**"Propuesta de Hardening para un servidor empresarial Linux/Windows"**

1. ¿Por qué he elegido este tema?

*-"Según el INE, el 43% de las PYMES en España sufrieron ciberataques en 2023 por configuraciones inseguras".*

*-"El Instituto Nacional de Ciberseguridad (INCIBE) dice que el 38% de los ciberataques a hospitales en España en 2023 explotaron servidores mal configurados, especialmente en servicios expuestos como RDP y bases de datos. Mi TFG abordará este problema aplicando hardening a un servidor Linux o Windows que simula un entorno hospitalario/empresarial, cerrando puertos innecesarios, implementando autenticación en dos factores (2FA) para SSH y cifrando datos sensibles (PGP)."*

* Idea principal del TFG:

El proyecto consistirá en la aplicación de técnicas de hardening sobre un servidor [Linux o Windows], simulando un entorno empresarial real. El objetivo es reducir la superficie de ataque mediante la configuración segura de servicios, gestión de usuarios y políticas de acceso, siguiendo estándares como CIS Benchmarks. Se incluirá una evaluación previa y posterior para demostrar la eficacia de las medidas implementadas."

* Tecnologías utilizadas:

- Herramientas: Lynis/OpenSCAP/Nmap, iptables o nftables (según el SO utilizado).

- Entorno: (VirtualBox/Proxmox/VMware) + (Ubuntu Server/CentOS/Windows Server 20xx).

- Documentación: CIS Benchmarks, guías NIST.

-Ayuda extra: En caso de duda preguntaré a mis compañeros de mi departamento de informática de la empresa en la que estoy trabajando actualmente. También utilizare en casos muy concretos la IA para que me resuelva duda y/o me haya quedado estancado en algún punto de la redacción.

Fecha de entrega: 4 de abril de 2025.