Extrelan 2008

Cáceres. Marzo de 2008

Técnicas y Procedimientos para la realización de Test de Intrusión

SG6 – Soluciones Globales en Seguridad de la Información

http://www.sg6.es

INDICE DE CONTENIDOS

PRIMERA PARTE: Sistemas de Información

Técnicas y Procedimientos para la realización de Test de Intrusión

SG6 – Soluciones Globales en Seguridad de la Información

http://www.sg6.es

Definiciones

- **Activo:** *"Cualquier valor cuantificable de naturaleza material o inmaterial de una organización"*

- **Amenaza:** *"Factor de riesgo externo representado por un peligro latente asociado a un fenómeno natural, tecnológico o humano, pudiendo manifestarse en un sitio específico por un tiempo determinado, produciendo efectos adversos a personas o bienes."* [Maskrey 1993]

- **Vulnerabilidad:** *"Factor de riesgo interno de un sistema expuesto a una amenaza, y se corresponde con su predisposición intrínseca a ser afectado o susceptible de daño."* [Cardona 1993]

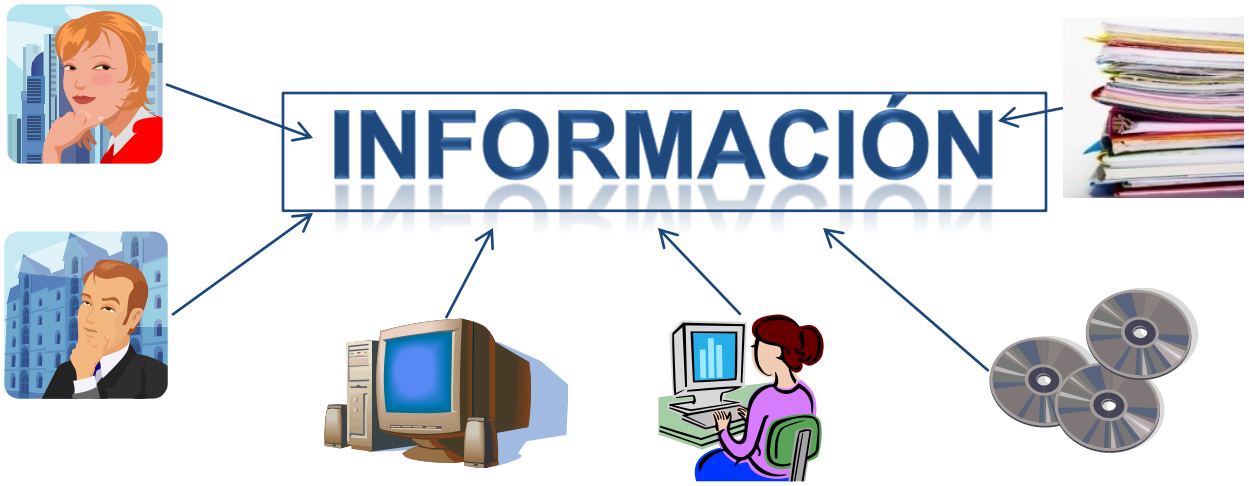
- **Riesgo:** *"Probabilidad de que una amenaza explote una vulnerabilidad."*

- **Impacto:** *"Cuantificación del daño ocasionado una vez materializada la amenaza"*

¿Qué es un Sistema de Información?

- "Un sistema de Información es el conjunto formado por los sistemas de IT, personas, datos y actividades que procesan, ya sea de manera manual o automática, la información de una organización." [Wikipedia]

- "Un sistema, ya sea manual o automático, que consta de personas, máquinas y/o métodos, organizados de tal manera que permitan reunir, procesar y transmitir información." [NIS]



¿Qué es un Sistema de Información?

- La información es uno de los activos más importantes en las organizaciones.

- Cada vez más, las organizaciones se sustentan sobre una base tecnológica. Por lo tanto, el impacto que se produce ante un incidente va en aumento.

