ESCUELA POLITÉCNICA NACIONAL

# CONSTRUCCIÓN Y EVOLUCIÓN DE SOFTWARE (ISWD633)

| | |
|---|---|
| **INTEGRANTES:** | • Ismael Toala<br>• Sebastián Donoso |
| **FECHA:** | 02-08-2025 |
| **TEMA:** | Taller 2: *Crea tu propia "librería personal"* |

🛠️ **Habilidad identificada**

**Escaneo y análisis de vulnerabilidades**

📚 **Librería: VulnScanLib**

Esta librería personal está compuesta por funciones reutilizables enfocadas en el reconocimiento pasivo, análisis de información y explotación básica mediante fuerza bruta. Está diseñada para quienes deseen realizar auditorías de seguridad a nivel principiante o intermedio.

🔧 **Funciones Incluidas**

**Reconocimiento_pasivo()**

- **Descripción**: Recolecta información públicamente disponible (OSINT) usando técnicas de *Google Dorking*.
- **Inputs**:
  - Nombre completo
  - Cédula de identidad
  - Dominio web u organización
- **Procedimiento**:
  - Realizar búsquedas avanzadas en Google para encontrar información indexada.
  - Identificar patrones: gustos, nombres de familiares, fechas importantes, correos electrónicos, contraseñas filtradas.
  - Guardar toda la información obtenida en una carpeta organizada por objetivo.
- **Tiempo estimado**: Variable, depende del objetivo.
- **Nivel**: Principiante

**Analisis_informacion()**

- **Descripción**: Procesa la información recolectada y la prepara para su uso posterior.
- **Inputs**:
  - Carpeta con archivos recolectados en la fase anterior
- **Procedimiento**:
  - Extraer los datos más relevantes y volcarlos en un archivo .txt.
  - Filtrar posibles datos útiles para construir un diccionario de contraseñas.
- **Tiempo estimado**: Variable
- **Nivel**: Medio

**Elaborar_diccionario_y_explotacion()**

- **Descripción**: Genera diccionarios personalizados y ejecuta pruebas de fuerza bruta.
- **Inputs**:
  - Archivo .txt con información relevante (nombres, fechas, palabras clave)
- **Procedimiento**:
  - Utilizar la herramienta crunch para generar diccionarios con base en los datos.
  - Automatizar ataques de fuerza bruta con scripts personalizados.
  - Probar las contraseñas obtenidas en diferentes servicios (correos, redes sociales) en busca de reutilización.
- **Tiempo estimado**: Variable
- **Nivel**: Medio

**Evaluación de la Librería**

| Criterio | Evaluación |
|---|---|
| **Claridad** | Las funciones están bien descritas, con inputs, procesos y nivel técnico. |
| **Reusabilidad** | Cada función puede ser utilizada por otros para procesos similares. |
| **Facilidad de Integración** | Se pueden integrar fácilmente a flujos de pentesting u otras librerías OSINT. |

**Posibles mejoras futuras**

- Agregar función Exportar_Informe() para generar reportes automáticos en PDF o Markdown.
- Crear una interfaz gráfica o usar Notion API para centralizar y visualizar mejor los hallazgos.
- Modularizar los scripts con buenas prácticas de desarrollo (manejo de errores, logs, etc.).