Tarea – HT-04

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

Evita el uso de contraseñas débiles, reduce ataques de fuerza bruta y permite conexiones seguras mediante claves cifradas.

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

Puede causar accesos no autorizados o interrupciones. Se mitiga usando firewalls, segmentación de red y revisando reglas de acceso.

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

Corrige vulnerabilidades y mejora estabilidad. No actualizar puede exponer el sistema a ataques y errores críticos.

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

Uso de CPU, memoria, disco, tráfico de red, logs del sistema y número de procesos activos.

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

Cifrado de datos, control de permisos, SELinux activo, copias de seguridad seguras y monitoreo constante.