Seguridad de la Información – CURSO 2025-2026

Práctica 1: Configuración del entorno Kali Linux - Taller de OpenSSL

Los objetivos de esta práctica son la configuración de nuestro entorno de trabajo para poder realizar las prácticas siguientes (Taller de OpenSSL) en entorno **Kali Linux nativo o** en **máquina virtual** actualizada **Kali Linux**, que tendrá instalado **OpenSSL versión 3 o superior**.

Herramientas básicas que han de ser instaladas / utilizadas en el entorno escogido:

OpenSSL (mínimo versión 3.20)
Editor de texto (vi, gedit, editor de notas, etc.)
Comando "xxd" de Linux (visualizador/editor binario)
Comando "dd" de Linux (copia binaria)
Comando "hexdump" de Linux (recomendado)
Utilidad "ripmime" de Linux (paquete ripmime, proceso de ficheros MIME)

Documentación básica:

- Wikipedia ASCII (https://es.wikipedia.org/wiki/ASCII)
- Wikipedia ISO/IEC 8859-1 (https://es.wikipedia.org/wiki/ISO/IEC_8859-1)
- Wikipedia BASE64 (https://es.wikipedia.org/wiki/Base64)
- Wikipedia MIME (https://es.wikipedia.org/wiki/Multipurpose_Internet_Mail_Extensions)
- Openssl Howto (https://openssl.cicei.com)
- Documentación de Openssl (https://www.openssl.org/docs/man3.2/index.html)
- ChatGPT (https://openai.com/chat) , DeepSeek (https://chat.deepseek.com), etc.

Objetivos:

- Definir y configurar en su caso, el entorno operativo Kali Linux, OpenSSL
- Entender la diferencia entre ficheros de texto y ficheros binarios
- Entender los estándares y formatos ASCII, ISO8859, BASE64 (PEM), MIME
- Primeros pasos con OpenSSL

Actividades obligatorias:

- Comandos básicos: openssl version, openssl speed
- Crear 2 archivos binarios (de 8 y 256 bytes) con openssl rand
- Convertirlos a Base64 (comandos base64 y openssl enc -a) y volver a binario, compararlos
- Crear un fichero binario con 16 bytes de valor cero (00) y otro con 64 bytes de valor 255 (FF)
- Visualizarlos en hexadecimal y en octal
- Enviarnos un mensaje de correo a nuestra propia cuenta con una pequeña imagen y un pequeño fichero Word (o similar) adjuntos.
- Desde la ventana de visualización del mensaje, descargar el mensaje como ".eml". Visualizarlo e interpretarlo
- Extraer los ficheros adjuntos en línea de comando con la utilidad "ripmime", después de instalar el paquete con el mismo nombre.
- Comparar los ficheros extraídos con los originales

Esta primera práctica no será entregada ni evaluada. Los estudiantes que siguen la asignatura por curso deberán mostrar al profesor los avances realizados en el laboratorio y los estudiantes que no siguen la asignatura por curso la podrán realizar (y lo aconsejamos encarecidamente) pero no es necesaria su entrega ni defensa.