- Cualquier amenaza que pueda afectar a los sistemas de información de la empresa supone un riesgo para los procesos de negocio de la organización.

Seguridad Informática vs Seguridad de la Información

- De manera errónea se utilizan estos dos conceptos indistintamente, pero son totalmente diferentes y sus marcos de aplicación son distintos.

- El campo de aplicación de la **Seguridad Informática** está orientado principalmente hacia los sistemas de TI, es decir, intenta solventar aspectos técnicos.

- La **Seguridad de la Información** no se limita únicamente a los sistemas, sino que también engloba la seguridad física, operacional y organizacional del sistema de información.

Objetivos de la Seguridad de la Información

- Los objetivos principales que pretende preservar la Seguridad de la Información son:
  - **Confidencialidad:** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
  - **Integridad:** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
  - **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran, a la información y sus activos asociados
- ¡La seguridad no es cualitativa sino cuantitativa!

SEGUNDA PARTE: Amenazas y Vulnerabilidades

Técnicas y Procedimientos para la realización de Test de Intrusión

SG6 – Soluciones Globales en Seguridad de la Información

http://www.sg6.es

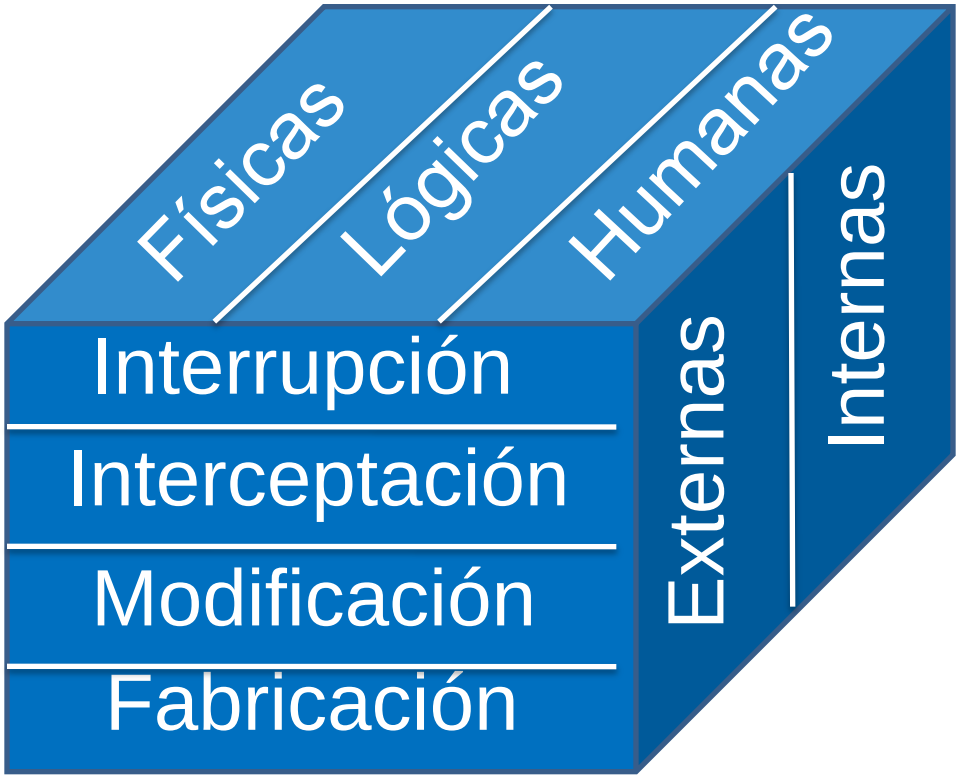
Clasificación de Amenazas

- **Atendiendo al origen:**
  - Externas. Se originan desde fuera de la organización.
  - Internas. Se producen desde dentro de la propia organización y suelen tener un mayor impacto sobre la misma.
- **Atendiendo al área de efecto:**
  - Físicas. Afectan a los elementos físicos de las organizaciones.
  - Lógicas**.** Su área de efecto engloba a todos los activos de naturaleza digital.
  - Humanas. Se centran en vulnerar la seguridad utilizando como medio a las personas.

