



PROGRAMACIÓN
PARA
CIBERSEGURIDAD

Instrucciones de uso



Descripción

Este script busca facilitarle al usuario las siguientes tareas:

- Cifrar mensajes
- Obtener metadata
- Enviar correos
- Escanear puertos
- Realizar Web Scraping
- DNS
- Hash



Instalación

Clonar el repositorio con el comando:
git clone https://github.com/angmont/PIA_PC.git
Para instalar módulos se usa:
pip install -r requirements.txt

argumento -t

Este argumento permite que el usuario pueda elegir la tarea que desee ejecutar
Ejemplo: py main.py -t dns

Módulos utilizados

Necesarios de instalar

- python_docx
- requests
- pyhunter
- openpyxl
- tqdm
- googlesearch_python
- BeautifulSoup
- docx
- Pillow
- PyPDF2

No necesarios de instalar

- socket
- argparse
- logging
- hashlib
- subprocess
- os
- time
- smtplib
- getpass
- ssl
- eyed3
- urllib
- entre otros

-t dns

Tarea enfocada precisamente a realizar consultas DNS, así como ver nuestro caché o inclusive borrarlo. No necesita de más argumentos, todas las actividades que se le puedan consultar al usuario se harán por medio de un menú, ya sólo sería cuestión del usuario escribir el número de su preferencia.

```
C:\Users\amont\PIA_PC>py main.py -t dns
¿Qué opción desea realizar?
[1] Consulta DNS
[2] Ver Caché
[3] Borrar Caché
[4] Salir
:
```

Aclaración: Los resultados de la opción 'Ver caché' se guardaran en una txt denominado 'Informacion_Cache' en la ruta donde se ejecutó el script.

-t cifrado

Esta tarea hace uso del ya tan conocido cifrado César, contiene 5 distintas funciones las cuales se pueden elegir mediante el argumento “-m”.

-m (cifmensaje / desmensaje)

Puede cifrar o descifrar cualquier mensaje que el usuario le presente, es necesario que se otorgue una llave para realizar el cifrado o descifrado (“-key”) así como el mensaje a cifrar o descifrar (“-msj”).

```
C:\Users\amont\PIA_PC>py main.py -t cifrar -m cifmensaje -msj ejemplo -key 3
hnhpsor
C:\Users\amont\PIA_PC>
```

-m cifgithub

Consulta la api de github, pero nos devuelve los resultados cifrados en un txt. Es necesario otorgar tanto el usuario de github al que se le desea consultar sus repositorios mediante la api (“-user”), así como la llave de cifrado (“-key”). Los resultados los podrá encontrar en la misma carpeta donde se ejecutó el script, bajo el nombre “usuario_cifgithub.txt”. (el usuario varía dependiendo del user)

```
C:\Users\amont\PIA_PC>py main.py -t cifrar -m cifgithub -user angmont -key 3
Hecho!
C:\Users\amont\PIA_PC>
```

-m (ciftxt / destxt)

Si desea cifrar o descifrar un archivo txt, puede hacerlo con el mismo script, sólo es necesario otorgar la ruta en donde se encuentra la carpeta con el archivo txt (“-ru”) junto con la llave (“-key”). Los resultados los podrá encontrar en la misma carpeta donde se ejecutó el script, bajo el nombre de dicho archivo junto con “_cifrado.txt” o “_descifrado.txt” según sea el caso.

```
C:\Users\amont\PIA_PC>py main.py -t cifrar -m destxt -ru C:\Users\amont\PIA_PC\angmont_cifgithub.txt -key 3
Hecho!
C:\Users\amont\PIA_PC>
```

-t correos

Realiza una consulta a la API de Hunter mediante el dominio que sea de preferencia, de ahí en adelante los resultados los guarda en un xlsx y los envía por correo.

