**SEGURIDAD INFORMÁTICA** – 2º SMR Torrelavega, febrero de 2024

Criterios: Se evaluarán únicamente las respuestas que estén debidamente **justificadas.**

**Contexto**

* Entorno de virtualización VirtualBox.
* Máquina virtual Kali Linux con tu nombre y la palabra ataca.
* Máquina virtual Metasploitable2 con tu nombre y la palabra atacada.
* Conexión entre ambas máquinas virtuales
* Máquina virtual Windows con tu nombre y la palabra recupera

**Tercera parte** (50 ptos)

1. Verificación de archivos.
   1. Descarga la aplicación PSPad Portable 64b (en inglés) de la web del fabricante.
   2. Explica con tus palabras qué es un hash y cómo puede utilizarse para verificar el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
   3. Calcula el hash **sha1** del archivo que te has descargado
   4. Contrasta el hash calculado con el que proporciona el fabricante.
2. Recuperación de datos
   1. En tu máquina virtual Windows Instala otro disco duro de 10 GB y formatéalo (rápidamente) con el sistema de archivos ntfs, asignándole la letra E:\ y tu nombre como etiqueta del volumen.
   2. En el disco E: crea una carpeta llamada tu\_nombre\_cervantes y guarda en ella un archivo con un fragmento del quijote y una foto de Cervantes.
   3. Borra la carpeta entera y copia en el disco E: otra carpeta con otros 2 archivos dentro. Vacía la papelera.
   4. Descarga la aplicación Disck Drill que permite recuperar documentos borrados.
   5. Escanea el nuevo volumen
   6. Muestra los archivos observados
   7. Recupera los archivos borrados
   8. Busca y menciona otras dos aplicaciones para recuperar datos.