Simulación de ataques en Kali Purple
(a la vez que su realización ir documentando en github con los pantallazos explicados más relevantes)

1.- Creación de diccionarios con PYDICTOR Y DYMERGE
Vamos a trabajar con la herramienta Pydictor, que permite la creación de diccionarios para fuerza bruta. Sus principales características son las siguientes:

- Pydictor se utiliza para crear diccionarios para fuerza bruta.
- Esta herramienta crea la lista de palabras tanto en palabras normales como en diferentes tipos de cifrado, como el cifrado base64.
- Pydictor está escrito en Python.
- Hay dos métodos para romper la contraseña usando esta herramienta:
    - crear una lista de palabras normales.
    - crear la lista de palabras en formato base64.

-Instala las herramientas Pydictor y Dymerge y crea dos diccionarios de palabras con Pydictor: uno con números y otro con una lista de palabras con letras en mayúsculas.
- fusiona los dos diccionarios anteriores en un solo llamado diccionarion con la herramienta Dymerge.

Al ataque!!!

Utilizaremos la herramienta Hydra para simular 2 ataques por fuerza bruta con diccionarion:

2.- Utilizar diccionarion con Hydra para simular un ataque de fuerza bruta en SSH:

1. **Instalar OpenSSH**
2. **Iniciar y configurar el servidor SSH** en Kali Purple.
3. **Crear un usuario** que simule ser el objetivo de tus pruebas.
4. **Conectar al servidor SSH** desde tu sistema.
5. **Simular un ataque de fuerza bruta** utilizando Hydra y diccionarion
6. **Revisar los logs** del sistema para analizar los intentos de conexión.
7. **Analizar los resultados** y estudiar cómo mitigar ataques similares en entornos reales.

3.- Utilizar diccionarion con Hydra para simular un ataque de fuerza bruta con HTTP (formulario web)

1. **Instalar y configurar DVWA(https://github.com/digininja/DVWA)** como una aplicación web vulnerable en tu servidor Apache local.
2. **Identificar los detalles del formulario de login** para poder construir el ataque.
3. **Usar Hydra** para realizar un ataque de fuerza bruta, utilizando diccionarion.
4. **Analizar los resultados** y estudiar cómo mitigar ataques similares en entornos reales.