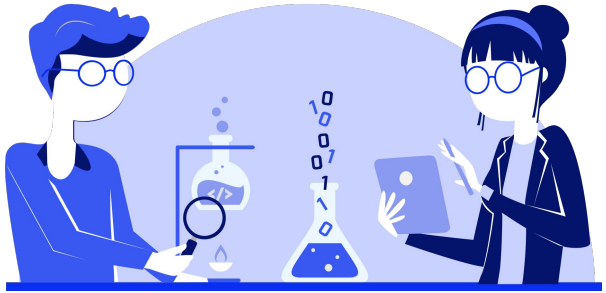
educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3 - Laboratorio adicional

Para poder realizar este laboratorio, se recomienda:

- Revisar contenidos previos.
- Descargar los elementos necesarios.



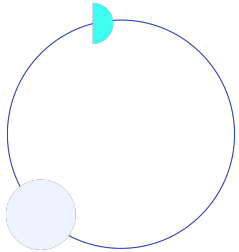
Ejercicio 1

Sigue las consignas para calcular el resumen de un mensaje con el algoritmo *SHA3-256* utilizando ***OpenSSL***:

1. Para consultar la documentación, utiliza **`man openssl-dgst`**.
2. Con el comando **`seq`** genera un archivo **`muestra.txt`** con los números de **1 al 20.000**.
3. Verifica los algoritmos soportados con el comando **`openssl dgst -list`**.
4. Para calcular el ***HMAC***, utilizaremos el subcomando **`openssl dgst`** con la opción ***sha-256***.

Ejercicio 2

Nuestro objetivo es **criptoanalizar contraseñas *hasheadas* para poder descifrarlas**. Lo haremos mediante el comando **hashcat**, a partir de la siguiente lista de contraseñas *hasheadas*:



$2y$10$TYau45etgP4173/zx1usm.uO34TXAld/8e0/jKC5b0jHCqs/MZGBi

$2y$10$qQVWugep3jGmh4ZHuHqw8exczy4t8BZ/Jy6H4vnbRiXw.BGwQUrHu

$2y$10$DuZ0T/Qieif009SdR5HD5OOiFl/WJaDyCDB/ztWIM.1koiDJrN5eu

$2y$10$0ClJ1l7LQxMNva/NwRa5L.4ly3EHB8eFR5CckXpgRRKAQHXvEL5oS

$2y$10$LIWMJJgX.Ti9DYrYiaotHuqi34eZ2axl8/i1Cd68GYsYAG02Icwve

1. En el Escritorio de la máquina virtual ***Kali Linux***, dentro de la carpeta ***cripto***, abre una terminal y escribe `hashcat - -help` para consultar las opciones necesarias para implementar el ataque por diccionario.
2. Utiliza el diccionario ***xato-net-10000.txt*** disponible en la carpeta ***Passwords*** dentro de la carpeta ***cripto***.
3. La lista de contraseñas *hasheadas* la encontrarás disponible bajo el nombre ***hashes.txt***.

¡Sigamos trabajando!