Primero hay que tener en cuenta que solo funciona para enviar correos desde una cuenta de Microsoft, teniendo esto en mente el script funciona de la siguiente manera:

Se deben ingresar los datos solicitados, como es el remitente ("rem"), el destinatario ("des"), el dominio a consultar ("url"), el contenido que llevará el correo ("cont") y el asunto ("asu").

```
C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main>py main.py -t correos -rem dariela.hurtadotrs@uanl.edu.mx -des alegmonald@gmail.com -cont "Hola, este es un ejemplo de envío de correos" -url uanl.mx -asu "Ejemplo PIA"
```

Posteriormente se le solicitará su API key de Hunter y la contraseña de su correo, pero no se preocupe, su API key y contraseña no serán mostradas en pantalla.

```
C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main>py main.py -t correos -rem dariela.hurtadotrs@uanl.edu.mx -des alegmonald@gmail.com -cont "Hola, este es un ejemplo de envío de correos" -url uanl.mx -asu "Ejemplo PIA"  
Ingresa tu API key:  
Ingresa su contraseña:
```

Por último se le mostrará en pantalla el proceso de conexión con el servidor de correo y si éste fue mandado con éxito o no.

```
C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main>py main.py -t correos -rem dariela.hurtadotrs@uanl.edu.mx -des alegmonald@gmail.com -cont "Hola, este es un ejemplo de envío de correos" -url uanl.mx -asu "Ejemplo PIA"  
Ingresa tu API key:  
Ingresa su contraseña:  
[+] Conectando con el Servidor de Correo.  
[+] Iniciando Encriptación de Sesión.  
[+] Iniciando Sesión en el Servidor de Correo.  
[+] Enviando Correo.  
[+] Correo Electrónico Enviado con Éxito a: alegmonald@gmail.com
```



-t metadata

Esta tarea se encarga de sacar el metadata de distintos tipos de archivos (png/jpg, pdf, docx, mp3) cuenta con la opción de sacar a un solo archivo o a toda una carpeta de éstos archivos.

Aclaración:

Si busca sacar el metadata de toda una carpeta de archivos, éstos deben de ser de la misma extensión.

-a (imagen / pdf / word / mp3)

Para sacar el metadata de una sola imagen, pdf, docx o mp3. Se debe ingresar el path donde se encuentra utilizando el parámetro "-ru" y de igual forma se debe ingresar un path donde estarán los resultados de ésta extracción "-mp".

Aclaración: en -a se debe aclarar de que tipo de documento se está hablando, por ejemplo: "-a imagen". Recuerde poner el nombre del archivo y su terminación.

```
C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main>py main.py -t metadata -a word -ru C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main\Docx\Docx\E1-Lectura_Scripts.docx -mp C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main\Docx\Meta_Docx
El archivo con los MetaDatos a sido creado de manera exitosa
```

-a (imagenes / pdfs / words / mp3s)

Si lo que desea es sacar el metadata de toda una carpeta de imágenes, pdfs, docxs o mp3s. Se debe ingresar el path donde se encuentra dicha carpeta utilizando el parámetro "-ru" y de igual forma se debe ingresar un path donde estarán los resultados de ésta extracción "-mp".

Aclaración: en -a se debe aclarar de que tipo de documento se está hablando, por ejemplo: "-a pdfs".

```
C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main>py main.py -t metadata -a pdfs -ru C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main\Pdf\PDF -mp C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main\Pdf\PDF_Meta
Los Metadatos del archivo pdf1.pdf si es que existen se han generado en un txt.
Los Metadatos del archivo pdf2.pdf si es que existen se han generado en un txt.
Los Metadatos del archivo pdf3.pdf si es que existen se han generado en un txt.
Los Metadatos del archivo pdf_1.pdf si es que existen se han generado en un txt.
```



-t web

Esta tarea realiza diversas actividades dentro del web scraping, cada una de estas se puede elegir con el argumento "-m".