Clasificación de Amenazas

- **Atendiendo al efecto que provoca:**
  - Interrupción. Esta amenaza afecta a la continuidad de los servicios, pudiendo hacer que estos queden inutilizados o no disponibles.
  - Interceptación. El propósito de esta clase se basa en el acceso no autorizado de un elemento a un determinado objeto.
  - Modificación. Implica que un elemento no autorizado, además de acceder al objeto ha conseguido modificarlo.
  - Fabricación. El objetivo de esta eventualidad es el de crear un objeto similar al atacado de tal manera que pueda suplantar al original.

Clasificación de Amenazas



Entorno de Demostración
OWASP - WebGoat

- La **Open Web Application Security Project (OWASP)** es una comunidad enfocada en la mejora de la seguridad del software que engloba miembros de todo el mundo.

- **OWASP Testing Guide** es una metodología para la realización de test de intrusión y evaluación de la seguridad de las aplicaciones Web. (http://www.owasp.org/index.php/Category:OWASP_Testing_Project)

- **WebGoat** representa una aplicación J2EE insegura, diseñada por OWASP para el aprendizaje de la evaluación de la seguridad de las aplicaciones Web. Su objetivo es servir como entorno de pruebas para la metodología creada por la comunidad. http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Clasificación de Vulnerabilidades

Errores de Diseño

- Este tipo de errores se producen cuando el diseño del flujo operacional del propio aplicativo es inseguro. Los motivos que originan este tipo de errores suelen ser la ignorancia, negligencia o simplemente el desconocimiento de algunos conceptos mínimos de seguridad.

- **Autenticación**

  - Autenticación insuficiente. Se presenta cuando un aplicativo Web permite a un atacante el acceso a contenido privilegiado o funcionalidades sin haberse autenticado. Ejemplo: http://www.paginadepruebas.es/Administrador/admin.php o http://www.paginadepruebas.es/administrar.php?autenticado=true

  - Validación débil en la recuperación de contraseñas. Se puede utilizar este ataque cuando el aplicativo permite a un atacante obtener o modificar la contraseña de otro usuario. Ejemplo: Hotmail hace unos años. http://127.0.0.1/WebGoat/attack?Screen=219&menu=310

Clasificación de Vulnerabilidades

Errores de Diseño

- **Autorización**

  - Predicción de credenciales. Este método permite a un atacante suplantar la identidad de un usuario legítimo. A todos los efectos, interactúa con el aplicativo como si fuera el usuario comprometido. Ejemplo: Cookie con nombre de usuario o número secuencial. http://127.0.0.1/WebGoat/attack?Screen=228&menu=310

  - Expiración de sesión insuficiente. Se produce cuando el tiempo de expiración de las credenciales es tal que permite a un atacante reutilizar credenciales suyas o de otros usuarios para autenticarse. Ejemplo: Uso de ordenadores compartidos.

  - Fijación de sesión. Si un aplicativo Web asigna siempre las mismas credenciales o ID a un usuario, estas pueden ser aprovechadas por un atacante para suplantarlo, siempre que este las conozca y el usuario comprometido se encuentre autenticado dentro del aplicativo.

Clasificación de Vulnerabilidades

Errores de Diseño

- **Ataques lógicos**
  - Abuso de Funcionalidad. Mediante este error, un atacante puede aprovechar las propias capacidades y funcionalidades de un aplicativo Web, para evadir los mecanismos de autenticación.
  - Validación de proceso insuficiente. Este ataque se presenta cuando un aplicativo permite a un atacante evadir o engañar el flujo de control de la aplicación. http://127.0.0.1/WebGoat/attack?Screen=49&menu=710

Clasificación de Vulnerabilidades

Errores de Programación y Configuración

- El desarrollo de un aplicativo no es más que la codificación del diseño realizado. El problema radica en que algunas veces muchas decisiones de diseño se toman en el mismo momento de la implementación.

