Buenas Prácticas Esenciales de Seguridad en Servidores Web Linux

Asegurar un servidor Linux es crucial para proteger tus servicios web de amenazas. Aquí tienes las prácticas esenciales para fortalecer la seguridad de tu servidor Linux.

1 Gestión de Actualizaciones

- Mantén el sistema, kernel y servicios actualizados y asegurate de instalar parches de seguridad rápidamente.

2 Control de Usuarios y Privilegios

- Deshabilita el acceso directo a root. Usa sudo y aplica mínimos privilegios a los usuarios.

3 Seguridad en Acceso Remoto (SSH)

- Permite solo claves SSH, cambia el puerto y usa Fail2Ban para evitar ataques por fuerza bruta.

4 Cortafuegos y Filtrado

- Configura un firewall y permite solo puertos y tráfico necesarios.

5 Deshabilita Servicios y Puertos No Utilizados

- Revisa y desactiva servicios innecesarios y cierra puertos no utilizados.

6 Detección de Intrusos (IDS)

Monitoriza la actividad del servidor y recibe alertas en tiempo real sobre accesos sospechosos.

7 Protección de Servicios Web

Configura HTTPS, cabeceras de seguridad y deshabilita módulos innecesarios.

8 Monitoreo y Auditoría

- Registra y revisa logs constantemente para detectar actividades anómalas.

9 Copias de Seguridad y Recuperación

- Realiza backups frecuentes y guardalos en varias ubicaciones para mayor seguridad y disponibilidad.

10 Seguridad en Aplicaciones y Bases de Datos

- Mantén bases de datos y aplicaciones actualizadas y restringe el acceso.

Estas prácticas fortalecen y protegen eficazmente tu servidor Linux contra amenazas amenazas cibernéticas.