Medidas de seguridad y vulnerabilidades de los servidores web

Aarón Rodríguez Bueno
Hugo Maldonado Cózar

Contenido

Tres partes fundamentales:

- Seguridad del Computador
- Seguridad del Sistema Operativo
- Seguridad del Servidor Web


Seguridad del Computador

Definición de Seguridad de un Computador

Protección de un sistema de información automatizado al que le sean aplicables los objetivos de preservar en el sistema lo siguiente:

- Confidencialidad
- Integridad
- Disponibilidad

Conocido como la Tríada CIA

Confidencialidad

Evitar la divulgación no autorizada de información.

Formas de conseguirlo:

- Cifrado
- Control de acceso
- Autenticación
- Autorización
- Seguridad física

Integridad

Guardar la información frente a modificaciones inadecuadas o destructivas.

Formas de conseguirlo:

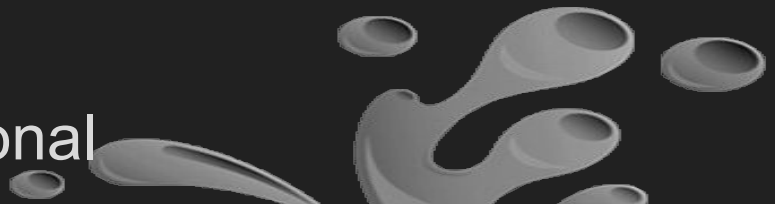
- Copias de seguridad
- Sumas de verificación
- Códigos de corrección de datos

Disponibilidad

Permitir que la información sea accesible y modificable en el tiempo.

Formas de conseguirlo:

- Protección física
- Redundancia computacional



Políticas y modelos de seguridad

- La seguridad del computador está definida por la política de seguridad.

- El cómo debe protegerse es responsabilidad de los mecanismos de seguridad.

- Se necesita detallar un modelo de seguridad.


Seguridad del Sistema Operativo

- Todos los sistemas operativos, como software que son, tiene vulnerabilidades.

- Todos tienen un modelo de confianza o Base de computación Segura del Sistema (TCB).

- Tres mecanismos para la confianza del TCB:
  - Funcionamiento en modo dual
  - Protección de memoria
  - Autorización del uso de los recursos

Fortalecimiento del Sistema Operativo

- Asegurar el sistema reduciendo la superficie de amenaza.
- Proceso que requiere planificación sobre los servicios.
- Se deben considerar multitud de puntos.
- Este proceso no tiene fin, evoluciona en el tiempo.

Fortalecimiento del Sistema Operativo

Etapas a considerar:

- Instalación
- Proceso de Arranque
- Ejecución del S.O.
- Actualizaciones
- Controles adicionales


Seguridad del Servidor Web

Vulnerabilidades de un Servidor Web

Los ciberataques se aprovechan de las vulnerabilidades de los servidores.

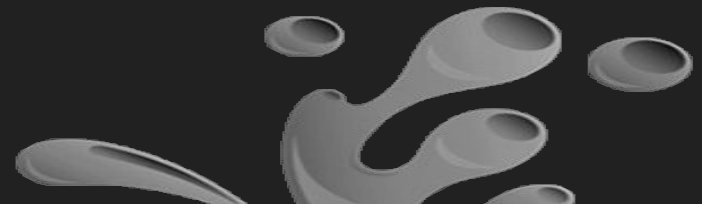
Por ello es importante conocer las vulnerabilidades propias de tu servidor web concreto.

En nuestro caso, describiremos las vulnerabilidades más comunes.

Tipos de vulnerabilidades

Las debilidades más comunes son:

- Archivos de muestra
- Divulgación del código fuente
- Ataques de Canonicalización
- Extensiones del servidor
- Desbordamiento del buffer



Vulnerabilidades de aplicaciones web

Ataques a las propias aplicaciones.

La principal diferencia es que el atacante se centra ahora en el código de aplicación personalizada y no en el software de servidor estándar.

De nuevo nos centraremos en las más comunes.

Vulnerabilidades de las aplicaciones de un Servidor

Tipos de vulnerabilidades:

- Encontrar aplicaciones web vulnerables mediante buscadores web
- Rastreo web
  - Herramientas de rastreo web
- Evaluación de aplicaciones web
- Explorador de Plug-ins
- Suites de herramientas

Medidas de seguridad preventivas

- Remover archivos de muestra no necesarios.

- Nunca se debe almacenar datos confidenciales (contraseñas), en el origen de la aplicación.

- Almacenar los scripts del servidor fuera del árbol de documentos.

Medidas de seguridad preventivas

- Mantenerse al día en la plataforma web.

- No codificar contraseñas (ni datos sensibles) de aplicaciones en archivos .asp, .asa, .php… Cargar fichero de configuración en RAM en tiempo de ejecución

- Parchear o deshabilitar las extensiones vulnerables conocidas.

¿Cómo detectar vulnerabilidades?

- Existen herramientas que automatizan el proceso de análisis de servidores web en busca de vulnerabilidades.

- Escáneres de vulnerabilidad de Servidores Web:

  - Algunos también pueden buscar posible malware.
  - Potencial arma de doble filo.
  - Subsanar fallos conforme los detecte la herramienta.


GRACIAS
¿Dudas?¿Preguntas?