el titular original de los derechos de autor que coloca el Programa bajo esta Licencia puede agregar una limitación de distribución geográfica explícita excluyendo a esos países, de manera que la distribución esté permitida solamente en o entre los países no excluídos de esa manera. En tal caso, esta Licencia incorpora la limitación como tal escrita en el cuerpo de esta Licencia

10. El Institute for Security and Open Methodologies (ISECOM) tiene la facultad de publicar versiones revisadas y/o nuevas versiones de la Licencia sobre Metodologías Abiertas.

Estas nuevas versiones serán similares en su espíritu a la versión actual, pero pueden diferir en los detalles al referirse a nuevos problemas o preocupaciones.

SIN GARANTIAS

11. DEBIDO A QUE ESTA METODOLOGÍA SE OTORGA SIN CARGO, NO HAY GARANTÍAS PARA LA MISMA, HASTA EL MÁXIMO ALCANCE PERMITIDO POR LAS LEYES VIGENTES. EXCEPTO CUANDO DE OTRA MANERA SEA ESTABLECIDO POR ESCRITO QUE LOS TITULARES DE LOS DERECHOS DE AUTOR Y/O TERCEROS, PROVEAN LA METODOLOGÍA "TAL COMO ESTÁ" SIN GARANTÍA ALGUNA NI DE NINGUNA CLASE, YA SEA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITADAS A LAS GARANTÍAS IMPLICADAS DE COMERCIABILIDAD Y APTITUD PARA UN PROPÓSITO PARTICULAR. EL RIESGO TOTAL EN LO QUE SE REFIERE A LA CALIDAD Y EL FUNCIONAMIENTO EN EL USO DE LA METODOLOGÍA ES EXCLUSIVAMENTE DEL USUARIO. SI LA METODOLOGÍA DEMOSTRARA SER INCOMPLETA O INCOMPATIBLE, EL USUARIO ASUME LOS COSTOS DE CUALQUIER SERVICIO, REPARACIÓN O CORRECCIÓN NECESARIAS.

12. BAJO NINGUNA CIRCUNSTANCIA, A MENOS QUE ESTÉ ESTABLECIDO POR LA LEY VIGENTE O ACORDADO POR ESCRITO, NINGUN TITULAR DE LOS DERECHOS DE AUTOR, O TERCEROS QUE USEN Y/O REDISTRIBUYAN ESTA METODOLOGÍA SIN MODIFICARLA COMO ESTÁ PERMITIDO EN ESTA LICENCIA, PODRÁN SER RESPONSABILIZADOS POR OTRAS PERSONAS POR DAÑOS, INCLUYENDO CUALQUIER DAÑO ESPECIAL, INCIDENTAL O DAÑOS CONSECUENTES QUE DERIVEN DEL USO O INCAPACIDAD PARA USAR ESTA METODOLOGÍA (INCLUYENDO PERO NO LIMITADO A LA PÉRDIDA DE DATOS O QUE LOS DATOS SEAN INVALIDADOS O PÉRDIDAS CAUSADAS POR CUALQUIER PERSONA O TERCEROS O FALLAS EN LAS METODOLOGÍAS PARA OPERAR CON CUALQUIER OTRAS METODOLOGÍAS), INCLUSO SI EL PROPIETARIO O TERCEROS HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

Bibliografía

[1] ISO/IEC 12207:2008 En el ciclo de vida del desarrollo del software https://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2FIEC+12207%3A2008&sourcekeyword=&source=google&adgroup=iso13&gclid=EAIaIQobChMIgeWn3_Cv1gIVDoCRCh098AC_EAAYAiAAEgKG__D_BwE . (Consulta 1/09/2017)

[2] Ciclo de Vida de Desarrollo de Software https://ingsw.pbworks.com/f/Ciclo+de+Vida+del+Software.pdf (Consulta 15/08/2018)

[3] Ciclo de vida de desarrollo de software https://www.innovativearchitects.com/KnowledgeCenter/basic-IT-systems/system-development-life-cycle.aspx (consulta 18/08/2018)

[4]OWASP https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (consulta 12/10/2019)

[5] Seguridad en Frameworks https://medium.com/@A01270898/seguridad-en-frameworks-c125f88b883 (consulta 13/10/2019)

[6] Sonarqube https://www.sonarqube.org/features/security/?gclid=Cj0KCQjw84XtBRDWARIsAAU1aM1NK0y-JpuLpAUr1KGlqDr9cb6U3ktTBV4GBIrnwyZco_RKtoqJKqUaArFoEALw_wcB (consulta 13/10/2019)

[7] El ciclo de vida de desarrollo de seguridad de Trustworthy Computing https://msdn.microsoft.com/es-es/library/ms995349.aspx (Consulta 10/09/2017)

[8] Seguridad en el Ciclo de Vida del Desarrollo de Software https://www.owasp.org/images/7/76/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf (Consulta 16/10/2019)

[9] Seguridad en el SDLC
https://www.gestiopolis.com/seguridad-en-sdlc-ciclo-de-vida-de-desarrollo-de-software/ (Consulta 14/10/2019)

[10] Metodología y Frameworks de Testeo de la seguridad en las aplicaciones
http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.1/contenido-recurso-216.html (Consulta 13/11/2019)