- La celeridad genera que dichas decisiones no estén lo suficientemente estudiadas.

- **Autenticación**
  - Fuerza Bruta. Este ataque consiste obtener información probando todas las combinaciones posibles mediante un proceso automatizado. Ejemplo: Obtención de contraseñas (fortificación).

- **Ataques en la parte cliente**
  - Suplantación de contenido. Mediante esta técnica un atacante consigue hacerle creer al usuario objetivo que cierto contenido de un aplicativo Web es legítimo, cuando no lo es. Ejemplo: Phising.

  - Cross-Site Scripting (XSS). Este método fuerza al aplicativo Web a repetir código que ha insertado el atacante, de tal manera que el navegador del cliente lo interprete y ejecute. http://127.0.0.1/WebGoat/attack?Screen=18&menu=410

Clasificación de Vulnerabilidades

Errores de Programación y Configuración

- **Ejecución de comandos**
  - Desbordamientos de buffer. Este tipo de técnica permite alterar el flujo de un programa a través de la modificación de contenidos de memoria.
  - Inyección SQL. Este ataque permite alterar los contenidos de las sentencias SQL que se generan a través de entradas del aplicativo Web. http://127.0.0.1/WebGoat/attack?Screen=6&menu=610
  - Inyección LDAP. Este ataque permite alterar los contenidos de las sentencias LDAP que se generan a través de entradas del aplicativo Web.

Clasificación de Vulnerabilidades

Errores de Programación y Configuración

- **Obtención de información**
  - Indexación de directorios. Esta función permite que el servidor liste los ficheros de un directorio determinado.
  - Path trasversal. Esta técnica permite el acceso a ficheros, directorio o incluso ejecutables que residen fuera del directorio raíz del servidor.
  - Recursos predecible. Mediante este proceso un atacante intenta acceder a recursos y funcionalidades que suelen estar ocultas pero accesibles en un servidor Web cuando este no está configurado correctamente.
    http://127.0.0.1/WebGoat/attack?Screen=10&menu=1010

TERCERA PARTE: Test de Intrusión

Técnicas y Procedimientos para la realización de Test de Intrusión

SG6 – Soluciones Globales en Seguridad de la Información

http://www.sg6.es

¿Qué es un Test de Intrusión ?

- Un test de intrusión es una evaluación de las medidas de protección de una organización y de los servicios expuestos a Internet.

- El objetivo es vulnerar la seguridad de los mecanismos implantados para conseguir por ejemplo un acceso no autorizado a la organización, obtener información sensible, interrumpir un servicio,… todo depende del alcance del test.

- Un test de intrusión es diferente de una revisión de seguridad exhaustiva.

Test de Intrusión de aplicativos Web. Metologías

- Para conseguir mantener una coherencia en las acciones y un orden en lo procedimientos, es necesario seguir algún tipo de metodología que guíe todo el proceso.

- Existen diversas metodologías para realizar test de intrusión, entre las más extendidas se encuentran:

  - OSSTMM de ISECOM (http://www.isecom.org/osstmm/)
  - ISSAF de OISSG (http://www.oissg.org/)
  - OWASP Testing Guide de OWASP (http://www.owasp.org/)

- Todas estas metodologías contienen muchos puntos en común, pero difieren en la manera de hacer algunas cosas.

- En el marco internacional OSSTMM una de las más relevantes.

