Tarea – HT-04

1. ¿Cómo puede la configuración de SSH y el uso de autenticación basada en claves mejorar la seguridad general del servidor?

Aumenta la seguridad al eliminar contraseñas vulnerables y usar claves criptográficas únicas para cada usuario autorizado.

2. ¿Qué riesgos podría implicar una incorrecta configuración de redes y cómo se pueden mitigar?

Podría exponer servicios al público o permitir ataques. Se previene con firewalls, reglas seguras y monitoreo del tráfico.

3. ¿Por qué es importante mantener los paquetes de software actualizados, y qué consecuencias podría tener no realizar actualizaciones regulares?

Actualizaciones corrigen fallos de seguridad y mejoran el rendimiento. No hacerlo deja el sistema expuesto a ataques.

4. Al realizar un análisis de servidores, ¿qué métricas son las más relevantes para detectar problemas de rendimiento y seguridad?

CPU, memoria, latencia de disco, actividad de red y registros del sistema son claves para detectar anomalías.

5. ¿Qué medidas adicionales podrías tomar para garantizar la seguridad de los sistemas de archivos y los datos almacenados en un servidor Red Hat?

Usar cifrado de disco, aplicar políticas de permisos, activar SELinux, y realizar auditorías y copias seguras periódicamente.