-m busqueda

Puede realizar cualquier busqueda en google dependiendo de lo que quiera el usuario, todos los resultados (links) los imprimirá en pantalla, solamente se deberá otorgar la busqueda deseada ("-bus").

```
C:\Users\amont\PIA_PC>py main.py -t web -m busqueda -bus cheetos
https://www.cheetos.com/
https://www.cheetos.com/
https://www.cheetos.com/es
https://cheetos.com.mx/
https://en.wikipedia.org/wiki/Cheetos
https://listado.mercadolibre.com.mx/cheetos
https://super.walmart.com.mx/promociones-especiales/pepsico/cheetos/_/cat3720141
https://www.target.com/p/cheetos-crunchy-flamin-hot-8-5oz/-/A-12992238
https://www.chedraui.com.mx/Departamentos/S%C3%BAper/Despensa/Botanas-y-Fru
tas-Secas/Frutas-Secas-y-Snacks/Cheetos-Flamin-Hot-226-8g/p/00000000003336
471?siteName=Sitio+de+Chedraui
https://twitter.com/cheetos_mx
https://www.superama.com.mx/catalogo/d-despensa/f-botanas-despensa/l-fritur
as/cheetos-xtra-flamin-hot-sabor-chile-y-limon-240-g/0750047802471
/search?q=cheetos&num=11&hl=en&tbm=isch&source=iu&ictx=1&fir=65Ub0PE96XnpAM
%252CdFm-cUK0pRgshM%252C_%253BHhgMtu_xx7g75M%252CZhyYRneEtCg89M%252C_%253B8
vdpDpRc4WrvzM%252CxCzvTwo_SWufC9M%252C_%253BX3_faY9ihSqLXM%252CrRCkevi56h4az
M%252C_%253Bbyphp-Es1fjCXdM%252CWxgmKo32G2fowM%252C_%253BDjFThtRn52lvIM%252C
SS73U8FQnebjyM%252C_&vet=1&usg=AI4_-kRTaoZE0IuK079LdtplTq7Yu59Gpw&sa=X&ved=
2ahUKewjp9JX9-PH0AhVHlmoFHUSJC9AQ_B16BAhaEAE#imgsrc=65Ub0PE96XnpAM
C:\Users\amont\PIA_PC>
```

-m (emails / img / pdf)

Cuando se trata de **-m emails**, podemos decir que comienza a buscar todos los emails existentes en la página de preferencia del usuario, sólo se tiene que otorgar el link ("-url") y después consultara bajo que nombre desea guardarlos en un txt.

```
C:\Users\amont\PIA_PC>py main.py -t web -m emails -url http://uanl.mx
Ingresa el nombre del archivo (sin el .txt): archivito
C:\Users\amont\PIA_PC>
```

En cambio, con **-m (img / pdf)**, el script buscará descargar cualquier imagen o pdf en el link que se provea ("-url").

Aclaración: En el caso de ejecutar **-m img**, se consultará por medio de un input el nombre de la carpeta donde se guardaran las imágenes, mientras que con **-m pdf** se descargarán en la ruta donde se ejecute el script.

```
C:\Users\amont\PIA_PC>py main.py -t web -m img -url http://uanl.mx
Nombre de la Carpeta Donde Desea Guardar Las Imagenes:- carpetita
B5 Imagenes encontradas!
Imagenes Descargadas!
C:\Users\amont\PIA_PC>
```



-t puertos

Esta función realiza un escaneo de puertos para verificar cuáles se encuentran abiertos dentro de una IP proporcionada por el usuario.

Se debe ingresar una IP y los puertos que se desean escanear, el programa, después de haber ingresado éstos datos, mostrará en pantalla una lista de los puertos ingresados, posteriormente iniciará a escanear y volverá a imprimir su resultado (si están abiertos o no).

```
C:\Users\Hurtado\Desktop\Facu\Prog_Ciberseg\PIA\PIA_PC-main>py main.py -t puertos -ip 192.168.100.12 -ports 22,80,25
Se revisará la ip: 192.168.100.12
Con los puertos: 22
Con los puertos: 80
Con los puertos: 25
Empieza el escaneo de la ip: 192.168.100.12 Con los puertos: 22,80,25
Puerto 22:      Cerrado
Puerto 80:      Cerrado
Puerto 25:      Cerrado
```

-t hash

Esta función realiza una obtención de hash de un archivo que el usuario proporcione, éste también debe de seleccionar que tipo de hash desea obtener.

Se debe proporcionar la ruta del archivo al que el usuario desea sacarle el hash, posteriormente el programa mostrará en pantalla un menú con distintas opciones de hash y lo mostrará en pantalla, el usuario deberá seleccionar el de su preferencia y éste script lo guardará en un txt.

```
C:\Users\Hurtado\Documents\GitHub\PIA_PC>py main.py -t hash

Inserte la ruta a analizar
: C:\Users\Hurtado\Documents\GitHub\PIA_PC

¿Qué hash desea realizar?
[1] Md5
[2] Sha512
[3] Sha256

: 1
```

