DOCUMENTACIÓN PIA CIBERSEGURIDAD

Autores: Carlos Enrique Ortega González, José Eduardo Rivera Gámez, Ximena Pérez Escamilla

Nombre del Proyecto: PIA CIBERSEGURIDAD

**DESCRIPCIÓN GENERAL**

Realizar diferentes Tareas de Ciberseguridad, como el escaneo de puertos, el web scraping, revisión de encabezados, información de sockets, cifrado César de mensaje, obtención de metadata, API de Shodan, obtención de hashes de archivos.

**SCRIPTS**

* PIA.py (script principal)
* Funciones.py (funciones para realizar las tareas de ciberseguridad)
* Hash.ps1 (obtener hash de archivos)

**PARÁMETROS**

* modo: Sirve para elegir la Tarea de Ciberseguridad que va a realizar el script.
  + CHOICES
  + p: Escaneo de puertos
  + s: Web Scraping
  + e: Revisión de encabezados
  + si: Información de sockets
  + cm: Cifrado César de mensaje
  + meta: Obtención de metadata
  + API: API de Shodan
  + hash: Obtener hashes de archivos
* target: IP para escanear puertos.
* url: Link de la página para realizar un web scraping o revisión de encabezados (\*\*Debe de escribirse con http/https y entre comillas\*\*).
* host: Dominio de la página de la que se obtendrán sus encabezados (\*\*Encierre en comillas el dominio “google.com” \*\*)
* msj: Mensaje que queremos cifrar (\*\*Encierre en comillas el mensaje “Hola mundo” \*\*)
* clave: Clave con la que queremos cifrar (\*\*La clave debe de ser un número\*\*)
* path: Ruta en donde se encuentran las imágenes para obtener su metadata (\*\*Encierre en comillas el path “C:\Users\user1\” \*\*)
* APIkey: Llave de la API del sitio <https://www.shodan.io/>
* search: Término a buscar en la API de Shodan (\*\*Encierre en comillas el término “camaras” \*\*)
* ruta: Ruta para analizar los hashes de los archivos encontrados (\*\*Encierre en comillas la ruta “C:\Users\user1\” \*\*)

**FUNCIONES**

**scanPorts(target)**

Realiza un escaneo de los puertos de la IP ingresada y solo toma en cuenta los puertos que estén abiertos, los puertos son guardados en el documento OpenPorts.csv junto a demás información de estos como su protocolo o IP de donde se encuentran. Se puede (\*\*Es necesario descargar un nmap como Zenmap <https://nmap.org/download.html> \*\*)

EJEMPLO DE USO:

- python PIA.py -modo p -target 127.0.0.1

Para realizar un escaneo completo cambie el último octeto de la IP por un 0/24, ejemplo 127.0.0.1 ---> 127.0.0.0/24

- python PIA.py -modo p -target 127.0.0.0/24

**SCRAPING \*\*Se ejecutan las 3 funciones\*\***

**scrapingImages(url)**

Realiza una búsqueda dentro del html de la página proporcionada en el url y encuentra todas las imágenes en este, las imágenes encontradas serán guardadas con el nombre dado en el html, en una carpeta con el nombre images.

**scrapingPDF(url)**

Realiza una búsqueda dentro del html de la página proporcionada en el url y encuentra todos los PDFs en este, los PDFs encontrados se guardaran con el nombre dado en el html, en una carpeta con el nombre pdfs, de otro modo no se creara.

**scrapingLinks(url)**

Realiza una búsqueda dentro del html de la página proporcionada en el url y encuentra todos los links en este, los links encontrados se imprimirán en pantalla.

EJEMPLO DE USO:

- python PIA.py -modo s -url “https://www.google.es”

**checkHeaders(url)**

Obtiene los encabezados del url proporcionado como lo puede ser la fecha, el servidor, entre otras cosas.

EJEMPLO DE USO:

- python PIA.py -modo e -url “https://www.google.es”

**socketInfo(hostname)**

Obtiene la información de los sockets encontrados en el host proporcionado y la guarda en el archivo Encabezados.txt, en la información se puede encontrar la familia ya sea IPv4 o IPv6, IP y puerto, entre otros.

EJEMPLO DE USO:

- python PIA.py -modo si -host “google.com”

**cifrado(mensaje, clave)**

Cifra un mensaje con el método César y con una clave por default de 4 (\*\*La clave se puede cambiar por cualquier otra con el parámetro de clave\*\*) **OBLIGATORIO INCLUIR MENSAJE**

EJEMPLO DE USO:

- python PIA.py -modo cm -msj "Hola mundo"

- python PIA.py -modo cm -msj "Hola mundo" -clave 8

**METADATA \*\*Solo se ejecuta la función printMeta, esta llama a las otras 2\*\***

**decode\_gps\_info(exif)**

Convierte las coordenadas de la latitud y longitud a unas mejor entendibles para todos.

**get\_exif\_metadata(image\_path)**

Obtiene la metadata de las imágenes.

**printMeta(path)**

Recoleta la metadata de las anteriores funciones y la guarda en Metadata.txt **OBLIGATORIO INGRESAR PATH**

EJEMPLO DE USO:

- python PIA.py -modo meta -path "C:\Users\user1\Pictures\"

**API(APIkey, search)**

Realiza una búsqueda en la API de Shodan **OBLIGATORIO INGRESAR APIKEY VALIDA Y TÉRMINO DE BÚSQUEDA**

**PowerShell(rhash)**

Obtiene todos los hashes de los archivos encontrados en la ruta proporcionada.

EJEMPLO DE USO:

- python PIA.py -modo hash -ruta "C:\Windows\System32\drivers\"