Test de Intrusión de aplicativos Web. Pasos

- **Recopilación de información**
  - Este punto se basa en la obtención de tanta información como se pueda de las aplicaciones objetivo y el sistema que las sustenta.
  - Entre las distintas acciones que se pueden tomar se encuentran las siguientes:
    - Obtención de versión tanto del servidor web como de la aplicación.
    - Descubrimiento de las aplicaciones instaladas en el servidor.
    - Descubrimiento de puertos.
    - Técnicas de Spidering y Googling
    - Análisis de códigos de error
    - Evaluación del Listener de la BBDD
    - Evaluación de la configuración de la aplicación

Test de Intrusión de aplicativos Web. Pasos

- **Comprobación del sistema de autenticación**
  - Este punto se basa en comprobar la robustez del sistema de autenticación en base a distintas técnicas.
    - Pruebas de diccionario
    - Fuerza Bruta
    - Evasión del sistema de autenticación (predicción de ID de sesión, SQL Injection, modificación de parámetros,..)
    - Path Traversal
    - Recordatorio de contraseña débil
    - Análisis de gestión de la caché y salida de sesión

Test de Intrusión de aplicativos Web. Pasos

- **Prueba de gestión de sesiones**
  - La gestión de sesiones comprende todos los controles que se realizan sobre el usuario, desde la autenticación hasta la finalización de la aplicación.
  - Los elementos a evaluar son los siguientes:
    - Análisis del esquema de gestión de sesiones
    - Manipulación de cookies y testigos de sesión.
    - Variables de sesión expuestas
    - Abuso de sesión

Test de Intrusión de aplicativos Web. Pasos

- **Análisis de validación de datos**
  - Esta parte suele ser una de las más extensas de una revisión de seguridad ya que suele ser la debilidad más común.
  - Este proceso se basa en validar todas las formas posibles de entradas de información por parte del usuario.
  - Las categorías principales son las siguientes:
    - Cross-Site Scripting
    - Inyección de SQL
    - Inyección de LDAP
    - Inyección de XML
    - Inyección de SSI
    - Inyección de Xpath
    - Inyección de IMAP/SMTP
    - Inyección de Código
    - Buffer OverFlow

Test de Intrusión de aplicativos Web. Pasos

- **Examen de denegación de servicio (Denial Of Service)**

  - El objetivo de este proceso consiste en inundar con suficiente tráfico una máquina objetivo con el fin de hacerla incapaz de sostener el volumen de peticiones que recibe.

  - Este tipo de examen no se presenta en todos los escenarios, ya que algunos entornos se encuentran en producción, por lo cual una interrupción del servicio puede ocasionar pérdidas sustanciales.

Test de Intrusión de aplicativos Web. Pasos

- **Comprobación de servicios Web/AJAX**

  - Los servicios web y SOA (Arquitectura Orientada a Servicios) permiten que las organizaciones y los procesos de negocio interoperen y crezcan a un ritmo elevado.

  - Las vulnerabilidades en servicios web son similares a otras vulnerabilidades como la inyección SQL, aunque presentan alguna más referente a XML.

  - Algunas pruebas que se llevan a cabo son las siguientes:
    - Pruebas estructurales de XML
    - Comprobación de XML a nivel de contenido
    - Comprobación de parámetros HTTP GET/REST
    - Adjuntos SOAP maliciosos

Test de Intrusión de aplicativos Web. Pasos

- **Redacción de Informes**
  - Este punto, pese a parecer el más sencillo de llevar acabo, en realidad es el más complejo y relevante debido a las implicaciones asociadas con el mismo.

  - La estimación del riesgo asociado es crítica para el negocio, ya que en la mayoría de casos, en base a los resultados que arroja se desprenden las salvaguardas oportunas.

  - Establecer un sistema de valoración de riesgos ahorrará tiempo y elimina las discusiones sobre prioridades, focalizando los esfuerzos sobre sobre los riesgos de mayor importancia.

  - Un mal informe que no plasme la realidad puede echar por tierra una revisión de seguridad excelente.
  - Los elementos que deben quedar reflejados son:
    - Identificación del riesgo
    - Estimar la probabilidad de ocurrencia
    - Estimar el impacto en la organización
    - Determinar la severidad del riesgo

FIN

- Ruegos y Preguntas